المختصر للمادة العلمية لشهادة مهندس أمن نظم معلومات معتمد

Certified information systems security professional
hashtag#CISSP

أسئل الله العظيم ان يكون هذا العمل خالص لوجهه، وادعوا كل من أستفد من المادة العلمية الدعاء ل أمي وأبى بالرحمة.

CISSP® | Certified Information Systems Security Professional

Emad M. Abdelhamid • 2nd
Technical Leader | SME IT Security Design @ Cisco - CX EMEA . ...
View my portfolio
1d • Edited •

+ Follow ...

Emad M. Abdelhamid · 2nd

Technical Leader | SME IT Security Design @ Cisco - CX EMEA .
CCIE#58413 | CCDE#20230008 | CISM®| CISA® | CRISC® | CDPSE™ |
ISO27001 LA | ITIL®v4 | F5® Big-IP | NSE4 & NSE7 | PCNSE

Cisco

Riyadh, Saudi Arabia · Contact info

500+ connections

About autour

Over 15 years of experience in Information Security, Infrastructure Security, Cloud Security and Network Security sections.

Experienced in securing on-premises, Cloud, Hybrid, and Multi-cloud architectures, with a focus on design and architecture.

I have Experience in designing, implementing, and measuring Network security Controls and relevant technology management Critical Success Factors (CSF), Key Performance Indicators (KPI), and Metrics.

Proficient in Information System Auditing, IT Risk Management, leading Network and Security teams, IT Security Policy implementation, and Infrastructure Project Management.

I hold multiple professional certifications, including CISM, CISA, CRISC, CDPSE, ISO27001 LA, COBIT5, and ITILv4, as well as technical certifications, such as CCIE Security, CCDE, PCNSE, NSE4, NSE7, and F5 Big-IP.

Extensive work experience in multinational, national, and governmental organizations, including sectors like power stations, manufacturing, construction, transportation, Health and Banking.

I have extensive knowledge and skills in IT governance, information security policies, business continuity planning, disaster recovery planning, vulnerability management, data and information protection, and information security awareness.

I also have strong technology capabilities in firewalls, IPS, web security, mail security, VPN, NAC, ADC, MFA, and network and security monitoring.

I am passionate about solving complex problems, enhancing security performance, and delivering value to clients and stakeholders. I enjoy working with diverse teams, collaborating with partners, and learning new technologies and trends.

Article

CISSP Module 1: Security and Risk Management إدارة الأمن والمخاطر

Emad M. Abdelhamid on LinkedIn

Introduction The Certified Information Systems Security Professional (CISSP) certification is a globally recognized credential in the field of information security. It encompasses a comprehensive body of knowledge designed to ensure professionals have the requisite skills to effectively design, implement,...

Article

CISSP Module 2: Asset Security (Asset Management) أمن الأصول -إدارة الأصول

Emad M. Abdelhamid on LinkedIn

Introduction Asset Security, also known as Asset Management, involves identifying, classifying, protecting, and managing information assets throughout their lifecycle. This domain focuses on ensuring that information assets are adequately protected and managed to support the...

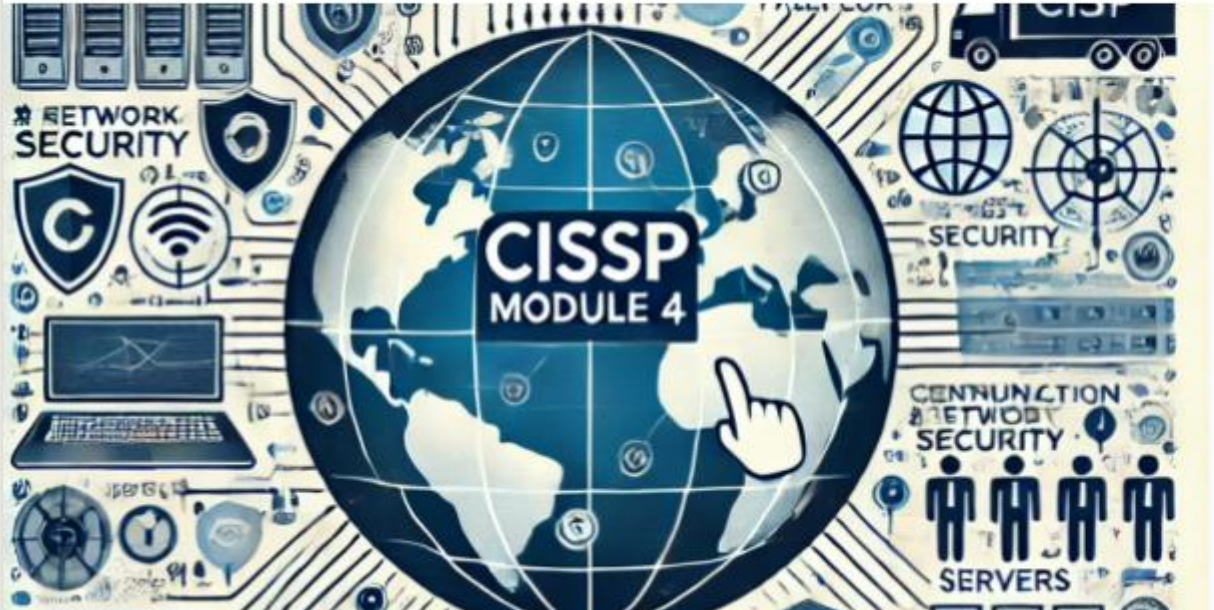
Article

CISSP Module 3: Security Architecture and Engineering الهندسة المعمارية والهندسة الأمنية

Emad M. Abdelhamid on LinkedIn

Introduction This module covers the foundational principles of security architecture and engineering. It includes various security models, cryptographic services, trusted computing bases, cloud computing, digital signatures, system vulnerabilities, cryptanalysis, and physical security. The aim is to...

Article



CISSP Module 4: Communication and Network Security الاتصالات وأمن الشبكات

Emad M. Abdelhamid on LinkedIn

Introduction This module covers the fundamental principles of secure communication and network security. It includes designing secure network architectures, understanding secure network components, implementing secure communication channels, ensuring secure remote access,...

Article

CISSP Module 5: Identity and Access Management (IAM) إدارة الهوية والوصول

Emad M. Abdelhamid on LinkedIn

Introduction This module covers the essential principles of Identity and Access Management (IAM), including identification, authentication, authorization, and accountability. يغطي هذا المقرر المبادئ الأساسية لإدارة الهوية والوصول بما في ذلك التعريف والمصادقة والتفويض والمساءلة It focuses on designing and...

Article

Module 6: Security Assessment and Testing تقييم الأمان والاختبار

Emad M. Abdelhamid on LinkedIn

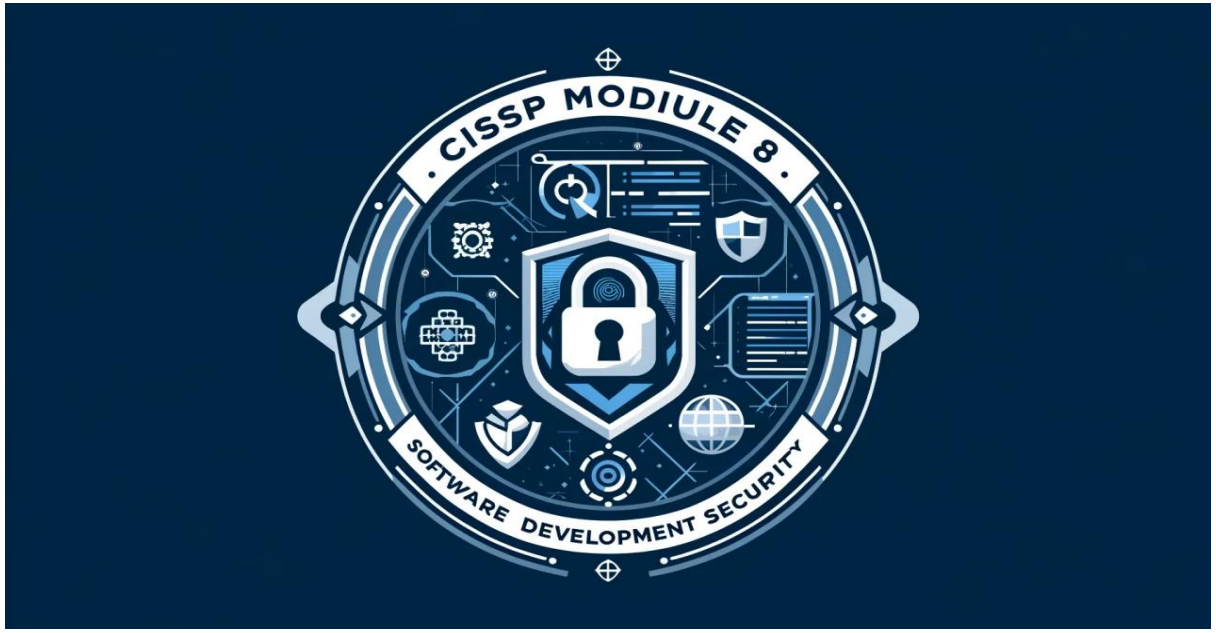
Introduction المقدمة Security assessment and testing are critical components of an organization's security management process. These activities help identify vulnerabilities, ensure compliance with regulations, and improve overall security posture. This module covers various strategies, techniques, and processes...

Article

Module 7: Security Operations / إدارة عمليات الامن السيبرانى

Emad M. Abdelhamid on LinkedIn

Introduction This module covers the principles and practices of security operations. It focuses on understanding and implementing effective security operations, managing security incidents, and ensuring continuous monitoring and improvement of security measures. The goal is to equip professional...



Module 7 : **Module 8: Software Development Security - أمن تطوير البرمجيات**

The module will guide you through the integration of security in the Software Development Life Cycle (SDLC), the application of security controls, the assessment of software security effectiveness, the evaluation of acquired software's security impact, database security, and the implementation of secure coding guidelines and standards.

Emad M. Abdelhamid • 2nd
Technical Leader | SME IT Security Design @ Cisco - CX EMEA . ...
View my portfolio
3w • Edited •

+ Follow ...

من باب تيسير العلوم باللغة العربية، سأقوم بإذن الله دورياً برفع مقالة لشرح مختصر لفصل من فصول شهادة تعتبر من أهم شهادات أمن المعلومات في العالم، وهي شهادة:

hashtag#CISSP - Certified Information Systems Security Professional

To facilitate the study of sciences in Arabic, I will periodically post articles that provide a brief overview of a chapter from one of the most important certifications in information security in the world, which is the:

CISSP - Certified Information Systems Security Professional

ستحتوي هذه المقالات على تلخيص مبدئي لمحتويات الفصل، يليه شرح كل جزء من أجزاء الفصل مدعوماً بأمثلة وتوضيحات وتعريفات. في نهاية كل جزء، سيكون هناك خمس أسئلة لاختبار فهم هذا الجزء مع شرح للإجابات قبل الدخول في الجزء التالي، وهكذا حتى انتهاء الفصل بخاتمة لما تم طرحه، يلي ذلك ذكر المصادر التي تم التجميع منها والتي ستكون مناسبة لدراسة المادة العلمية بالتفصيل في المستقبل.

These articles will include an initial summary of the chapter's contents, followed by a detailed explanation of each section, supported by examples, clarifications, and definitions. At the end of each section, there will be five questions to test the understanding of that section, along with explanations of the answers before moving on to the next section, and so on until the chapter concludes with a summary of what has been presented. This will be followed by the sources from which the material was gathered, which will be suitable for a detailed study of the subject in the future.

ولكنها غير كافية وتحتاج للتحضير. هذه المقالات، بإذن الله، ستكون مقدمة جيدة للتحضير للشهادة بالتفصيل من المصادر المذكورة في نهاية كل مقال.

These articles, once completed, will serve as a good introduction to preparing for the certification. However, they are not sufficient on their own and will require detailed preparation from the sources mentioned at the end of each article.
hashtag#CISSP

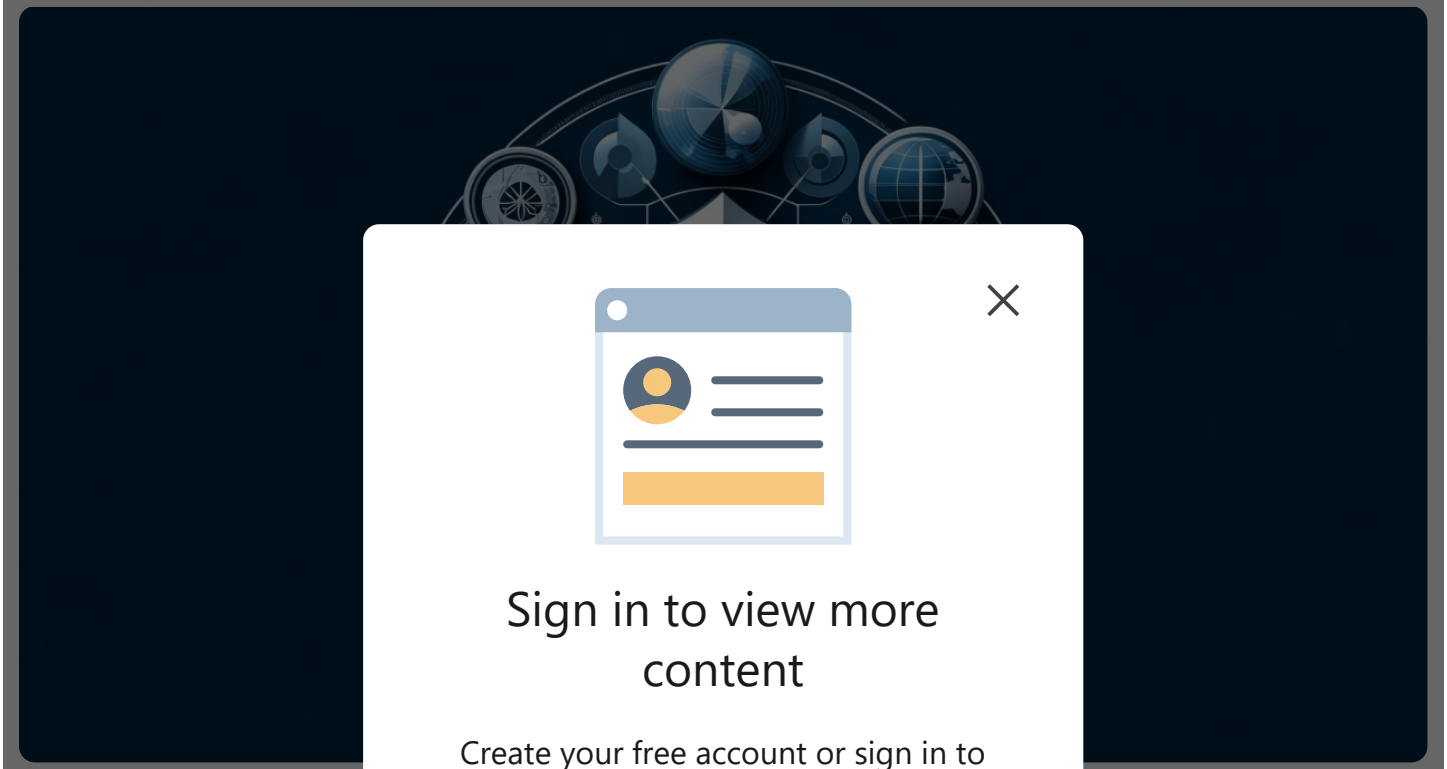
المقالات

For Module 1 : https://lnkd.in/dkkyFGdW
For Module 2 : https://lnkd.in/dNUWhiJs
For Module 3: https://lnkd.in/dsqBXhEc
For Module 4: https://lnkd.in/d_DBAm4h
For Module 5: https://lnkd.in/dGPDeKWF
For Module 6: https://lnkd.in/dZHHJKJx
For Module 7: https://lnkd.in/d_JswW5W
For Module 8: https://lnkd.in/dQsQHqgR

Resources - المصادر

1- Official (ISC)² CISSP Study Guide
2- CISSP (ISC)² Official Practice Tests
3- CISSP All-in-One Exam Guide by Shon Harris
4- Cybrary – CISSP Training by Kelly Handerhan https://lnkd.in/d4zrAkJz
5- Oreilly – CISSP Training by Sari Greene https://lnkd.in/dANS-hVc.
6- CISSP bundles by Thor Pedersen https://lnkd.in/d2tpqaJk
7- CISSP MindMaps YouTube Playlist from Destination Certification https://lnkd.in/deJM44xX

Articles People Learning Jobs Games Get the app



CISSP Mod
Manageme

Emad M. Ab
Technical Lead
CCIE#58413 | (
ISO27001 LA |
Published Jun

+ Follow

™ |

Introduction

The Certified Information Systems Security Professional (CISSP) certification is a globally recognized credential in the field of information security. It encompasses a comprehensive body of knowledge designed to ensure professionals have the requisite skills to effectively design, implement, and manage security programs. The CISSP curriculum is divided into eight domains, with the first domain focusing on

Like Comment Share 371 · 26 Comments

necessary for managing and protecting an organization’s information assets.

شهادة أخصائي أمن نظم المعلومات المعتمد هي اعتماد معترف به عالميًا في مجال أمن المعلومات وتشمل مجموعة شاملة من المعرفة المصممة لضمان أن يكون لدى المهنيين المهارات اللازمة لتصميم وتنفيذ وإدارة برامج الأمن بفعالية تنقسم مناهج إلى ثمانية مجالات يركز أولها على إدارة الأمن والمخاطر ويؤسس هذا المجال المبادئ الأساسية اللازمة لإدارة وحماية أصول معلومات المنظمة

Module 1 Brief:

The Security and Risk Management module covers the essential aspects of creating and maintaining a secure environment within an organization. It is divided into several key areas:

يغطي قسم إدارة الأمن والمخاطر الجوانب الأساسية لإنشاء والحفاظ على بيئة آمنة داخل المنظمة وهو مقسم إلى عدة مجالات رئيسية

1. Confidentiality, Integrity, and Availability (CIA Triad): السرية النزاهة والتوافر
Ensuring information is protected from unauthorized access, maintaining its accuracy and completeness, and ensuring it is available to authorized users when needed.

السرية النزاهة والتوافر: ضمان حماية المعلومات من الوصول غير المصرح به والحفاظ على دقتها واكتمالها وضمان توفرها للمستخدمين المصرح لهم عند الحاجة

2. Governance and Policy الحوكمة والسياسة Developing and enforcing security policies, standards, guidelines, and procedures to ensure consistent security practices across the organization.

الحوكمة والسياسة : تطوير وتنفيذ سياسات ومعايير وإرشادات وإجراءات الأمن لضمان ممارسات أمنية متسقة عبر المنظمة

3. Risk Management إدارة المخاطر Identifying, assessing, mitigating, and monitoring risks to the organization’s information assets through various strategies and methodologies.

إدارة المخاطر : تحديد وتقييم وتخفيف ومراقبة المخاطر التي تواجه أصول معلومات المنظمة من خلال استراتيجيات ومنهجيات مختلفة

4. Legal and Regulatory Compliance الامتثال القانوني والتنظيمي Ensuring adherence to relevant laws, regulations, and standards to protect information and avoid legal consequences.

الامتثال القانوني والتنظيمي: ضمان الالتزام بالقوانين واللوائح والمعايير ذات الصلة لحماية المعلومات وتجنب العواقب القانونية

5. Professional Ethics الأخلاقيات المهنية Upholding ethical standards and principles in the practice of information security.

الأخلاقيات المهنية : الحفاظ على المعايير والمبادئ الأخلاقية في ممارسة أمن المعلومات

6. Security Governance حوكمة الأمن Establishing and maintaining a framework for managing and overseeing the organization's security efforts.

حوكمة الأمن: إنشاء والحفاظ على إطار عمل لإدارة والإشراف على جهود الأمن في المنظمة

7. Threat Modeling نمذجة التهديدات Identifying potential threats and vulnerabilities to the organization's information systems and assessing their potential impact.

نمذجة التهديدات: تحديد التهديدات المحتملة ونقاط الضعف في نظم معلومات المنظمة وتقييم تأثيرها المحتمل

8. Business Continuity and Disaster Recovery Planning تخطيط استمرارية الأعمال والتعافي من الكوارث Developing plans and procedures to ensure the organization can continue operations and recover quickly in the event of a disruption or disaster.

تخطيط استمرارية الأعمال والتعافي من الكوارث : تطوير خطط وإجراءات لضمان استمرار عمليات المنظمة والتعافي بسرعة في حالة حدوث اضطراب أو كارثة

Graph 1: CIA

1. Confidentiality, Integrity, and Availability (CIA Triad):

• Confidentiality

Confidentiality ensures that sensitive information is accessed only by authorized individuals. It involves implementing access controls, encryption, ensuring the principle of least privilege, and data classification to identify and protect sensitive

information.

تضمن السر ية أن الوصول إلى المعلومات الحساسة يتم فقط من قبل الأفراد المصرح لهم وتشمل تطبيق ضوابط الوصول التشفير ضمان مبدأ الحد الأدنى من الامتياز وتصنيف البيانات لتحديد وحماية المعلومات الحساسة

• ***Access Controls:*** Include methods like mandatory access control (MAC), discretionary access control (DAC), role-based access control (RBAC), and attribute-based access control (ABAC) to ensure only authorized individuals can access sensitive information.

ضوابط الوصول تشمل طرق مثل : التحكم في الوصول الإلزامي , التحكم في الوصول التقديري, التحكم في الوصول المستند إلى الدور, والتحكم في الوصول المستند إلى السمة لضمان أن الأفراد المصرح لهم فقط يمكنهم الوصول إلى المعلومات الحساسة

• ***Encryption:*** Techniques such as symmetric encryption (AES) and asymmetric encryption (RSA) protect data at rest, in transit, and in use.

التشفير : تقنيات مثل التشفير المتماثل والتشفير غير المتماثل لحماية البيانات المخزنة او أثناء النقل وفي الاستخدام

• ***Least Privilege:*** This principle ensures users are granted the minimum level of access necessary to perform their job functions, reducing the risk of unauthorized access.

الحد الأدنى من الامتياز : يضمن هذا المبدأ أن يحصل المستخدمون على أقل مستوى من الوصول اللازم لأداء وظائفهم الوظيفية مما يقلل من خطر الوصول غير المصرح به

• ***Data Classification:*** Organizing data based on sensitivity and criticality helps in applying appropriate protection measures. Categories might include public, internal, confidential, and top secret.

تصنيف البيانات : تنظيم البيانات بناءً على الحساسية والأهمية يساعد في تطبيق تدابير الحماية المناسبة قد تشمل الفئات عامة داخلية سر ية وسر ية للغاية

-Example: Using AES-256 encryption to protect sensitive customer data stored in a database.

استخدام التشفير لحماية بيانات العملاء الحساسة المخزنة في قاعدة البيانات

-Example: A company implements RBAC to ensure only employees with the role of "HR Manager" can access the payroll system. Additionally, junior accountants are

given access only to the financial records needed for their tasks, not to all company financial data.

تقوم شركة بتطبيق لضمان أن الموظفين ذوي دور مدير الموارد البشرية فقط يمكنهم الوصول إلى نظام الرواتب بالإضافة إلى ذلك يتم منح المحاسبين الصغار الوصول فقط إلى السجلات المالية المطلوبة لمهامهم وليس إلى جميع البيانات المالية للشركة

• Integrity النزاهة

Integrity ensures that information is accurate and complete and that it has not been tampered with. Techniques include hashing, digital signatures, checksums, and access controls and regular audits.

تضمن النزاهة أن المعلومات دقيقة وكاملة ولم يتم العبث بها تشمل التقنيات المستخدمة التجزئة التوقيعات الرقمية مجموع التحقق الدوري وضوابط الوصول والتدقيقات المنتظمة

• **Hashing:** Algorithms like SHA-256 and SHA-3 create a fixed-size hash value from input data, ensuring data has not been altered. If even a single bit changes, the hash value will be different.

التجزئة تستخدم الخوارزميات لإنشاء قيمة تجزئة ذات حجم ثابت من البيانات المدخلة مما يضمن عدم تغيير البيانات إذا تغيرت حتى بت واحد ستكون قيمة التجزئة مختلفة

• **Digital Signatures:** These use asymmetric cryptography to provide assurance about the origin and integrity of a message or document. They are commonly used in emails and software distribution.

التوقيعات الرقمية: تستخدم هذه التشفير غير المتماثل لتوفير ضمانات حول أصل وسلامة الرسالة أو الوثيقة تستخدم عادة في البريد الإلكتروني وتوزيع البرمجيات

• **Checksums and Cyclic Redundancy Checks (CRCs):** Simple error-detecting codes like CRCs ensure data integrity during storage and transmission by comparing the stored checksum with a newly calculated one.

مجموع التحقق الدوري : أكواد بسيطة للكشف عن الأخطاء مثل تضمن سلامة البيانات أثناء التخزين والنقل من خلال مقارنة مجموع التحقق المخزن بواحد محسوب حديثًا

• **Access Controls and Audits:** Regular audits and strict access controls help in monitoring and ensuring the integrity of critical data.

ضوابط الوصول والتدقيقات: تساعد التدقيقات المنتظمة وضوابط الوصول الصارمة في مراقبة وضمان سلامة البيانات الحيوية

-Example: Using SHA-256 to generate a hash value for software files ensures they have not been tampered with during transfer.

استخدام الهاش لإنشاء قيمة تجزئة لملفات البرامج يضمن عدم العبث بها أثناء النقل

-Example: Signing email messages with a digital signature verifies the sender's identity and ensures the content has not been altered.

توقيع رسائل البريد الإلكتروني بتوقيع رقمي يتحقق من هوية المرسل ويضمن عدم تغيير المحتوى

-Example: Employing CRC checks to verify the integrity of files downloaded from the internet. Implementing access logs and conducting regular audits detect unauthorized changes to critical files.

استخدام فحوصات للتحقق من سلامة الملفات التي تم تنزيلها من الإنترنت. تنفيذ سجلات الوصول وإجراء التدقيقات المنتظمة للكشف عن التغييرات غير المصرح بها في الملفات الحيوية

• Availability التوافر

Availability ensures that information and resources are accessible to authorized users when needed. This is achieved through redundancy, failover mechanisms, and DoS mitigation strategies, with regular testing and updates of disaster recovery plans.

يضمن التوافر أن تكون المعلومات والموارد متاحة للمستخدمين المصرح لهم عند الحاجة يتم تحقيق ذلك من خلال التكرار آليات التحويل الفوري واستراتيجيات تخفيف هجمات الحرمان من الخدمة مع إجراء اختبارات وتحديثات منتظمة لخطط التعافي من الكوارث

• ***Redundancy:*** Techniques like RAID, load balancing, and redundant power supplies ensure continuous availability of data and services even in case of hardware failures.

التكرار : تقنيات مثل توزيع الأحمال ومصادر الطاقة الاحتياطية تضمن توفر البيانات والخدمات بشكل مستمر حتى في حالة فشل الأجهزة

• ***Disaster Recovery Plans (DRP):*** These plans include strategies for data backup, recovery, and maintaining critical functions during and after a disaster.

خطط التعافي من الكوارث : تتضمن هذه الخطط استراتيجيات لنسخ البيانات احتياطيًا واستعادتها والحفاظ على الوظائف الحيوية خلال وبعد الكارثة

• ***Failover Mechanisms:*** Systems like hot, warm, and cold sites, as well as automated

failover solutions, ensure operations continue without significant interruption.

آليات التحويل الفوري: تضمن أنظمة مثل المواقع الساخنة والدافئة والباردة بالإضافة إلى الحلول التلقائية للتحويل الفوري استمرار العمليات دون انقطاع كبير

• ***Denial-of-Service (DoS) Mitigation:*** Strategies include using firewalls, intrusion prevention systems (IPS), and traffic analysis tools to detect and mitigate DoS attacks.

تخفيف هجمات الحرمان من الخدمة : تشمل الاستراتيجيات استخدام الجدران النارية أنظمة منع التطفل وأدوات تحليل حركة المرور للكشف عن هجمات وتخفيفها

-Example: Using RAID 5 for data storage ensures data availability even if one disk fails.

استخدام لتخزين البيانات يضمن توفر البيانات حتى في حالة فشل قرص واحد

-Example: Developing detailed disaster recovery plans to restore systems and data after a disruption. For example, a company may set up a warm site to quickly switch operations in case of a major disaster.

تطوير خطط مفصلة للتعافي من الكوارث لاستعادة الأنظمة والبيانات بعد الاضطراب. على سبيل المثال قد تقوم الشركة بإنشاء موقع دافئ للتبديل السريع للعمليات في حالة حدوث كارثة كبيرة

Multiple Choice Questions:

1. What is the primary goal of the CIA Triad in information security?

A. To increase the complexity of the security system

B. To ensure information confidentiality, integrity, and availability

C. To promote the use of advanced cryptographic techniques

D. To facilitate regulatory compliance

2. Which of the following ensures that sensitive information is accessed only by authorized individuals?

A. Integrity

B. Availability

C. Confidentiality

D. Non-repudiation

3. What technique involves creating a fixed-size hash value from input data to ensure data integrity?

A. Encryption

B. Digital Signatures

C. Hashing

D. Access Control

4. What principle ensures that users are granted the minimum level of access necessary to perform their job functions?

A. Need-to-Know

B. Separation of Duties

C. Least Privilege

D. Dual Control

5. What is a common strategy to ensure availability of data in case of hardware failure?

A. Encryption

B. RAID

C. Hashing

D. Digital Signatures

Answers and Explanations:

1. Answer: B. To ensure information confidentiality, integrity, and availability

Explanation: The CIA Triad is fundamental in information security to ensure information is protected in terms of confidentiality, integrity, and availability.

أساسياً في أمن المعلومات لضمان حماية المعلومات (CIA) يعد مثلث السرية والنزاهة والتوافر
من حيث السرية والنزاهة والتوافر

2. Answer: C. Confidentiality

Explanation: Confidentiality ensures that sensitive information is accessed only by authorized individuals, protecting it from unauthorized access.

تضمن السرية أن المعلومات الحساسة لا يمكن الوصول إليها إلا من قبل الأفراد المصرح لهم،
مما يحميها من الوصول غير المصرح به

3. Answer: C. Hashing

Explanation: Hashing creates a fixed-size hash value from input data, ensuring data integrity by making it easy to detect alterations.

تنشئ التجزئة قيمة تجزئة بحجم ثابت من البيانات المدخلة، مما يضمن سلامة البيانات من خلال
تسهيل اكتشاف التعديلات

4. Answer: C. Least Privilege

Explanation: The principle of least privilege ensures users are granted the minimum level of access necessary to perform their job functions, reducing the risk of unauthorized access.

يضمن مبدأ الحد الأدنى من الامتياز أن يحصل المستخدمون على أقل مستوى من الوصول
اللازم لأداء وظائفهم الوظيفية، مما يقلل من خطر الوصول غير المصرح به

5. Answer: B. RAID

Explanation: RAID (Redundant Array of Independent Disks) is a common strategy used to ensure data availability in case of hardware failure.

استراتيجية شائعة لضمان توفر البيانات في (مجموعة متكررة من الأقراص المستقلة) RAID يعد
حالة فشل الأجهزة

Graph 2: Business Objectives

2. Governance and Policy الحوكمة والسياسة

• **Security Policies سياسات الأمن**

• **Security policies** are high-level management directives that define the approach to managing information security. This includes policies like information security, acceptable use, and data privacy policies.

سياسات الأمن هي توجيهات إدارية على مستوى عالٍ تحدد النهج لإدارة أمن المعلومات وتشمل سياسات مثل أمن المعلومات الاستخدام المقبول وسياسات خصوصية البيانات

• **High-Level Management Directives:** These policies provide the strategic direction for all security efforts in the organization. Examples include Information Security Policy, Acceptable Use Policy, and Data Privacy Policy.

التوجيهات الإدارية عالية المستوى توفر هذه السياسات التوجيه الاستراتيجي لجميع جهود الأمن في المنظمة تشمل الأمثلة سياسة أمن المعلومات سياسة الاستخدام المقبول وسياسة خصوصية البيانات

• **Policy Lifecycle:** This involves the creation, approval, implementation, monitoring, and updating of security policies.

دورة حياة السياسة يشمل ذلك إنشاء السياسات الموافقة عليها تنفيذها مراقبتها وتحديثها

1.Creation: Drafting policies based on organizational needs, regulatory requirements, and industry best practices.

إنشاء صياغة السياسات بناءً على احتياجات المنظمة المتطلبات التنظيمية وأفضل الممارسات في الصناعة

2.Approval: Obtaining management approval to ensure alignment with organizational goals.

الموافقة الحصول على موافقة الإدارة

3.Implementation: Communicating policies to all employees and providing necessary training.

التنفيذ توصيل السياسات لجميع الموظفين وتوفير التدريب اللازم

4.Monitoring: Regularly reviewing policies to ensure they are being followed and are effective.

المراقبة مراجعة السياسات بانتظام لضمان اتباعها وفعاليتها

5.Updating: Revising policies as necessary to address new threats and changing business needs.

التحديث تعديل السياسات حسب الضرورة لمواجهة التهديدات الجديدة واحتياجات العمل المتغيرة

-Example: Developing an Information Security Policy that outlines the organization's approach to managing and protecting information assets.

تطوير سياسة أمن المعلومات التي تحدد نهج المنظمة في إدارة وحماية أصول المعلومات

-Example: Implementing an Acceptable Use Policy that specifies acceptable and unacceptable behaviors when using company IT resources.

تنفيذ سياسة الاستخدام المقبول التي تحدد السلوكيات المقبولة وغير المقبولة عند استخدام موارد تكنولوجيا المعلومات للشركة

-Example: Creating a Data Privacy Policy that details how personal data will be collected, used, and protected.

إنشاء سياسة خصوصية البيانات التي تفصل كيفية جمع البيانات الشخصية واستخدامها وحمايتها

• **Security Standards, Guidelines, and Procedures المعايير الأمنية والإرشادات والإجراءات**

Standards, guidelines, and procedures support security policies by providing detailed instructions and best practices for implementing security controls.

تدعم المعايير والإرشادات والإجراءات الأمنية السياسات الأمنية من خلال توفير تعليمات مفصلة وأفضل الممارسات لتطبيق ضوابط الأمان

• **Standards:** Mandatory requirements for implementing security controls. Examples include password complexity standards and encryption standards.

المعايير المتطلبات الإلزامية لتطبيق ضوابط الأمان تشمل الأمثلة معايير تعقيد كلمات المرور ومعايير التشفير

• **Guidelines:** Recommended best practices for achieving security objectives. Examples include guidelines for secure software development and data handling.

الإرشادات أفضل الممارسات الموصى بها لتحقيق أهداف الأمان تشمل الأمثلة إرشادات لتطوير البرمجيات الآمن والتعامل مع البيانات

• **Procedures:** Step-by-step instructions for carrying out specific security tasks.

Examples include incident response procedures and backup procedures.

الإجراءات تعليمات خطوة بخطوة لتنفيذ مهام الأمان المحددة تشمل الأمثلة إجراءات الاستجابة للحوادث وإجراءات النسخ الاحتياطي

-Example: Implementing a password complexity standard that requires passwords to be at least eight characters long and include a mix of letters, numbers, and special characters.

تنفيذ معيار تعقيد كلمة المرور الذي يتطلب أن تكون كلمات المرور مكونة من ثمانية أحرف على الأقل وتتضمن مزيجًا من الأحرف والأرقام والرموز الخاصة

-Example: Developing guidelines for secure software development that recommend practices such as code reviews and security testing.

تطوير إرشادات لتطوير البرمجيات الآمن توصي بممارسات مثل مراجعات الشفرات واختبار الأمان

-Example: Creating incident response procedures that outline the steps to take in the event of a security breach.

إنشاء إجراءات الاستجابة للحوادث التي تحدد الخطوات التي يجب اتخاذها في حالة حدوث اختراق أمني

Multiple Choice Questions:

1. What is the primary purpose of security policies within an organization?

A. To increase the complexity of the security system

B. To define the approach to managing information security

C. To promote the use of advanced cryptographic techniques

D. To facilitate regulatory compliance

2. Which of the following is a high-level management directive that provides strategic direction for security efforts in the organization?

A. Procedure

B. Guideline

C. Standard

D. Policy

3. What does the policy lifecycle involve?

A. Creation, approval, implementation, monitoring, and updating of security policies

B. Developing new encryption methods

C. Ensuring high availability of information systems

D. Conducting regular security audits

4. Which of the following provides step-by-step instructions for carrying out specific security tasks?

A. Standard

B. Policy

C. Procedure

D. Guideline

5. What is the purpose of security standards within an organization?

A. To provide mandatory requirements for implementing security controls

B. To recommend best practices for achieving security objectives

C. To establish high-level management directives

D. To ensure the use of advanced cryptographic techniques

Answers and Explanations:

1. Answer: B. To define the approach to managing information security

Explanation: The primary purpose of security policies is to define the approach to managing information security within an organization.

الهدف الرئيسي من السياسات الأمنية هو تحديد النهج لإدارة أمن المعلومات داخل المنظمة

2. Answer: D. Policy

Explanation: A policy is a high-level management directive that provides strategic

direction for security efforts in the organization.

السياسة هي توجيه إداري على مستوى عالٍ يوفر التوجيه الاستراتيجي لجهود الأمن في المنظمة

3. Answer: A. Creation, approval, implementation, monitoring, and updating of security policies

Explanation: The policy lifecycle involves the creation, approval, implementation, monitoring, and updating of security policies to ensure they remain effective and relevant.

تتضمن دورة حياة السياسة إنشاء السياسات والموافقة عليها وتنفيذها ومراقبتها وتحديثها لضمان بقائها فعالة وذات صلة

4. Answer: C. Procedure

Explanation: A procedure provides step-by-step instructions for carrying out specific security tasks within an organization.

الإجراء يقدم تعليمات خطوة بخطوة لتنفيذ مهام الأمان المحددة داخل المنظمة

5. Answer: A. To provide mandatory requirements for implementing security controls

Explanation: Security standards provide mandatory requirements for implementing security controls to ensure consistent and effective security practices.

توفر المعايير الأمنية متطلبات إلزامية لتطبيق ضوابط الأمان لضمان ممارسات أمنية متسقة وفعالة

Graph 3: Risk Assessment Matrix

3. Risk Management إدارة المخاطر

• Risk Identification تحديد المخاطر

Risk identification involves determining the potential threats that could negatively affect the organization’s information assets. This includes identifying both internal

and external threats.

تحديد المخاطر يشمل تحديد التهديدات المحتملة التي يمكن أن تؤثر سلبًا على أصول معلومات المنظمة ويتضمن ذلك تحديد التهديدات الداخلية والخارجية

• **Internal Threats:** These originate from within the organization and can include employee misconduct, insider threats, and system failures.

التهديدات الداخلية تنشأ هذه من داخل المنظمة ويمكن أن تشمل سوء سلوك الموظفين والتهديدات الداخلية وفشل النظام

• **External Threats:** These originate from outside the organization and can include cyber attacks, natural disasters, and supply chain disruptions.

التهديدات الخارجية تنشأ هذه من خارج المنظمة ويمكن أن تشمل الهجمات الإلكترونية والكوارث الطبيعية واضطرابات سلسلة التوريد

-Example:Identifying potential threats such as phishing attacks targeting employees.

تحديد التهديدات المحتملة مثل هجمات التصيد الاحتيالي التي تستهدف الموظفين

-Example: Recognizing natural disasters like earthquakes as external threats that could disrupt business operations.

التعرف على الكوارث الطبيعية مثل الزلازل كتهديدات خارجية يمكن أن تعطل عمليات الأعمال

• Risk Assessment تقييم المخاطر

Risk assessment involves evaluating the identified risks to understand their potential impact and likelihood. This includes qualitative and quantitative risk assessments.

يشمل تقييم المخاطر تقييم المخاطر المحددة لفهم تأثيرها المحتمل واحتمال حدوثها ويتضمن ذلك تقييمات المخاطر النوعية والكمية

• **Qualitative Risk Assessment:** This method uses descriptive categories to assess risks, such as high, medium, and low.

تقييم المخاطر النوعي يستخدم هذا الأسلوب فئات وصفية لتقييم المخاطر مثل عالي متوسط ومنخفض

• **Quantitative Risk Assessment:** This method uses numerical values and statistical models to assess risks, often involving calculations like Annual Loss Expectancy (ALE).

تقييم المخاطر الكمي يستخدم هذا الأسلوب القيم العددية والنماذج الإحصائية لتقييم المخاطر وغالبًا ما يتضمن حسابات مثل التوقع السنوي للخسارة (ALE)

***Annual Loss Expectancy (ALE):** A calculation used in quantitative risk assessment to estimate the annual financial loss from a specific risk.

التوقع السنوي للخسارة : حساب يستخدم في تقييم المخاطر الكمي لتقدير الخسارة المالية السنوية من خطر محدد

$$ALE = SLE \times ARO$$

SLE : (Single Loss Expectancy) - الخسارة الفردية المتوقعة

ARO: (Annual Rate of Occurrence) - معدل حدوث الخطر السنوي

-Example Calculation: Suppose the SLE (Single Loss Expectancy) for a potential data breach is $100,000, and the ARO (Annual Rate of Occurrence) is 2. The ALE (Annual Loss Expectancy) can be calculated as follows:

$ALE = SLE \times ARO$ALE=SLE×ARO

ALE=100,000×2=200,000ALE=100,000×2=200,000

• This means the estimated annual financial loss from the data breach risk is $200,000.

هذا يعني أن الخسارة المالية السنوية المقدرة من خطر خرق البيانات هي 200,000 دولار

-Example: Performing a qualitative risk assessment to categorize identified risks based on their potential impact on the organization.

إجراء تقييم المخاطر النوعي لتصنيف المخاطر المحددة بناءً على تأثيرها المحتمل على المنظمة

-Example: Using the ALE formula to estimate the financial impact of a data breach, where SLE is $100,000 and ARO is 2, resulting in an ALE of $200,000.

استخدام صيغة ALE لتقدير التأثير المالي لخرق البيانات حيث تكون SLE هي 100,000 دولار و ARO هي 2 مما ينتج عنه ALE بقيمة 200,000 دولار

• Risk Mitigation تخفيف المخاطر

Risk mitigation involves implementing measures to reduce the impact and likelihood of risks. This includes risk avoidance, risk transference, risk reduction, and risk acceptance.

يشمل تخفيف المخاطر تنفيذ تدابير لتقليل تأثير واحتمال المخاطر ويتضمن ذلك تجنب المخاطر نقل المخاطر تقليل المخاطر وقبول المخاطر

• **Risk Avoidance:** Taking steps to eliminate a risk by not engaging in activities that would incur the risk.

تجنب المخاطر اتخاذ خطوات للقضاء على الخطر عن طريق عدم الانخراط في الأنشطة التي قد تنطوي على الخطر

• **Risk Transference:** Shifting the risk to a third party, such as through insurance or outsourcing.

نقل المخاطر تحويل الخطر إلى طرف ثالث مثل التأمين أو الاستعانة بمصادر خارجية

• **Risk Reduction:** Implementing controls to minimize the impact or likelihood of the risk.

تقليل المخاطر تنفيذ الضوابط لتقليل تأثير أو احتمال الخطر

• **Risk Acceptance:** Acknowledging the risk and choosing to accept it without taking any specific measures to address it.

قبول المخاطر الاعتراف بالخطر واختيار قبوله دون اتخاذ أي تدابير محددة لمعالجته

-Example: Implementing a firewall and antivirus software to reduce the risk of cyber attacks.

تنفيذ جدار ناري وبرمجيات مكافحة الفيروسات لتقليل خطر الهجمات الإلكترونية

-Example: Purchasing cyber insurance to transfer the financial risk associated with data breaches to an insurance company.

شراء التأمين السيبراني لنقل الخطر المالي المرتبط بخرق البيانات إلى شركة التأمين

-Example: Deciding to accept the risk of minor software bugs that do not significantly affect operations.

اتخاذ قرار بقبول خطر الأخطاء البرمجية البسيطة التي لا تؤثر بشكل كبير على العمليات

Multiple Choice Questions:

1. What is the primary purpose of risk identification within an organization?

A. To develop new security technologies

B. To determine potential threats that could negatively affect information assets

C. To ensure compliance with regulations

D. To enhance user experience

2. Which of the following is an internal threat?

A. Phishing attacks

B. Natural disasters

C. Insider threats

D. Supply chain disruptions

3. What method uses descriptive categories to assess risks?

A. Quantitative Risk Assessment

B. Annual Loss Expectancy (ALE)

C. Qualitative Risk Assessment

D. Risk Transference

4. What calculation is used in quantitative risk assessment to estimate the annual financial loss from a specific risk?

A. SLE

B. ARO

C. ALE

D. ROI

5. What is an example of risk transference?

A. Implementing a firewall

B. Purchasing insurance

C. Accepting minor software bugs

D. Avoiding risky activities

Answers and Explanations:

1. Answer: B. To determine potential threats that could negatively affect information assets

Explanation: The primary purpose of risk identification is to determine potential threats that could negatively affect the organization's information assets.

الهدف الرئيسي من تحديد المخاطر هو تحديد التهديدات المحتملة التي يمكن أن تؤثر سلبًا على أصول معلومات المنظمة

2. Answer: C. Insider threats

Explanation: Insider threats are internal threats originating from within the organization, such as employee misconduct or system failures.

التهديدات الداخلية هي تهديدات داخلية تنشأ من داخل المنظمة مثل سوء سلوك الموظفين أو فشل النظام

3. Answer: C. Qualitative Risk Assessment

Explanation: Qualitative risk assessment uses descriptive categories like high, medium, and low to assess risks.

يستخدم تقييم المخاطر النوعي فئات وصفية مثل عالي متوسط ومنخفض لتقييم المخاطر

4. Answer: C. ALE

Explanation: ALE (Annual Loss Expectancy) is a calculation used in quantitative risk assessment to estimate the annual financial loss from a specific risk.

هو حساب يستخدم في تقييم المخاطر الكمي لتقدير الخسارة (ALE) التوقع السنوي للخسارة المالية السنوية من خطر محدد

5. Answer: B. Purchasing insurance

Explanation: Risk transference involves shifting the risk to a third party, such as through purchasing insurance.

يتضمن نقل المخاطر تحويل الخطر إلى طرف ثالث مثل شراء التأمين

Graph 4: Compliance

4. Legal and Regulatory Compliance الامتثال القانوني والتنظيمي

• Data Protection Laws قوانين حماية البيانات

Organizations must comply with various data protection laws and regulations to protect personal and sensitive information. Examples include the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

يجب على المنظمات الامتثال لمختلف قوانين ولوائح حماية البيانات لحماية المعلومات الشخصية والحساسة تشمل الأمثلة اللائحة العامة لحماية البيانات (GDPR) وقانون خصوصية المستهلك في كاليفورنيا (CCPA)

• **GDPR:** A comprehensive data protection law in the European Union that sets guidelines for the collection, processing, and storage of personal data.

اللائحة العامة لحماية البيانات قانون شامل لحماية البيانات في الاتحاد الأوروبي يحدد إرشادات لجمع ومعالجة وتخزين البيانات الشخصية

• **CCPA:** A state statute intended to enhance privacy rights and consumer protection for residents of California, USA.

قانون خصوصية المستهلك في كاليفورنيا قانون حكومي يهدف إلى تعزيز حقوق الخصوصية وحماية المستهلكين لسكان كاليفورنيا بالولايات المتحدة الأمريكية

-Example: Ensuring that the organization complies with GDPR by implementing appropriate data protection measures and conducting regular data protection impact assessments (DPIAs).

من خلال تنفيذ تدابير حماية (GDPR) ضمان امتثال المنظمة للائحة العامة لحماية البيانات البيانات المناسبة وإجراء تقييمات تأثير حماية البيانات بانتظام (DPIAs)

-Example: Updating privacy policies to meet the requirements of the CCPA, including providing consumers with the right to access and delete their personal information.

تحديث سياسات الخصوصية لتلبية متطلبات قانون خصوصية المستهلك في كاليفورنيا (CCPA)

بما في ذلك منح المستهلكين الحق في الوصول إلى معلوماتهم الشخصية وحذفها

• Industry Regulations اللوائح الصناعية

Industry-specific regulations ensure that organizations adhere to standards that protect sensitive information. Examples include the Health Insurance Portability and Accountability Act (HIPAA) for healthcare and the Payment Card Industry Data Security Standard (PCI DSS) for payment processing.

تضمن اللوائح الصناعية الخاصة بالصناعة أن تلتزم المنظمات بالمعايير التي تحمي المعلومات الحساسة تشمل الأمثلة قانون نقل التأمين الصحي والمساءلة (HIPAA) ومعيار للرعاية الصحية أمان بيانات صناعة بطاقات الدفع (PCI DSS) لمعالجة الدفع

• HIPAA: A US law designed to provide privacy standards to protect patients' medical records and other health information.

قانون نقل التأمين الصحي والمساءلة قانون أمريكي مصمم لتوفير معايير الخصوصية لحماية السجلات الطبية للمرضى وغيرها من المعلومات الصحية

• PCI DSS: A set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.

معيار أمان بيانات صناعة بطاقات الدفع مجموعة من معايير الأمان المصممة لضمان أن جميع الشركات التي تقبل أو تعالج أو تخزن أو تنقل معلومات بطاقة الائتمان تحافظ على بيئة آمنة

-Example: Implementing HIPAA compliance measures to ensure the confidentiality and security of patients' health information.

لضمان سرية وأمان (HIPAA) تنفيذ تدابير الامتثال لقانون نقل التأمين الصحي والمساءلة المعلومات الصحية للمرضى

-Example: Ensuring compliance with PCI DSS by implementing security measures for credit card data during transactions.

من خلال تنفيذ تدابير (PCI DSS) ضمان الامتثال لمعيار أمان بيانات صناعة بطاقات الدفع الأمان لبيانات بطاقة الائتمان أثناء المعاملات

• International Laws القوانين الدولية

Organizations operating across multiple countries must comply with various international laws and regulations. This includes laws like the General Data Protection Regulation (GDPR) in Europe and the Personal Data Protection Act (PDPA)

in Singapore.

يجب على المنظمات التي تعمل عبر دول متعددة الامتثال لمختلف القوانين واللوائح الدولية في أوروبا وقانون حماية (GDPR) يشمل ذلك القوانين مثل اللائحة العامة لحماية البيانات في سنغافورة (PDPA) البيانات الشخصية

• **GDPR:** A comprehensive data protection law in the European Union that sets guidelines for the collection, processing, and storage of personal data.

اللائحة العامة لحماية البيانات قانون شامل لحماية البيانات في الاتحاد الأوروبي يحدد إرشادات لجمع ومعالجة وتخزين البيانات الشخصية

• **PDPA:** A data protection law in Singapore that governs the collection, use, and disclosure of personal data by organizations.

قانون حماية البيانات الشخصية قانون حماية البيانات في سنغافورة يحكم جمع واستخدام وكشف البيانات الشخصية من قبل المنظمات

-Example: Ensuring compliance with GDPR by implementing appropriate data protection measures and conducting regular data protection impact assessments (DPIAs).

من خلال تنفيذ تدابير حماية البيانات (GDPR) ضمان الامتثال للائحة العامة لحماية البيانات المناسبة وإجراء تقييمات تأثير حماية البيانات بانتظام (DPIAs)

-Example: Complying with PDPA by updating privacy policies to meet its requirements, including obtaining consent from individuals before collecting their personal data.

من خلال تحديث سياسات الخصوصية لتلبية (PDPA) الامتثال لقانون حماية البيانات الشخصية متطلباته بما في ذلك الحصول على موافقة الأفراد قبل جمع بياناتهم الشخصية

Multiple Choice Questions:

1. What is the primary purpose of data protection laws like GDPR?

A. To increase the complexity of data management

B. To ensure the protection of personal and sensitive information

C. To promote the use of advanced encryption methods

D. To facilitate data sharing between organizations

2. Which of the following is an example of an industry-specific regulation?

A. GDPR

B. HIPAA

C. PDPA

D. CCPA

3. What does the GDPR regulate?

A. The use of encryption technologies

B. The collection, processing, and storage of personal data

C. The development of new software applications

D. The creation of security policies

4. Which of the following laws governs the collection, use, and disclosure of personal data in Singapore?

A. GDPR

B. HIPAA

Cyber security qualification review: CRISC (Certified...

Mowen L. · 2 years ago

NIST SP 800-37 Rev. 2

Nick Webb 💥 · 6 years ago

C. PDPA

D. CCPA

5. What is the purpose of PCI DSS?

A. To regulate data protection in the healthcare industry

B. To establish standards for protecting credit card information

C. To provide guidelines for data sharing

D. To enhance privacy rights for California residents

Answers and Explanations:

1. Answer: B. To ensure the protection of personal and sensitive information

Explanation: The primary purpose of data protection laws like GDPR is to ensure the protection of personal and sensitive information.

هو ضمان حماية المعلومات الشخصية (GDPR) الهدف الرئيسي من قوانين حماية البيانات مثل والحساسة

2. Answer: B. HIPAA

Explanation: HIPAA is an industry-specific regulation designed to provide privacy standards to protect patients' medical records and other health information.

يعد قانون نقل التأمين الصحي والمساءلة (HIPAA) لائحة صناعية خاصة بالصناعة مصمم لتوفير معايير الخصوصية لحماية السجلات الطبية للمرضى وغيرها من المعلومات الصحية

3. Answer: B. The collection, processing, and storage of personal data

Explanation: GDPR regulates the collection, processing, and storage of personal data to protect individuals' privacy.

تنظم اللائحة العامة لحماية البيانات (GDPR) جمع ومعالجة وتخزين البيانات الشخصية لحماية خصوصية الأفراد

4. Answer: C. PDPA

Explanation: The Personal Data Protection Act (PDPA) governs the collection, use, and disclosure of personal data in Singapore.

يحكم قانون حماية البيانات الشخصية (PDPA) جمع واستخدام وكشف البيانات الشخصية في سنغافورة

5. Answer: B. To establish standards for protecting credit card information

Explanation: PCI DSS is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.

هو مجموعة من معايير الأمان المصممة (PCI DSS) معيار أمان بيانات صناعة بطاقات الدفع لضمان أن جميع الشركات التي تقبل أو تعالج أو تخزن أو تنقل معلومات بطاقة الائتمان تحافظ على بيئة آمنة

Graph 5 : $(ISC)^2$ Code of Ethics

5. Professional Ethics الأخلاقيات المهنية

• Code of Ethics مدونة الأخلاقيات

The $(ISC)^2$ Code of Ethics provides guidelines for ethical behavior in the field of

information security. It emphasizes the importance of integrity, honesty, and responsibility.

إرشادات للسلوك الأخلاقي في مجال أمن المعلومات وتشدد على (ISC)² توفر مدونة أخلاقيات أهمية النزاهة والأمانة والمسؤولية

• **Protect Society:** Ensure that actions benefit the public good and do not harm others.

حماية المجتمع ضمان أن الأعمال تفيد الصالح العام ولا تضر الآخرين

• **Act Honorably:** Conduct oneself with honesty and integrity in all professional dealings.

التصرف بشرف التصرف بنزاهة وأمانة في جميع التعاملات المهنية

• **Act Fairly:** Treat all individuals and groups with fairness and respect.

التصرف بعدالة معاملة جميع الأفراد والمجموعات بالعدل والاحترام

• **Act Responsibly:** Accept responsibility for one's actions and their consequences.

التصرف بمسؤولية قبول المسؤولية عن الأعمال وعواقبها

• **Act Diligently:** Perform duties with diligence and competence.

التصرف بجدية أداء الواجبات بجدية وكفاءة

-Example: Reporting a security breach to the relevant authorities to protect society and uphold ethical standards.

الإبلاغ عن اختراق أمني للسلطات المعنية لحماية المجتمع والحفاظ على المعايير الأخلاقية

-Example: Treating all clients and colleagues with fairness and respect, regardless of their background or status.

معاملة جميع العملاء والزملاء بالعدل والاحترام بغض النظر عن خلفيتهم أو وضعهم

• Importance of Ethics in Information Security أهمية الأخلاقيات في أمن المعلومات

Upholding ethical standards is crucial in maintaining trust and credibility in the field of information security. It helps professionals navigate complex situations and make decisions that align with moral and legal standards.

الحفاظ على المعايير الأخلاقية أمر بالغ الأهمية في الحفاظ على الثقة والمصداقية في مجال

أمن المعلومات ويساعد المهنيين على التنقل في المواقف المعقدة واتخاذ قرارات تتماشى مع المعايير الأخلاقية والقانونية

-Example: Making an ethical decision to disclose a vulnerability to a software vendor rather than exploiting it for personal gain.

اتخاذ قرار أخلاقي بالكشف عن نقطة ضعف لبائع البرمجيات بدلاً من استغلالها لتحقيق مكاسب شخصية

-Example: Upholding confidentiality agreements and not disclosing sensitive information about clients or projects.

الالتزام باتفاقيات السرية وعدم الكشف عن معلومات حساسة حول العملاء أو المشاريع

Multiple Choice Questions:

1. What is one of the key principles of the (ISC)² Code of Ethics?

A. Maximize personal gain

B. Act honorably

C. Focus on profit

D. Avoid responsibility

2. Which of the following best describes "Act Diligently" in the (ISC)² Code of Ethics?

A. Ensure actions benefit the public good

B. Conduct oneself with honesty

C. Perform duties with diligence and competence

D. Treat all individuals with fairness

3. Why is upholding ethical standards important in information security?

A. To increase profits

B. To maintain trust and credibility

C. To exploit vulnerabilities

D. To reduce workload

4. What does "Act Fairly" entail according to the (ISC)² Code of Ethics?

A. Performing duties competently

B. Treating all individuals and groups with fairness and respect

C. Ensuring the public good

D. Avoiding responsibility for actions

5. What should an information security professional do if they discover a vulnerability in a client's system?

A. Exploit it for personal gain

B. Ignore it to avoid extra work

C. Report it to the relevant authorities

D. Sell the information to a competitor

Answers and Explanations:

1. Answer: B. Act honorably

Explanation: One of the key principles of the (ISC)² Code of Ethics is to act honorably, conducting oneself with honesty and integrity in all professional dealings.

أحد المبادئ الرئيسية في مدونة أخلاقيات (ISC)² هو التصرف بشرف والتصرف بنزاهة وأمانة في جميع التعاملات المهنية

2. Answer: C. Perform duties with diligence and competence

Explanation: "Act Diligently" means to perform duties with diligence and competence, ensuring that tasks are completed to the best of one's ability.

تعني التصرف بجدية أداء الواجبات بجدية وكفاءة وضمان إنجاز المهام بأفضل قدرات الشخص

3. Answer: B. To maintain trust and credibility

Explanation: Upholding ethical standards is important in information security to maintain trust and credibility, helping professionals navigate complex situations and

make morally and legally aligned decisions.

الحفاظ على المعايير الأخلاقية أمر مهم في أمن المعلومات للحفاظ على الثقة والمصداقية ويساعد المهنيين على التنقل في المواقف المعقدة واتخاذ قرارات تتماشى مع المعايير الأخلاقية والقانونية

4. Answer: B. Treating all individuals and groups with fairness and respect

Explanation: "Act Fairly" in the $(ISC)^2$ Code of Ethics entails treating all individuals and groups with fairness and respect, regardless of their background or status.

يتضمن التصرف بعدالة في مدونة أخلاقيات $(ISC)^2$ معاملة جميع الأفراد والمجموعات بالعدل والاحترام بغض النظر عن خلفيتهم أو وضعهم

5. Answer: C. Report it to the relevant authorities

Explanation: An information security professional should report a vulnerability in a client's system to the relevant authorities to protect society and uphold ethical standards.

يجب على محترف أمن المعلومات الإبلاغ عن نقطة ضعف في نظام العميل للسلطات المعنية لحماية المجتمع والحفاظ على المعايير الأخلاقية

Graph 6: Security Governance

6. Security Governance حوكمة الأمن

• Security Governance Framework إطار حوكمة الأمن

Security governance involves establishing and maintaining a framework to guide the organization’s security efforts. This includes defining roles, responsibilities, and processes for managing security.

تتضمن حوكمة الأمن إنشاء والحفاظ على إطار عمل لتوجيه جهود الأمان في المنظمة يشمل ذلك تحديد الأدوار والمسؤوليات والعمليات لإدارة الأمان

• **Roles and Responsibilities:** Clearly defining who is responsible for various aspects of security within the organization.

الأدوار والمسؤوليات تحديد بوضوح من هو المسؤول عن الجوانب المختلفة للأمان داخل المنظمة

• **Security Policies and Procedures:** Developing policies and procedures that provide guidelines for security practices and incident response.

السياسات والإجراءات الأمنية تطوير سياسات وإجراءات توفر إرشادات للممارسات الأمنية والاستجابة للحوادث

• **Risk Management:** Implementing processes to identify, assess, and mitigate risks to the organization's information assets.

إدارة المخاطر تنفيذ عمليات لتحديد وتقييم وتخفيف المخاطر على أصول معلومات المنظمة

• **Compliance:** Ensuring that the organization adheres to relevant laws, regulations, and standards.

الامتثال ضمان التزام المنظمة بالقوانين واللوائح والمعايير ذات الصلة

-Example: Assigning specific security responsibilities to different roles within the organization, such as a Chief Information Security Officer (CISO) overseeing the overall security program.

تعيين مسؤوليات أمان محددة لأدوار مختلفة داخل المنظمة مثل كبير موظفي أمن المعلومات (CISO) للإشراف على برنامج الأمان العام

-Example: Developing a comprehensive incident response plan that outlines the steps to be taken in the event of a security breach.

تطوير خطة استجابة شاملة للحوادث التي تحدد الخطوات التي يجب اتخاذها في حالة حدوث اختراق أمني

• Alignment with Business Objectives التوافق مع أهداف العمل

Security governance should align with the organization's business objectives to ensure that security efforts support overall business goals. This involves integrating security into business processes and decision-making.

يجب أن تتماشى حوكمة الأمن مع أهداف العمل في المنظمة لضمان أن تدعم جهود الأمان الأهداف العامة للأعمال يشمل ذلك دمج الأمان في عمليات الأعمال واتخاذ القرارات

• **Integration into Business Processes:** Ensuring that security is considered in all business processes, from strategic planning to day-to-day operations.

الدمج في عمليات الأعمال ضمان مراعاة الأمان في جميع عمليات الأعمال من التخطيط الاستراتيجي إلى العمليات اليومية

• **Support for Business Goals:** Aligning security initiatives with business goals, such as protecting customer data to build trust and enhance the company's reputation.

دعم أهداف الأعمال مواءمة المبادرات الأمنية مع أهداف الأعمال مثل حماية بيانات العملاء لبناء الثقة وتعزيز سمعة الشركة

-Example: Integrating security requirements into the product development lifecycle to ensure new products meet security standards and protect customer data.

دمج متطلبات الأمان في دورة حياة تطوير المنتج لضمان أن المنتجات الجديدة تفي بمعايير الأمان وتحمي بيانات العملاء

-Example: Aligning a security awareness program with business goals by educating employees on the importance of protecting sensitive information and how it supports the organization's reputation.

مواءمة برنامج الوعي الأمني مع أهداف الأعمال من خلال تثقيف الموظفين حول أهمية حماية المعلومات الحساسة وكيف يدعم ذلك سمعة المنظمة

Multiple Choice Questions:

1. What is the primary goal of security governance within an organization?

A. To implement the latest security technologies

B. To align security efforts with business objectives

C. To increase the complexity of the security system

D. To focus solely on regulatory compliance

2. Which of the following best describes a security governance framework?

A. A set of technical controls to protect information systems

B. A comprehensive approach to managing security roles, responsibilities, and processes

C. A list of security tools and technologies

D. A collection of encryption algorithms

3. How can security governance align with business objectives?

A. By integrating security into business processes and decision-making

B. By focusing on implementing advanced cryptographic techniques

C. By outsourcing all security functions

D. By ensuring employees use complex passwords

4. What is one of the key components of a security governance framework?

A. Developing new software applications

B. Defining roles and responsibilities

C. Increasing the budget for security technologies

D. Conducting daily vulnerability scans

5. What is an example of integrating security into business processes?

A. Developing a new encryption algorithm

B. Creating a comprehensive incident response plan

C. Ensuring security is considered in all business processes

D. Training employees to use complex passwords

Answers and Explanations:

1. Answer: B. To align security efforts with business objectives

Explanation: The primary goal of security governance is to align security efforts with business objectives to ensure that security supports the overall goals of the organization.

الهدف الرئيسي لحوكمة الأمن هو مواءمة جهود الأمان مع أهداف الأعمال لضمان أن تدعم الأمان الأهداف العامة للمنظمة

2. Answer: B. A comprehensive approach to managing security roles,

responsibilities, and processes

Explanation: A security governance framework involves a comprehensive approach to managing security roles, responsibilities, and processes within an organization.

يتضمن إطار حوكمة الأمن نهجًا شاملاً لإدارة الأدوار والمسؤوليات والعمليات الأمنية داخل المنظمة

3. Answer: A. By integrating security into business processes and decision-making

Explanation: Security governance can align with business objectives by integrating security into business processes and decision-making.

يمكن لحوكمة الأمن أن تتماشى مع أهداف الأعمال عن طريق دمج الأمان في عمليات الأعمال واتخاذ القرارات

4. Answer: B. Defining roles and responsibilities

Explanation: One of the key components of a security governance framework is defining roles and responsibilities for managing security within the organization.

أحد المكونات الرئيسية لإطار حوكمة الأمن هو تحديد الأدوار والمسؤوليات لإدارة الأمان داخل المنظمة

5. Answer: C. Ensuring security is considered in all business processes

Explanation: Integrating security into business processes means ensuring that security is considered in all business processes, from strategic planning to day-to-day operations.

يعني دمج الأمان في عمليات الأعمال ضمان مراعاة الأمان في جميع عمليات الأعمال من التخطيط الاستراتيجي إلى العمليات اليومية

Graph 7: Threat Modeling

7. Threat Modeling نمذجة التهديدات

• **Threat Identification تحديد التهديدات**

Threat modeling involves identifying potential threats to the organization’s information systems. This includes understanding the sources of threats, such as malicious actors or natural disasters, and the methods they might use to exploit vulnerabilities.

تتضمن نمذجة التهديدات تحديد التهديدات المحتملة لنظم معلومات المنظمة يشمل ذلك فهم مصادر التهديدات مثل الجهات الفاعلة الخبيثة أو الكوارث الطبيعية والطرق التي قد يستخدمونها لاستغلال نقاط الضعف

• **Sources of Threats:** These can include internal sources (e.g., disgruntled employees) and external sources (e.g., hackers, natural disasters).

مصادر التهديدات يمكن أن تشمل المصادر الداخلية (مثل الموظفين الساخطين) والمصادر الخارجية (مثل القراصنة والكوارث الطبيعية)

• **Methods of Exploitation:** These can include phishing, malware, social engineering, and physical attacks.

طرق الاستغلال يمكن أن تشمل التصيد الاحتيالي البرامج الضارة الهندسة الاجتماعية والهجمات المادية

-Example: Identifying phishing attacks as a potential threat from external sources targeting employees.

تحديد هجمات التصيد الاحتيالي كتهديد محتمل من المصادر الخارجية التي تستهدف الموظفين

-Example: Recognizing disgruntled employees as a potential internal threat that could lead to data breaches or sabotage.

التعرف على الموظفين الساخطين كتهديد داخلي محتمل قد يؤدي إلى اختراق البيانات أو التخريب

• Threat Assessment تقييم التهديدات

Threat assessment involves evaluating the identified threats to determine their potential impact on the organization’s information assets. This includes assessing the likelihood and severity of each threat.

يشمل تقييم التهديدات تقييم التهديدات المحددة لتحديد تأثيرها المحتمل على أصول معلومات المنظمة يتضمن ذلك تقييم احتمال وشدة كل تهديد

• **Likelihood:** The probability that a particular threat will occur.

الاحتمالية احتمال حدوث تهديد معين

• **Severity:** The potential impact or damage that the threat could cause if it occurs.

الشدة التأثير المحتمل أو الضرر الذي قد يسببه التهديد إذا حدث

-Example: Assessing the likelihood and severity of phishing attacks to determine their potential impact on the organization.

تقييم احتمال وشدة هجمات التصيد الاحتيالي لتحديد تأثيرها المحتمل على المنظمة

-Example: Evaluating the potential impact of a disgruntled employee leaking sensitive data.

تقييم التأثير المحتمل لتسريب موظف ساخط للبيانات الحساسة

• Threat Mitigation تخفيف التهديدات

Threat mitigation involves implementing measures to reduce the impact and likelihood of identified threats. This includes using technical controls, administrative controls, and physical controls.

يشمل تخفيف التهديدات تنفيذ تدابير لتقليل تأثير واحتمال التهديدات المحددة يتضمن ذلك استخدام الضوابط التقنية الضوابط الإدارية والضوابط المادية

• **Technical Controls:** These include firewalls, intrusion detection systems, and antivirus software.

الضوابط التقنية تشمل هذه الجدران النارية أنظمة الكشف عن التطفل وبرمجيات مكافحة الفيروسات

• **Administrative Controls:** These include policies, procedures, and training programs.

الضوابط الإدارية تشمل هذه السياسات والإجراءات وبرامج التدريب

• **Physical Controls:** These include security guards, locks, and surveillance cameras.

الضوابط المادية تشمل هذه الحراس الأمنيين الأقفال وكاميرات المراقبة

-Example: Implementing email filtering and anti-phishing training to mitigate the threat of phishing attacks.

تنفيذ تصفية البريد الإلكتروني والتدريب على مكافحة التصيد الاحتيالي لتخفيف تهديد هجمات

التصيد الاحتيالي

-Example: Installing surveillance cameras and access controls to mitigate the threat of physical attacks.

تركيب كاميرات المراقبة وضوابط الوصول لتخفيف تهديد الهجمات المادية

Multiple Choice Questions:

1. What is the primary purpose of threat modeling?

A. To develop new security technologies

B. To identify potential threats to information systems

C. To ensure compliance with regulations

D. To enhance user experience

2. Which of the following is an internal source of threats?

A. Hackers

B. Natural disasters

C. Disgruntled employees

D. Malware

3. What does threat assessment involve?

A. Implementing security controls

B. Evaluating the likelihood and severity of identified threats

C. Developing new encryption methods

D. Conducting regular security audits

4. What is an example of a technical control used for threat mitigation?

A. Surveillance cameras

B. Security policies

C. Firewalls

D. Training programs

5. What is the purpose of physical controls in threat mitigation?

A. To increase the complexity of security systems

B. To protect information systems through physical means

C. To develop new software applications

D. To enhance the user experience

Answers and Explanations:

1. Answer: B. To identify potential threats to information systems

Explanation: The primary purpose of threat modeling is to identify potential threats to the organization's information systems.

الهدف الرئيسي من نمذجة التهديدات هو تحديد التهديدات المحتملة لنظم معلومات المنظمة

2. Answer: C. Disgruntled employees

Explanation: Disgruntled employees are an internal source of threats as they originate from within the organization.

الموظفون الساخطون هم مصدر داخلي للتهديدات لأنهم ينشأون من داخل المنظمة

3. Answer: B. Evaluating the likelihood and severity of identified threats

Explanation: Threat assessment involves evaluating the likelihood and severity of identified threats to determine their potential impact.

يشمل تقييم التهديدات تقييم احتمال وشدة التهديدات المحددة لتحديد تأثيرها المحتمل

4. Answer: C. Firewalls

Explanation: Firewalls are an example of a technical control used for threat mitigation.

الجدران النارية هي مثال على الضوابط التقنية المستخدمة لتخفيف التهديدات

5. Answer: B. To protect information systems through physical means

Explanation: Physical controls in threat mitigation protect information systems through physical means, such as security guards and surveillance cameras.

تحمي الضوابط المادية في تخفيف التهديدات نظم المعلومات بوسائل مادية مثل الحراس الأمنيين وكاميرات المراقبة

Graph 8: Threat Scenario

8. Business Continuity and Disaster Recovery Planning تخطيط استمرارية الأعمال والتعافي من الكوارث

• Business Continuity Planning (BCP) تخطيط استمرارية الأعمال

BCP involves developing plans and procedures to ensure that critical business functions can continue during and after a disaster. This includes identifying essential functions, developing recovery strategies, and conducting regular testing and updates.

يشمل تخطيط استمرارية الأعمال تطوير خطط وإجراءات لضمان استمرار الوظائف التجارية الحيوية أثناء وبعد الكارثة يشمل ذلك تحديد الوظائف الأساسية تطوير استراتيجيات التعافي وإجراء اختبارات وتحديثات منتظمة

• **Identifying Essential Functions:** Determining which business functions are critical to the organization’s operations.

تحديد الوظائف الأساسية تحديد الوظائف التجارية التي تعتبر حيوية لعمليات المنظمة

• **Developing Recovery Strategies:** Creating strategies to restore critical functions quickly and efficiently.

تطوير استراتيجيات التعافي إنشاء استراتيجيات لاستعادة الوظائف الحيوية بسرعة وكفاءة

• **Regular Testing and Updates:** Conducting regular tests and updates to ensure the BCP remains effective and relevant.

الاختبارات والتحديثات المنتظمة إجراء اختبارات وتحديثات منتظمة لضمان بقاء تخطيط استمرارية الأعمال فعالًا وذات صلة

-Example: Identifying the organization's payroll function as critical and developing strategies to ensure it can continue in the event of a disaster.

تحديد وظيفة الرواتب في المنظمة كوظيفة حيوية وتطوير استراتيجيات لضمان استمرارها في حالة حدوث كارثة

-Example: Conducting regular disaster recovery drills to test the effectiveness of the BCP and make necessary adjustments.

إجراء تدريبات منتظمة على التعافي من الكوارث لاختبار فعالية تخطيط استمرارية الأعمال وإجراء التعديلات اللازمة

• Disaster Recovery Planning (DRP) تخطيط التعافي من الكوارث

DRP focuses on restoring IT systems and data after a disaster. This includes data backup, recovery procedures, and establishing recovery time objectives (RTO) and recovery point objectives (RPO).

يركز تخطيط التعافي من الكوارث على استعادة نظم وتطبيقات البيانات بعد الكارثة يشمل ذلك النسخ الاحتياطي للبيانات إجراءات الاستعادة وتحديد أهداف وقت الاستعادة وأهداف نقطة الاستعادة

• **Data Backup:** Regularly backing up data to ensure it can be restored after a disaster.

النسخ الاحتياطي للبيانات إجراء نسخ احتياطي منتظم للبيانات لضمان إمكانية استعادتها بعد الكارثة

• **Recovery Procedures:** Developing detailed procedures for restoring IT systems and data.

إجراءات الاستعادة تطوير إجراءات مفصلة لاستعادة نظم وتطبيقات البيانات

• **RTO and RPO:** Establishing RTOs and RPOs to define acceptable downtime and data loss.

أهداف وقت الاستعادة وأهداف نقطة الاستعادة تحديد أهداف وقت الاستعادة وأهداف نقطة الاستعادة لتعريف الوقت المقبول للتوقف وفقدان البيانات

****RTO:*** The maximum acceptable amount of time to restore a function after a disaster.

أهداف وقت الاستعادة الحد الأقصى المقبول من الوقت لاستعادة وظيفة بعد الكارثة

RPO: The maximum acceptable amount of data loss measured in time.

أهداف نقطة الاستعادة الحد الأقصى المقبول لفقدان البيانات مقاسًا بالوقت

-Example Calculation:

Suppose an organization has an RTO of 4 hours for their email system. This means that after a disaster, the email system must be restored within 4 hours to be acceptable.

افترض أن لدى المنظمة أهداف وقت الاستعادة لمدة 4 ساعات لنظام البريد الإلكتروني الخاص بها هذا يعني أنه بعد الكارثة يجب استعادة نظام البريد الإلكتروني في غضون 4 ساعات ليكون مقبولاً

• If the RPO is set to 1 hour, the maximum acceptable data loss for the email system is 1 hour of emails.

إذا تم تعيين أهداف نقطة الاستعادة إلى 1 ساعة فإن الحد الأقصى المقبول لفقدان البيانات لنظام البريد الإلكتروني هو ساعة واحدة من رسائل البريد الإلكتروني

-Example: Implementing a daily data backup schedule to ensure data can be restored to within the last 24 hours.

تنفيذ جدول النسخ الاحتياطي اليومي للبيانات لضمان إمكانية استعادة البيانات في آخر 24 ساعة

-Example: Developing detailed recovery procedures to restore critical IT systems within the established RTO.

تطوير إجراءات استعادة مفصلة لاستعادة نظم تكنولوجيا المعلومات الحيوية في الوقت المحدد

Multiple Choice Questions:

1. What is the primary purpose of Business Continuity Planning (BCP)?

A. To develop new security technologies

B. To ensure critical business functions can continue during and after a disaster

C. To increase profits

D. To enhance user experience

2. What does Disaster Recovery Planning (DRP) focus on?

A. Restoring IT systems and data after a disaster

B. Implementing new business strategies

C. Developing marketing plans

D. Enhancing customer service

3. What is an example of a recovery strategy in BCP?

A. Developing new software applications

B. Creating strategies to restore critical functions quickly

C. Conducting market research

D. Training employees on new technologies

4. What does RTO stand for in disaster recovery planning?

A. Recovery Time Objective

B. Recovery Technology Optimization

C. Risk Treatment Option

D. Remote Teleworking Operation

5. What is the purpose of data backup in DRP?

A. To ensure data can be restored after a disaster

B. To enhance the user experience

C. To increase system complexity

D. To improve customer satisfaction

Answers and Explanations:

1. Answer: B. To ensure critical business functions can continue during and

after a disaster

Explanation: The primary purpose of Business Continuity Planning (BCP) is to ensure that critical business functions can continue during and after a disaster.

الهدف الرئيسي من تخطيط استمرارية الأعمال (BCP) هو ضمان استمرار الوظائف التجارية الحيوية أثناء وبعد الكارثة

2. Answer: A. Restoring IT systems and data after a disaster

Explanation: Disaster Recovery Planning (DRP) focuses on restoring IT systems and data after a disaster.

يركز تخطيط التعافي من الكوارث (DRP) على استعادة نظم وتطبيقات البيانات بعد الكارثة

3. Answer: B. Creating strategies to restore critical functions quickly

Explanation: An example of a recovery strategy in BCP is creating strategies to restore critical functions quickly and efficiently.

مثال على استراتيجية الاستعادة في تخطيط استمرارية الأعمال (BCP) هو إنشاء استراتيجيات لاستعادة الوظائف الحيوية بسرعة وكفاءة

4. Answer: A. Recovery Time Objective

Explanation: RTO stands for Recovery Time Objective, which is the maximum acceptable amount of time to restore a function after a disaster.

أهداف وقت الاستعادة (RTO) تعني الحد الأقصى المقبول من الوقت لاستعادة وظيفة بعد الكارثة

5. Answer: A. To ensure data can be restored after a disaster

Explanation: The purpose of data backup in DRP is to ensure that data can be restored after a disaster.

الغرض من النسخ الاحتياطي للبيانات في تخطيط التعافي من الكوارث (DRP) هو ضمان إمكانية استعادة البيانات بعد الكارثة

Conclusion

In conclusion, the Security and Risk Management domain of the CISSP certification is

essential for understanding the foundational principles necessary to protect and manage an organization's information assets. This domain covers a wide range of topics, from the CIA Triad to risk management, legal compliance, and professional ethics. By mastering these concepts, professionals can ensure that their organizations are well-equipped to handle security challenges and maintain the integrity, confidentiality, and availability of their information systems.

في الختام يعد مجال إدارة الأمن والمخاطر من شهادة أساسياً لفهم المبادئ الأساسية اللازمة لحماية وإدارة أصول معلومات المنظمة يغطي هذا المجال مجموعة واسعة من الموضوعات من مثلث إلى إدارة المخاطر الامتثال القانوني والأخلاقيات المهنية من خلال إتقان هذه المفاهيم يمكن للمهنيين ضمان تجهيز منظماتهم بشكل جيد للتعامل مع تحديات الأمن والحفاظ على نزاهة وسرية وتوافر نظم المعلومات الخاصة بهم

CISSP Resources fo Module 1

1- Official (ISC)² CISSP Study Guide

2- CISSP (ISC)² Official Practice Tests

3- CISSP All-in-One Exam Guide by Shon Harris

4- Cybrary – CISSP Training by Kelly Handerhan

https://www.cybrary.it/course/cissp

5- Oreilly – CISSP Training by Sari Greene

https://www.oreilly.com/library/view/cissp-4th-edition/9780135328613/?_gl=1*jwhz1z*_ga*MTgyMDY2NDI5LjE3MTczNzAwMDI.*_ga_092EL089CH*MTcxNzM3MDAwMi4xLjEuMTcxNzM3MDEwNi41OC4wLjA.

6- CISSP bundles by Thor Pedersen

https://thorteaches.com/cissp/

7- CISSP MindMaps YouTube Playlist from Destination Certification

https://www.youtube.com/playlist?list=PLZKdGEfEyJhLd-pJhAD7dNbJyUgpqI4pu

Hamzah Alhaidari 1mo
اليمن إب

Thanks.

Like · Reply

Adham Mohamed Elahwal 2mo
Cloud Transformation - Principle Consulting Architect

Good Luck Brother 🔔

Like · Reply

Mahmoud Kamal Tawfik 2mo
Network and Security Consultant - | CCIE Enterprise #67851 | CCDE v3 Written | HP-ASE Architect v2 | PMP | ITILv4 ...

ربنا يجازيك كل خير يا هندسه 💔

Like · Reply | 1 Reaction

Ahmed Medhat 2mo
Paratrooper 🪂 | Human Centered | LSSMBB® | Lean Manufacturing & Digitalization Leader | Process Excellence Pr...

Shady Zayed

Like · Reply | 1 Reaction

See more comments

To view or add a comment, sign in

More articles by this author

Module 7: Security

Module 6: Security

CISSP Module 5: Identi

Operations / إدارة عمليات...
Aug 5, 2024

Assessment and Testing...
Jul 28, 2024

and Access Manageme
Jul 8, 2024

See all

Insights from the community

Cybersecurity

How do you choose the right ISMS framework for your organization?

IT Consulting

What criteria should you use to measure the effectiveness of a cybersecurity program?

Vulnerability Assessment

How do you benchmark and improve your CVSS performance and maturity?

Cyber Operations

What are some of the tools and frameworks that you use for cyber risk analysis and management?

Information Security

How do you manage security risks in different environments?

Computer Engineering

How can you conduct a penetration test that is consistent with your organization's risk management strategy?

Show more

Others also viewed

Be Ready for ISC2 CAP Exam by Following Simple Tips
Anindita Kumar · 3y

How to do ISO27001 Continual Improvement (Clause 10.1)
Chris Hall · 1y

Congratulations – you now have your ISO27001 certificate. What now?

Chris Hall · 1y

Template and example of ISO27001 Risk and Opportunities to the ISMS (Clause 6.1.1)

Chris Hall · 2y

NIST SP 800-37 Rev. 2

Philip D. S. · 6y

How To Pass CRISC Exam Easily

Ben Pournader · 6y

Show more

Explore topics

Sales

Marketing

Business Administration

HR Management

Content Management

Engineering

Soft Skills

See All

إدارة الأصول
Asset Management

Emad M. Abdelhamid • 2nd
Technical Leader | SME IT Security Design @ Cisco - CX EMEA . ...
View my portfolio

3w • Edited •

ستكمالاً لما بدأناه في المقال السابق سنقوم بشرح الفصل الثاني من شهادة ال CISSP
وهو فصل شيق ويعتبر أسهل فصول الشهادة ويتحدث عن إدارة الأصول (Asset Management)
ويشمل تحديد الأصول وتصنيفها وحمايتها وإدارتها طوال دورة حياتها. يركز هذا الفصل على ضمان حماية الأصول المعلوماتية وإدارتها بشكل كافٍ لدعم أهداف الأمن وإدارة المخاطر في المنظمة

ويحتوي على 9 أجزاء

1. جرد الأصول وإدارتها Asset Inventory and Management
2. تعيين الملكية Assigning Ownership
3. تصنيف الأصول بناءً على القيمة Classifying Assets Based on Value
4. حماية البيانات بناءً على التصنيف Data Protection Based on Classification
5. إدارة دورة حياة البيانات Data Lifecycle Management
6. إتلاف البيانات والتخلص منها Data Destruction and Disposal
7. إدارة الحقوق الرقمية Digital Rights Management (DRM)
8. منع فقدان البيانات Data Loss Prevention (DLP)
9. تقييم الأصول ومراجعتها Asset Assessment and Review

ستحتوي هذه المقالات على
تلخيص مبدئي لمحتويات الفصل، يليه شرح كل جزء من أجزاء الفصل مدعوماً بأمثلة وتوضيحات وتعريفات. في نهاية كل جزء، سيكون هناك خمس أسئلة لاختبار فهم هذا الجزء مع شرح للإجابات قبل الدخول في الجزء التالي، وهكذا حتى انتهاء الفصل بخاتمة لما تم طرحه، يلي ذلك ذكر المصادر التي تم التجميع منها والتي ستكون مناسبة لدراسة المادة العلمية بالتفصيل في المستقبل.

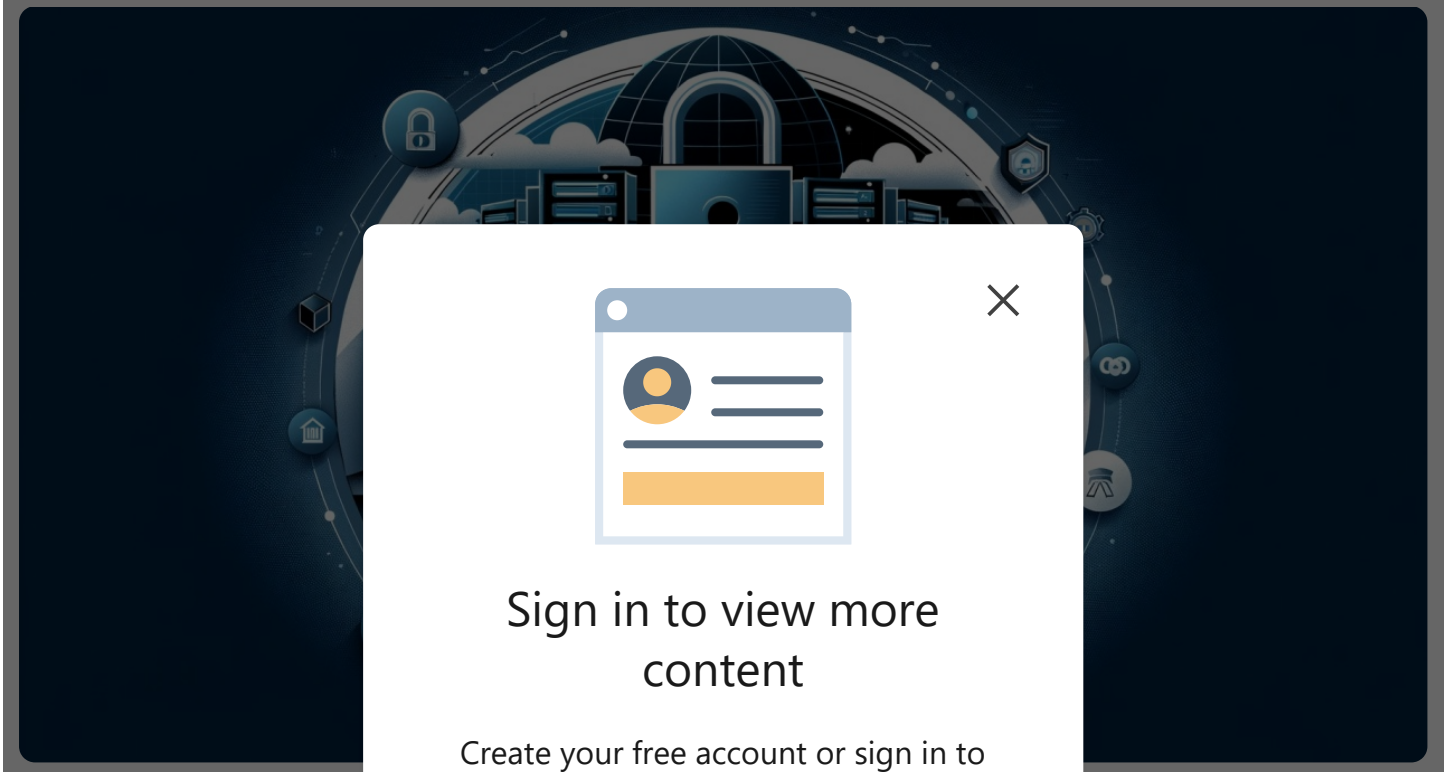
These articles will include:
An initial summary of the chapter's contents, followed by a detailed explanation of each section, supported by examples, clarifications, and definitions. At the end of each section, there will be five questions to test the understanding of that section, along with explanations of the answers before moving on to the next section, and so on until the chapter concludes with a summary of what has been presented. This will be followed by the sources from which the material was gathered, which will be suitable for a detailed study of the subject in the future.

المقالات

For Module 1 : https://lnkd.in/dkkyFGdW
For Module 2 : https://lnkd.in/dNUWhiJs
For Module 3: https://lnkd.in/dsqBXhEc
For Module 4: https://lnkd.in/d_DBAm4h
For Module 5: https://lnkd.in/dGPDeKWF
For Module 6: https://lnkd.in/dZHHJKJx
For Module 7: https://lnkd.in/d_JswW5W
For Module 8: https://lnkd.in/dQsQHqgR

Resources - المصادر

1- Official (ISC)² CISSP Study Guide
2- CISSP (ISC)² Official Practice Tests
3- CISSP All-in-One Exam Guide by Shon Harris
4- Cybrary – CISSP Training by Kelly Handerhan https://lnkd.in/d4zrAkJz
5- Oreilly – CISSP Training by Sari Greene https://lnkd.in/dANS-hVc.
6- CISSP bundles by Thor Pedersen https://lnkd.in/d2tpqaJk
7- CISSP MindMaps YouTube Playlist from Destination Certification https://lnkd.in/deJM44xX



CISSP Mod et Manageme أمر

Emad M. Ab
Technical Lead
CCIE#58413 | ™ |
ISO27001 LA |

Published Jun 10, 2024

Introduction

Asset Security, also known as Asset Management, involves identifying, classifying,

to support the organization's security and risk management objectives.

إدارة الأصول، المعروفة أيضًا بإدارة الأصول الأمنية، تشمل تحديد الأصول وتصنيفها وحمايتها وإدارتها طوال دورة حياتها. يركز هذا المجال على ضمان حماية الأصول المعلوماتية وإدارتها بشكل كافٍ لدعم أهداف الأمن وإدارة المخاطر في المنظمة

Module Brief:

The Asset Security module is divided into several key areas:

يتم تقسيم وحدة إدارة الأصول إلى عدة مجالات رئيسية

1. Asset Inventory and Management جرد الأصول وإدارتها

This involves creating and maintaining a comprehensive list of all information assets within an organization, including hardware, software, and data assets. It ensures that all assets are tracked, maintained, and protected throughout their lifecycle.

يشمل إنشاء وصيانة قائمة شاملة بجميع الأصول المعلوماتية داخل المنظمة، بما في ذلك الأجهزة والبرمجيات وأصول البيانات. يضمن تتبع وصيانة وحماية جميع الأصول طوال دورة حياتها

2. Assigning Ownership تعيين الملكية

This focuses on assigning responsibility for the protection and management of an asset to a specific individual or department, ensuring accountability and proper handling of assets.

يركز على تعيين المسؤولية عن حماية وإدارة الأصل لشخص أو قسم معين، مما يضمن المساءلة والمعالجة الصحيحة للأصول

3. Classifying Assets Based on Value تصنيف الأصول بناءً على القيمة

This involves categorizing data based on its value, sensitivity, and criticality to ensure appropriate levels of protection and handling.

يشمل تصنيف البيانات بناءً على قيمتها وحساسيتها وأهميتها لضمان مستويات حماية ومعالجة مناسبة

4. Data Protection Based on Classification حماية البيانات بناءً على التصنيف

This describes the methods used to protect data based on its classification, including

encryption, access control, and backup.

يصف الطرق المستخدمة لحماية البيانات بناءً على تصنيفها، بما في ذلك التشفير والتحكم في الوصول والنسخ الاحتياطي

5. Data Lifecycle Management إدارة دورة حياة البيانات

This explains the stages of the data lifecycle, from creation to disposal, and the processes involved in each stage.

يشرح مراحل دورة حياة البيانات، من الإنشاء إلى التخلص، والعمليات المتضمنة في كل مرحلة

6. Data Destruction and Disposal إتلاف البيانات والتخلص منها

This details the methods and practices for securely destroying and disposing of data that is no longer needed.

يوضح الطرق والممارسات لتدمير والتخلص من البيانات بشكل آمن عندما لم تعد بحاجة إليها.

7. Digital Rights Management (DRM) إدارة الحقوق الرقمية

This describes how DRM technologies protect digital content by controlling its use, distribution, and access.

يصف كيف تحمي تقنيات إدارة الحقوق الرقمية خلال التحكم في استخدامه وتوزيعه والوصول إليه

8. Data Loss Prevention (DLP) منع فقدان البيانات

This explains how DLP technologies monitor, detect, and prevent the unauthorized transfer of data, protecting sensitive information from data breaches.

يشرح كيف تراقب وتكتشف وتمنع تقنيات منع فقدان البيانات ونقل البيانات غير المصرح به، وحماية المعلومات الحساسة من خروقات البيانات

9. Asset Assessment and Review تقييم الأصول ومراجعتها

This involves evaluating the value, risk, and security posture of information assets through regular assessments, audits, and reviews.

يشمل تقييم قيمة الأصول والمخاطر ووضع الأمان من خلال التقييمات والمراجعات الدورية

1. Asset Inventory and Management جرد الأصول وإدارتها

• Asset Inventory جرد الأصول

Asset inventory involves maintaining a comprehensive list of all information assets within the organization.

يشمل جرد الأصول الحفاظ على قائمة شاملة بجميع الأصول المعلوماتية داخل المنظمة.

- **Hardware Inventory جرد الأجهزة**

Keeping a detailed record of all physical devices such as servers, workstations, and network equipment.

الاحتفاظ بسجل مفصل لجميع الأجهزة المادية مثل الخوادم وأجهزة الكمبيوتر ومعدات الشبكة

-Example: Listing all company laptops, including their serial numbers and assigned users.

مثال: إدراج جميع أجهزة الكمبيوتر المحمولة الخاصة بالشركة، بما في ذلك الأرقام التسلسلية والمستخدمين المخصصين لها

- **Software Inventory جرد البرمجيات**

Documenting all software applications and licenses used within the organization.

توثيق جميع تطبيقات البرامج والتراخيص المستخدمة داخل المنظمة

-Example: Recording all software licenses for Microsoft Office used in the company.

مثال: تسجيل جميع تراخيص البرامج المستخدمة في الشركة

- **Data Inventory جرد البيانات**

Maintaining a list of all critical data assets, including their location and access controls.

الحفاظ على قائمة بجميع أصول البيانات الحيوية، بما في ذلك موقعها وضوابط الوصول إليها

-Example: Documenting the locations of all customer databases and their access permissions.

مثال: توثيق مواقع جميع قواعد بيانات العملاء وأذونات الوصول إليها

• Asset Lifecycle Management إدارة دورة حياة الأصول

Asset lifecycle management involves managing assets from their acquisition to their disposal, ensuring they are adequately protected and maintained throughout their lifecycle.

تشمل إدارة دورة حياة الأصول إدارة الأصول من استحواذها إلى التخلص منها، مما يضمن حمايتها وصيانتها بشكل كافٍ طوال دورة حياتها.

Example: Implementing policies and procedures for the acquisition, maintenance, and disposal of IT assets.

تنفيذ السياسات والإجراءات لاستحواذ وصيانة والتخلص من الأصول التكنولوجية

- **Acquisition الاستحواذ**

Establishing procedures for acquiring new assets, including vendor selection and procurement processes.

وضع إجراءات للاستحواذ على أصول جديدة، بما في ذلك اختيار الموردين وعمليات الشراء

-Example: Following a standardized procurement process for purchasing new servers.

وضع إجراءات للاستحواذ على أصول جديدة، بما في ذلك اختيار الموردين وعمليات الشراء

- **Maintenance الصيانة**

Ensuring regular maintenance and updates to keep assets functioning effectively.

ضمان الصيانة الدورية والتحديثات للحفاظ على الأصول تعمل بشكل فعال

-Example: Scheduling regular updates and patches for software applications to

ensure they remain secure and functional.

مثال: جدولة التحديثات والبرامج التصحيحية بانتظام لتطبيقات البرمجيات لضمان بقائها آمنة وفعالة

- **Disposal التخلص**

Implementing secure disposal methods for assets that are no longer needed.

تنفيذ طرق التخلص الآمن للأصول التي لم تعد بحاجة إليها

-Example: Securely wiping and then recycling old hard drives.

مثال: مسح آمن ثم إعادة تدوير الأقراص الصلبة القديمة

Multiple Choice Questions:

1. What is the primary purpose of asset inventory in asset management?

A. To generate revenue from assets

B. To maintain a comprehensive list of all information assets

C. To sell assets to external parties

D. To remove assets from the inventory

2. Which process involves managing assets from their acquisition to their disposal?

A. Asset classification

B. Asset ownership

C. Asset lifecycle management

D. Asset disposal

3. What is an example of asset inventory?

A. Selling obsolete equipment

B. Maintaining an inventory of hardware, software, and data assets

C. Removing outdated software from the system

D. Assigning responsibility for asset protection

4. Why is asset lifecycle management important in asset management?

A. To categorize assets based on sensitivity

B. To assign responsibility for the protection and management of an asset

C. To manage assets from their acquisition to their disposal

D. To sell assets to external parties

5. What is the role of asset inventory in asset management?

A. To sell assets to external parties

B. To categorize data based on its value

C. To maintain a comprehensive list of all information assets

D. To remove data from the system

Answers and Explanations:

1. Answer: B. To maintain a comprehensive list of all information assets

Explanation: The primary purpose of asset inventory in asset management is to maintain a comprehensive list of all information assets within the organization.

الهدف الرئيسي من جرد الأصول في إدارة الأصول هو الحفاظ على قائمة شاملة بجميع الأصول المعلوماتية داخل المنظمة

2. Answer: C. Asset lifecycle management

Explanation: Asset lifecycle management involves managing assets from their acquisition to their disposal, ensuring they are adequately protected and maintained throughout their lifecycle.

تشمل إدارة دورة حياة الأصول إدارة الأصول من استحواذها إلى التخلص منها، مما يضمن حمايتها وصيانتها بشكل كافٍ طوال دورة حياتها

3. Answer: B. Maintaining an inventory of hardware, software, and data assets

Explanation: An example of asset inventory is maintaining a comprehensive list of hardware, software, and data assets within the organization.

مثال على جرد الأصول هو الحفاظ على قائمة شاملة بالأجهزة والبرمجيات وأصول البيانات داخل المنظمة

4. Answer: C. To manage assets from their acquisition to their disposal

Explanation: Asset lifecycle management is important because it ensures that assets are managed from their acquisition to their disposal, maintaining their protection and value throughout their lifecycle.

إدارة دورة حياة الأصول مهمة لأنها تضمن إدارة الأصول من استحواذها إلى التخلص منها، مما يحافظ على حمايتها وقيمتها طوال دورة حياتها

5. Answer: C. To maintain a comprehensive list of all information assets

Explanation: The role of asset inventory in asset management is to maintain a comprehensive list of all information assets within the organization.

دور جرد الأصول في إدارة الأصول هو الحفاظ على قائمة شاملة بجميع الأصول المعلوماتية داخل المنظمة

---

2. Assigning Ownership تعيين الملكية

• Asset Ownership ملكية الأصول

Asset ownership involves assigning responsibility for the protection and management of an asset to a specific individual or department.

يشمل تحديد ملكية الأصول تعيين المسؤولية عن حماية وإدارة الأصل لشخص أو قسم معين

-Example: Assigning a data owner to be responsible for the protection and management of customer data.

تعيين مالك للبيانات ليكون مسؤولاً عن حماية وإدارة بيانات العملاء

- **Data Owner مالك البيانات**

The individual responsible for the overall protection and management of data.

الفرد المسؤول عن الحماية العامة وإدارة البيانات

-Example: The head of the IT department being designated as the data owner for all company IT assets.

مثال: تعيين رئيس قسم تكنولوجيا المعلومات كمالك للبيانات لجميع أصول الشركة المتعلقة بتكنولوجيا المعلومات

- **Data Custodian أمين البيانات**

The individual or entity responsible for the safe custody, transport, and storage of the data.

الفرد أو الكيان المسؤول عن حفظ البيانات بأمان ونقلها وتخزينها

-Example: The IT security team acting as the data custodian for encrypted backups.

مثال: فريق أمن تكنولوجيا المعلومات يتصرف كأمين للبيانات للنسخ الاحتياطية المشفرة

- **Data Steward مشرف البيانات**

The individual responsible for ensuring data quality and integrity.

الفرد المسؤول عن ضمان جودة البيانات ونزاهتها

-Example: A database administrator acting as a data steward, ensuring data accuracy and consistency.

مثال: مسؤول قاعدة البيانات يتصرف كمشرف على البيانات، لضمان دقة البيانات واتساقها

- **Data Processor معالج البيانات**

The entity that processes data on behalf of the data owner.

الكيان الذي يعالج البيانات نيابة عن مالك البيانات

-Example: An external cloud service provider acting as a data processor for storing and managing data.

مثال: مزود خدمة سحابية خارجي يتصرف كمعالج بيانات لتخزين وإدارة البيانات

- Data Subject موضوع البيانات

The individual whose personal data is being processed.

الفرد الذي تتم معالجة بياناته الشخصية

-Example: A customer whose personal information is stored and processed by the company.

مثال: عميل يتم تخزين ومعالجة معلوماته الشخصية من قبل الشركة

Multiple Choice Questions:

1. What is the primary purpose of asset ownership in asset management?

A. To generate revenue from assets

B. To assign responsibility for the protection and management of an asset

C. To sell assets to external parties

D. To remove assets from the inventory

2. Which role is responsible for the overall protection and management of data?

A. Data Processor

B. Data Custodian

C. Data Owner

D. Data Subject

3. What is an example of a data custodian's responsibility?

A. Ensuring data quality and integrity

B. Processing data on behalf of the data owner

C. Safe custody, transport, and storage of data

D. Assigning responsibility for data protection

4. Why is the role of a data steward important in asset management?

A. To generate revenue from data

B. To ensure data quality and integrity

C. To sell data to external parties

D. To remove data from the inventory

5. What is the role of a data processor in asset management?

A. To sell data to external parties

B. To categorize data based on its value

C. To process data on behalf of the data owner

D. To remove data from the system

Answers and Explanations:

1. Answer: B. To assign responsibility for the protection and management of an asset

Explanation: The primary purpose of asset ownership in asset management is to assign responsibility for the protection and management of an asset to a specific individual or department.

الهدف الرئيسي من ملكية الأصول في إدارة الأصول هو تعيين المسؤولية عن حماية وإدارة الأصل لشخص أو قسم معين

2. Answer: C. Data Owner

Explanation: The data owner is responsible for the overall protection and management of data.

مالك البيانات هو المسؤول عن الحماية العامة وإدارة البيانات

3. Answer: C. Safe custody, transport, and storage of data

Explanation: A data custodian is responsible for the safe custody, transport, and storage of data.

أمين البيانات مسؤول عن حفظ البيانات بأمان ونقلها وتخزينها

4. Answer: B. To ensure data quality and integrity

Explanation: The role of a data steward is important in asset management because

it ensures data quality and integrity.

دور مشرف البيانات مهم في إدارة الأصول لأنه يضمن جودة البيانات ونزاهتها

5. Answer: C. To process data on behalf of the data owner

Explanation: The role of a data processor in asset management is to process data on behalf of the data owner.

دور معالج البيانات في إدارة الأصول هو معالجة البيانات نيابة عن مالك البيانات

---

3. Classifying Assets Based on Value تصنيف الأصول بناءً على القيمة

• Data Classification Policy سياسة تصنيف البيانات

Data classification policy defines the criteria for categorizing data based on its sensitivity and value to the organization.

تحدد سياسة تصنيف البيانات معايير تصنيف البيانات بناءً على حساسيتها وقيمتها للمنظمة.

-Example: A policy that categorizes data as public, internal, confidential, or highly confidential.

سياسة تصنف البيانات كبيانات عامة أو داخلية أو سرية أو شديدة السرية

• Data Handling Procedures إجراءات معالجة البيانات

Data handling procedures outline the steps for managing data based on its classification to ensure proper protection.

توضح إجراءات معالجة البيانات الخطوات الخاصة بإدارة البيانات بناءً على تصنيفها لضمان الحماية المناسبة

-Example: Procedures for encrypting confidential data during transmission and storage.

إجراءات لتشفير البيانات السرية أثناء الإرسال والتخزين

• Baseline and Guidelines الخطوط الأساسية والإرشادات

Baseline and guidelines provide standardized practices for data classification and handling.

تقدم الخطوط الأساسية والإرشادات ممارسات موحدة لتصنيف ومعالجة البيانات.

-Example: A baseline requiring all confidential data to be encrypted and guidelines for handling highly confidential data.

خط أساسي يتطلب تشفير جميع البيانات السرية وإرشادات لمعالجة البيانات شديدة السرية

• Security Labels and Markings التسميات والعلامات الأمنية

• Security Labels التسميات الأمنية

Labels used to indicate the classification level of data, such as "Confidential" or "Top Secret."

التسميات المستخدمة للإشارة إلى مستوى تصنيف البيانات، مثل "سري" أو "سري للغاية

• System Readable قابل للقراءة بالنظام

Security labels that can be interpreted by computer systems to enforce access controls.

التسميات الأمنية التي يمكن تفسيرها بواسطة أنظمة الكمبيوتر لفرض ضوابط الوصول

• Human Readable قابل للقراءة من البشر

Security markings that are easily understood by humans, such as headers on documents indicating classification level.

العلامات الأمنية التي يسهل فهمها من قبل البشر، مثل العناوين في المستندات التي تشير إلى مستوى التصنيف

• Security Marking العلامات الأمنية

The practice of marking documents and data with classification levels to ensure

proper handling.

ممارسة وضع علامات على المستندات والبيانات بمستويات التصنيف لضمان المعالجة الصحيحة

Multiple Choice Questions:

1. What is the primary purpose of a data classification policy in asset management?

A. To generate revenue from data

B. To define criteria for categorizing data based on sensitivity and value

C. To sell data to external parties

D. To remove data from the inventory

2. Which process involves outlining the steps for managing data based on its classification?

A. Data classification policy

B. Data handling procedures

C. Baseline and guidelines

D. Security labeling

3. What is an example of a baseline in data classification and handling?

A. Selling obsolete data

B. Requiring all confidential data to be encrypted

C. Removing outdated data from the system

D. Assigning responsibility for data protection

4. Why are security labels important in data classification?

A. To categorize data based on sensitivity

B. To indicate the classification level of data

C. To remove data from the inventory

D. To sell data to external parties

5. What is the role of data handling procedures in asset management?

A. To sell data to external parties

B. To define criteria for categorizing data

C. To outline the steps for managing data based on its classification

D. To remove data from the system

Answers and Explanations:

1. Answer: B. To define criteria for categorizing data based on sensitivity and value

Explanation: The primary purpose of a data classification policy in asset management is to define the criteria for categorizing data based on its sensitivity and value to the organization.

الهدف الرئيسي من سياسة تصنيف البيانات في إدارة الأصول هو تحديد معايير تصنيف البيانات بناءً على حساسيتها وقيمتها للمنظمة

2. Answer: B. Data handling procedures

Explanation: Data handling procedures outline the steps for managing data based on its classification to ensure proper protection.

توضح إجراءات معالجة البيانات الخطوات الخاصة بإدارة البيانات بناءً على تصنيفها لضمان الحماية المناسبة

3. Answer: B. Requiring all confidential data to be encrypted

Explanation: An example of a baseline in data classification and handling is requiring all confidential data to be encrypted.

مثال على خط أساسي في تصنيف ومعالجة البيانات هو ضرورة تشفير جميع البيانات السرية

4. Answer: B. To indicate the classification level of data

Explanation: Security labels are important in data classification because they indicate the classification level of data, ensuring proper handling and protection.

التسميات الأمنية مهمة في تصنيف البيانات لأنها تشير إلى مستوى تصنيف البيانات، مما يضمن المعالجة والحماية المناسبة

5. Answer: C. To outline the steps for managing data based on its classification

Explanation: The role of data handling procedures in asset management is to outline the steps for managing data based on its classification to ensure proper protection.

دور إجراءات معالجة البيانات في إدارة الأصول هو توضيح الخطوات الخاصة بإدارة البيانات بناءً على تصنيفها لضمان الحماية المناسبة

---

4. Data Protection Based on Classification حماية البيانات بناءً على التصنيف

• Data in Rest البيانات في الراحة

Data that is stored on physical or digital media and not actively moving through the network.

البيانات المخزنة على وسائل مادية أو رقمية والتي لا تتحرك بنشاط عبر الشبكة

- **Protection Methods طرق الحماية**

1. **Encryption التشفير:** Encrypting stored data to prevent unauthorized access.

-Example: Encrypting a database containing customer information.

تشفير قاعدة بيانات تحتوي على معلومات العملاء

2. Access Control التحكم في الوصول: Implementing access controls to restrict who can view or modify the data.

-Example: Restricting access to sensitive files to only authorized personnel.

تقييد الوصول إلى الملفات الحساسة ليقتصر على الموظفين المصرح لهم فقط

3. Backup النسخ الاحتياطي: Regularly backing up data to ensure it can be restored in case of loss or corruption.

-Example: Scheduling daily backups of critical business data.

جدولة النسخ الاحتياطية اليومية للبيانات الحيوية للأعمال

• Data in Motion البيانات في الحركة

Data that is actively moving through the network, such as being transmitted between systems.

البيانات التي تتحرك بنشاط عبر الشبكة، مثل البيانات التي تُنقل بين الأنظمة

- **Protection Methods طرق الحماية**

1. **End-to-End Encryption التشفير من النهاية إلى النهاية:** Encrypting data from the source to the destination to prevent interception.

-Example: Using end-to-end encryption for email communications.

استخدام التشفير من النهاية إلى النهاية للاتصالات البريدية

2. Link Encryption تشفير الروابط: Encrypting data as it travels over specific network segments.

-Example: Encrypting data over a VPN connection.

3. Onion Routing التوجيه البصلي: Using multiple layers of encryption to anonymize the data's path through the network.

-Example: Using the Tor network for secure and anonymous browsing.

استخدام شبكة تور للتصفح الآمن والمجهول

• Archive and Retention Period الأرشفة وفترة الاحتفاظ

- **Archiving الأرشفة:** Storing data that is no longer actively used but must be retained for legal, regulatory, or historical purposes.

-Example: Archiving financial records for seven years for regulatory compliance.

أرشفة السجلات المالية لمدة سبع سنوات للامتثال التنظيمي

- **Retention Period فترة الاحتفاظ:** Defining how long data must be retained before it can be safely deleted.

-Example: Retaining customer data for five years after the end of the business relationship.

الاحتفاظ ببيانات العملاء لمدة خمس سنوات بعد انتهاء العلاقة التجارية

• Roles in Data Protection الأدوار في حماية البيانات

1. **Data Owner مالك البيانات**

The individual or entity responsible for the overall protection and management of data.

الفرد أو الكيان المسؤول عن الحماية العامة وإدارة البيانات

-Example: The head of the IT department being designated as the data owner for all company IT assets.

مثال: تعيين رئيس قسم تكنولوجيا المعلومات كمالك للبيانات لجميع أصول الشركة المتعلقة بتكنولوجيا المعلومات

2. Data Processor معالج البيانات

The entity that processes data on behalf of the data owner.

الكيان الذي يعالج البيانات نيابة عن مالك البيانات

-Example: An external cloud service provider acting as a data processor for storing and managing data.

مثال: مزود خدمة سحابية خارجي يتصرف كمعالج بيانات لتخزين وإدارة البيانات

3. Data Custodian أمين البيانات

The individual or entity responsible for the safe custody, transport, and storage of the data.

الفرد أو الكيان المسؤول عن حفظ البيانات بأمان ونقلها وتخزينها

-Example: The IT security team acting as the data custodian for encrypted backups.

مثال: فريق أمن تكنولوجيا المعلومات يتصرف كأمين للبيانات للنسخ الاحتياطية المشفرة

4. Data Steward مشرف البيانات

The individual responsible for ensuring data quality and integrity.

الفرد المسؤول عن ضمان جودة البيانات ونزاهتها

-Example: A database administrator acting as a data steward, ensuring data accuracy and consistency.

مثال: مسؤول قاعدة البيانات يتصرف كمشرف على البيانات، لضمان دقة البيانات واتساقها

5. Data Subject موضوع البيانات

The individual whose personal data is being processed.

الفرد الذي تتم معالجة بياناته الشخصية

-Example: A customer whose personal information is stored and processed by the company.

مثال: عميل يتم تخزين ومعالجة معلوماته الشخصية من قبل الشركة

Multiple Choice Questions:

1. What is the role of a data owner in data protection?

A. To process data on behalf of the data owner

B. To ensure data quality and integrity

C. To be responsible for the overall protection and management of data

D. To safely store and transport data

2. What method can be used to protect data in rest?

A. End-to-End Encryption

B. Link Encryption

C. Backup

D. Onion Routing

3. What is an example of data in motion?

A. Data stored on a hard drive

B. Data being transmitted between systems

C. Archived financial records

D. Backed-up data on a server

4. Why is a retention period important in data management?

A. To ensure data is encrypted

B. To define how long data must be retained before deletion

C. To classify data based on sensitivity

D. To manage data access controls

5. What is an example of end-to-end encryption?

A. Encrypting a database containing customer information

B. Using VPN for secure connection

C. Encrypting data for email communications

D. Anonymizing data's path through the network

Answers and Explanations:

1. Answer: C. To be responsible for the overall protection and management of data

Explanation: The data owner is responsible for the overall protection and management of data.

مالك البيانات مسؤول عن الحماية العامة وإدارة البيانات

2. Answer: C. Backup

Explanation: One method to protect data in rest is regularly backing up the data to ensure it can be restored in case of loss or corruption.

إحدى طرق حماية البيانات في الراحة هي النسخ الاحتياطي المنتظم للبيانات لضمان استعادتها في حالة الفقد أو التلف

3. Answer: B. Data being transmitted between systems

Explanation: Data in motion refers to data that is actively moving through the network, such as being transmitted between systems.

البيانات في الحركة تشير إلى البيانات التي تتحرك بنشاط عبر الشبكة، مثل البيانات التي تُنقل بين الأنظمة

4. Answer: B. To define how long data must be retained before deletion

Explanation: A retention period is important because it defines how long data must be retained before it can be safely deleted.

فترة الاحتفاظ مهمة لأنها تحدد المدة التي يجب فيها الاحتفاظ بالبيانات قبل أن يتم حذفها بأمان

5. Answer: C. Encrypting data for email communications

Explanation: End-to-end encryption is a method used to protect data during transmission, such as encrypting data for email communications.

التشفير من النهاية إلى النهاية هو طريقة تستخدم لحماية البيانات أثناء الإرسال، مثل تشفير البيانات للاتصالات البريدية

---

5. Data Lifecycle Management إدارة دورة حياة البيانات

• Data Creation إنشاء البيانات

Data creation involves generating new data, either manually or automatically, through business processes and activities.

يشمل إنشاء البيانات توليد بيانات جديدة، إما يدويًا أو تلقائيًا، من خلال العمليات والأنشطة التجارية

-Example: Creating a new customer record in a CRM system.

إنشاء سجل عميل جديد في نظام إدارة علاقات العملاء

• **Data Storage تخزين البيانات**

Data storage involves saving data in physical or digital formats for future use and reference.

يشمل تخزين البيانات حفظ البيانات في صيغ مادية أو رقمية للاستخدام والمراجع المستقبلية

-Example: Storing documents on a secure file server.

تخزين المستندات على خادم ملفات آمن

NIS2 Requirements: 10 Ideas in Which Asset Management...

InvGate · 2 months ago

• Data Usage استخدام البيانات

Data usage involves accessing and using data for various business purposes and decision-making processes.

يشمل استخدام البيانات الوصول إلى البيانات واستخدامها لأغراض تجارية مختلفة وعمليات اتخاذ القرار

-Example: Analyzing sales data to identify market trends.

تحليل بيانات المبيعات لتحديد اتجاهات السوق

• Data Archiving أرشفة البيانات

Data archiving involves moving data that is no longer actively used to a separate storage system for long-term retention.

يشمل أرشفة البيانات نقل البيانات التي لم تعد مستخدمة بنشاط إلى نظام تخزين منفصل للاحتفاظ طويل الأجل

-Example: Archiving old financial records that are no longer needed for day-to-day operations.

أرشفة السجلات المالية القديمة التي لم تعد مطلوبة للعمليات اليومية

• Data Disposal التخلص من البيانات

Data disposal involves securely destroying data that is no longer needed or required to be retained.

يشمل التخلص من البيانات تدمير البيانات بشكل آمن والتي لم تعد مطلوبة أو يجب الاحتفاظ بها

-Example: Shredding old paper records or securely wiping digital storage devices.

تقطيع السجلات الورقية القديمة أو مسح الأجهزة الرقمية بشكل آمن

Multiple Choice Questions:

1. What is the primary purpose of data creation in the data lifecycle?

A. To destroy old data

B. To generate new data through business processes

C. To store data for future use

D. To archive old data

2. Which process involves saving data in physical or digital formats for future use?

A. Data creation

B. Data storage

C. Data archiving

D. Data disposal

3. What is an example of data usage in the data lifecycle?

A. Creating a new customer record

B. Storing documents on a file server

C. Analyzing sales data for decision-making

D. Archiving old financial records

4. Why is data archiving important in the data lifecycle?

A. To destroy old data

B. To generate new data

C. To move data that is no longer actively used to a separate storage system

D. To securely wipe digital storage devices

5. What is the role of data disposal in the data lifecycle?

A. To generate new data

B. To store data for future use

C. To move data to a separate storage system

D. To securely destroy data that is no longer needed

Answers and Explanations:

1. Answer: B. To generate new data through business processes

Explanation: The primary purpose of data creation in the data lifecycle is to generate new data through business processes and activities.

الهدف الرئيسي من إنشاء البيانات في دورة حياة البيانات هو توليد بيانات جديدة من خلال العمليات والأنشطة التجارية

2. Answer: B. Data storage

Explanation: Data storage involves saving data in physical or digital formats for future use and reference.

يشمل تخزين البيانات حفظ البيانات في صيغ مادية أو رقمية للاستخدام والمراجع المستقبلية

3. Answer: C. Analyzing sales data for decision-making

Explanation: An example of data usage in the data lifecycle is accessing and

analyzing sales data for decision-making purposes.

مثال على استخدام البيانات في دورة حياة البيانات هو الوصول إلى بيانات المبيعات وتحليلها لأغراض اتخاذ القرار

4. Answer: C. To move data that is no longer actively used to a separate storage system

Explanation: Data archiving is important because it involves moving data that is no longer actively used to a separate storage system for long-term retention.

أرشفة البيانات مهمة لأنها تشمل نقل البيانات التي لم تعد مستخدمة بنشاط إلى نظام تخزين منفصل للاحتفاظ طويل الأجل

5. Answer: D. To securely destroy data that is no longer needed

Explanation: The role of data disposal in the data lifecycle is to securely destroy data that is no longer needed or required to be retained.

دور التخلص من البيانات في دورة حياة البيانات هو تدمير البيانات بشكل آمن والتي لم تعد مطلوبة أو يجب الاحتفاظ بها

---

6. Data Destruction and Disposal إتلاف البيانات والتخلص منها

• Defendable Destruction الإتلاف القابل للدفاع

Defendable destruction involves securely destroying data in a manner that ensures it cannot be recovered or reconstructed.

يشمل الإتلاف القابل للدفاع تدمير البيانات بشكل آمن لضمان عدم إمكانية استعادتها أو إعادة بنائها

-Example: Using multiple methods to destroy data on a hard drive to prevent data

recovery.

استخدام طرق متعددة لتدمير البيانات على قرص صلب لمنع استعادة البيانات

• Media Destruction تدمير الوسائط

Media destruction involves physically destroying storage media to render data unrecoverable.

يشمل تدمير الوسائط تدمير وسائط التخزين ماديًا لجعل البيانات غير قابلة للاسترجاع

-Example: Shredding or disintegrating old hard drives and CDs.

تقطيع أو تفكيك الأقراص الصلبة القديمة والأقراص المدمجة

• Methods of Data Destruction طرق تدمير البيانات

1. **Shredding التقطيع:** Cutting paper documents or storage media into small pieces.

-Example: Shredding paper records containing sensitive information.

تقطيع السجلات الورقية التي تحتوي على معلومات حساسة

2. Disintegrating التفكيك: Breaking down storage media into small, unrecoverable pieces.

-Example: Using a disintegrator to destroy hard drives.

استخدام مفكك لتدمير الأقراص الصلبة

3. Incinerating الحرق: Burning data storage media to ashes.

-Example: Incinerating old paper records and CDs.

حرق السجلات الورقية القديمة والأقراص المدمجة

4. Drilling الحفر: Drilling holes into storage media to physically destroy it.

-Example: Drilling through hard drives to render them unusable.

الحفر عبر الأقراص الصلبة لجعلها غير قابلة للاستخدام

5. Degaussing إزالة المغنطة: Using a strong magnetic field to erase data on

magnetic media.

-Example: Degaussing old tapes and hard drives.

استخدام مجال مغناطيسي قوي لمسح البيانات على الأشرطة القديمة والأقراص الصلبة

6. Crypto Shredding التقطيع بالتشفير: Encrypting data and then deleting the encryption keys.

-Example: Encrypting and crypto shredding data on a cloud storage service.

تشفير وتقطيع البيانات بالتشفير على خدمة تخزين السحابة

7. Overwriting الكتابة فوق: Writing new data over existing data to prevent recovery.

-Example: Overwriting data on a hard drive multiple times to ensure it is unrecoverable.

الكتابة فوق البيانات على قرص صلب عدة مرات لضمان عدم استرجاعها

8. Wiping المسح: Using software to securely erase data from storage devices.

-Example: Using a data wiping tool to erase all data on a laptop.

استخدام أداة مسح البيانات لمسح جميع البيانات على جهاز كمبيوتر محمول

9. Erasure المسح: Removing data from storage devices through software-based methods.

-Example: Using a secure erase function to delete data from an SSD.

استخدام وظيفة مسح آمنة لحذف البيانات من القرص الصلب

Multiple Choice Questions:

1. What is the primary purpose of defendable destruction?

A. To sell data to external parties

B. To securely destroy data to ensure it cannot be recovered

C. To store data for future use

D. To archive old data

2. Which method involves physically destroying storage media to render data unrecoverable?

A. Degaussing

B. Crypto Shredding

C. Media Destruction

D. Overwriting

3. What is an example of shredding in data destruction?

A. Burning data storage media

B. Using a strong magnetic field to erase data

C. Cutting paper documents into small pieces

D. Writing new data over existing data

4. Why is data wiping important in data destruction?

A. To generate new data

B. To store data for future use

C. To securely erase data from storage devices

D. To archive old data

5. What is the role of incinerating in data destruction?

A. Encrypting data before deletion

B. Burning data storage media to ashes

C. Drilling holes into storage media

D. Breaking down storage media into small pieces

Answers and Explanations:

1. Answer: B. To securely destroy data to ensure it cannot be recovered

Explanation: The primary purpose of defendable destruction is to securely destroy data in a manner that ensures it cannot be recovered or reconstructed.

الهدف الرئيسي من الإتلاف القابل للدفاع هو تدمير البيانات بشكل آمن لضمان عدم إمكانية استعادتها أو إعادة بنائها

2. Answer: C. Media Destruction

Explanation: Media destruction involves physically destroying storage media to render data unrecoverable.

يشمل تدمير الوسائط تدمير وسائط التخزين ماديًا لجعل البيانات غير قابلة للاسترجاع

3. Answer: C. Cutting paper documents into small pieces

Explanation: Shredding in data destruction involves cutting paper documents or storage media into small pieces to ensure data cannot be recovered.

التقطيع في تدمير البيانات يشمل تقطيع المستندات الورقية أو وسائط التخزين إلى قطع صغيرة لضمان عدم إمكانية استعادة البيانات

4. Answer: C. To securely erase data from storage devices

Explanation: Data wiping is important in data destruction because it uses software to securely erase data from storage devices.

المسح البيانات مهم في تدمير البيانات لأنه يستخدم البرامج لمسح البيانات من أجهزة التخزين بشكل آمن

5. Answer: B. Burning data storage media to ashes

Explanation: Incinerating in data destruction involves burning data storage media to ashes to ensure data cannot be recovered.

الحرق في تدمير البيانات يشمل حرق وسائط تخزين البيانات إلى رماد لضمان عدم إمكانية استعادة البيانات

---

7. Digital Rights Management (DRM) إدارة الحقوق الرقمية

• DRM Technologies تقنيات إدارة الحقوق الرقمية

DRM technologies protect digital content by controlling how it can be used, distributed, and accessed.

تحمي تقنيات إدارة الحقوق الرقمية (DRM) المحتوى الرقمي من خلال التحكم في كيفية استخدامه وتوزيعه والوصول إليه.

-Example: Using DRM to restrict copying and sharing of digital books.

استخدام إدارة الحقوق الرقمية (DRM) لتقييد نسخ ومشاركة الكتب الرقمية

• Access Controls التحكم في الوصول

DRM implements access controls to restrict who can view or use digital content.

تنفذ إدارة الحقوق الرقمية (DRM) ضوابط الوصول لتقييد من يمكنه عرض أو استخدام المحتوى الرقمي

-Example: Restricting access to a video stream to authorized users only.

تقييد الوصول إلى بث الفيديو للمستخدمين المصرح لهم فقط

• Encryption التشفير

DRM uses encryption to protect digital content from unauthorized access.

تستخدم إدارة الحقوق الرقمية التشفير لحماية المحتوى الرقمي من الوصول غير المصرح به

-Example:Encrypting e-books to prevent unauthorized reading or copying.

تشفير الكتب الإلكترونية لمنع القراءة أو النسخ غير المصرح به

Multiple Choice Questions:

1. What is the primary purpose of DRM technologies?

A. To generate revenue from digital content

B. To protect digital content by controlling its use and distribution

C. To sell digital content to external parties

D. To remove digital content from the inventory

2. Which DRM method involves restricting who can view or use digital content?

A. Encryption

B. Access Controls

C. Archiving

D. Shredding

3. What is an example of encryption in DRM?

A. Restricting copying and sharing of digital books

B. Encrypting e-books to prevent unauthorized reading or copying

C. Burning digital content to ashes

D. Writing new data over existing digital content

4. Why are access controls important in DRM?

A. To generate new digital content

B. To define criteria for categorizing digital content

C. To restrict who can view or use digital content

D. To archive old digital content

5. What is the role of encryption in DRM?

A. To sell digital content to external parties

B. To securely destroy digital content

C. To protect digital content from unauthorized access

D. To store digital content for future use

Answers and Explanations:

1. Answer: B. To protect digital content by controlling its use and distribution

Explanation: The primary purpose of DRM technologies is to protect digital content by controlling how it can be used, distributed, and accessed.

الهدف الرئيسي من تقنيات إدارة الحقوق الرقمية هو حماية المحتوى الرقمي من خلال التحكم في كيفية استخدامه وتوزيعه والوصول إليه

2. Answer: B. Access Controls

Explanation: Access controls in DRM restrict who can view or use digital content.

ضوابط الوصول في إدارة الحقوق الرقمية تقيد من يمكنه عرض أو استخدام المحتوى الرقمي

3. Answer: B. Encrypting e-books to prevent unauthorized reading or copying

Explanation: An example of encryption in DRM is encrypting e-books to prevent unauthorized reading or copying.

مثال على التشفير في إدارة الحقوق الرقمية هو تشفير الكتب الإلكترونية لمنع القراءة أو النسخ غير المصرح به

4. Answer: C. To restrict who can view or use digital content

Explanation: Access controls are important in DRM because they restrict who can view or use digital content.

ضوابط الوصول مهمة في إدارة الحقوق الرقمية لأنها تقيد من يمكنه عرض أو استخدام المحتوى الرقمي

5. Answer: C. To protect digital content from unauthorized access

Explanation: The role of encryption in DRM is to protect digital content from unauthorized access.

دور التشفير في إدارة الحقوق الرقمية هو حماية المحتوى الرقمي من الوصول غير المصرح به

---

8. Data Loss Prevention (DLP) منع فقدان البيانات

• DLP Technologies تقنيات منع فقدان البيانات

DLP technologies monitor and control data transfers to prevent unauthorized access and data breaches.

تقنيات منع فقدان البيانات (DLP) تراقب وتتحكم في نقل البيانات لمنع الوصول غير المصرح به والانتهاكات البيانات.

-Example: Using DLP software to block the transfer of sensitive data through email.

لمنع نقل البيانات الحساسة عبر البريد الإلكتروني DLP استخدام برنامج

• Content Inspection فحص المحتوى

DLP technologies inspect the content of data being transferred to detect sensitive information.

تفحص محتوى البيانات المنقولة لاكتشاف المعلومات الحساسة DLP تقنيات

-Example: Inspecting outgoing emails to detect and block the transfer of credit card numbers.

فحص رسائل البريد الإلكتروني الصادرة لاكتشاف ومنع نقل أرقام بطاقات الائتمان

• Policy Enforcement تنفيذ السياسات

DLP technologies enforce organizational policies regarding the handling and transfer of sensitive data.

تنفذ سياسات المنظمة بشأن معالجة ونقل البيانات الحساسة DLP تقنيات

-Example: Enforcing a policy that prevents employees from transferring sensitive data to personal cloud storage.

تنفيذ سياسة تمنع الموظفين من نقل البيانات الحساسة إلى تخزين السحابة الشخصية

• Incident Response الاستجابة للحوادث

DLP technologies provide alerts and tools for responding to data breach incidents.

توفر تنبيهات وأدوات للاستجابة لحوادث خرق البيانات DLP تقنيات

-Example: Generating an alert when an unauthorized attempt to transfer sensitive data is detected.

إنشاء تنبيه عند اكتشاف محاولة غير مصرح بها لنقل البيانات الحساسة

• Most Famous DLP Solutions أشهر حلول منع فقدان البيانات

1- Symantec DLP

Symantec's DLP solution offers comprehensive protection for data in motion, at rest, and in use, with advanced content inspection and incident response capabilities.

يوفر حل سيمانتك حماية شاملة للبيانات في الحركة والراحة والاستخدام، مع قدرات فحص المحتوى المتقدمة والاستجابة للحوادث

-Example: Using Symantec DLP to prevent unauthorized sharing of sensitive files via email.

مثال: استخدام سيمانتك لمنع مشاركة الملفات الحساسة غير المصرح بها عبر البريد الإلكتروني.

2- McAfee Total Protection for DLP

McAfee's DLP solution integrates with their broader security platform, providing data protection across endpoints, networks, and the cloud.

يتكامل حل مكافي مع منصتهم الأمنية الأوسع، ويوفر حماية البيانات عبر النقاط النهائية والشبكات والسحابة

-Example: Using McAfee DLP to monitor and control data transfers to USB devices.

مثال: استخدام مكافي لمراقبة والتحكم في نقل البيانات إلى أجهزة الاقراص الصلبة المحمولة

3- Forcepoint DLP

Forcepoint's DLP solution emphasizes human-centric security, focusing on understanding user behavior and preventing data breaches through behavioral analytics.

يركز حل فورسبوينت على الأمان المرتكز على الإنسان، مع التركيز على فهم سلوك المستخدم ومنع خروقات البيانات من خلال تحليلات السلوك

-Example: Using Forcepoint DLP to detect and block anomalous data transfer activities.

مثال: استخدام فورسبوينت لاكتشاف ومنع أنشطة نقل البيانات الشاذة

4- Digital Guardian DLP

Digital Guardian's DLP solution offers both endpoint and network data protection, with strong capabilities for protecting intellectual property and regulated data.

يوفر حل ديجيتال جارديان حماية البيانات عبر النقاط النهائية والشبكات، مع قدرات قوية لحماية الملكية الفكرية والبيانات المنظمة

 Example: Using Digital Guardian DLP to enforce encryption on sensitive data before transfer.

مثال: استخدام ديجيتال جارديان لفرض التشفير على البيانات الحساسة قبل النقل

Multiple Choice Questions:

1. What is the primary purpose of DLP technologies?

A. To generate revenue from data

B. To monitor and control data transfers to prevent unauthorized access

C. To sell data to external parties

D. To remove data from the inventory

2. Which DLP method involves inspecting the content of data being transferred?

A. Content Inspection

B. Policy Enforcement

C. Incident Response

D. Data Encryption

3. What is an example of policy enforcement in DLP?

A. Inspecting outgoing emails to detect sensitive information

B. Blocking the transfer of sensitive data through email

C. Enforcing a policy that prevents transferring sensitive data to personal cloud storage

D. Generating an alert for unauthorized data transfer

4. Why is content inspection important in DLP?

A. To generate new data

B. To define criteria for categorizing data

C. To detect sensitive information being transferred

D. To securely store data

5. What is the role of incident response in DLP?

A. To sell data to external parties

B. To securely destroy data

C. To provide alerts and tools for responding to data breach incidents

D. To archive old data

Answers and Explanations:

1. Answer: B. To monitor and control data transfers to prevent unauthorized access

Explanation: The primary purpose of DLP technologies is to monitor and control data transfers to prevent unauthorized access and data breaches.

الهدف الرئيسي من تقنيات منع فقدان البيانات هو مراقبة وتحكم في نقل البيانات لمنع الوصول غير المصرح به وانتهاكات البيانات

2. Answer: A. Content Inspection

Explanation: Content inspection in DLP involves inspecting the content of data being transferred to detect sensitive information.

يشمل فحص المحتوى فحص محتوى البيانات المنقولة لاكتشاف المعلومات الحساسة

3. Answer: C. Enforcing a policy that prevents transferring sensitive data to personal cloud storage

Explanation: An example of policy enforcement in DLP is enforcing a policy that prevents employees from transferring sensitive data to personal cloud storage.

مثال على تنفيذ السياسة هو تنفيذ سياسة تمنع الموظفين من نقل البيانات الحساسة إلى تخزين السحابة الشخصية

4. Answer: C. To detect sensitive information being transferred

Explanation: Content inspection is important in DLP because it helps detect sensitive information being transferred and prevents unauthorized data breaches.

فحص المحتوى مهم لأنه يساعد في اكتشاف المعلومات الحساسة المنقولة ومنع خرق البيانات غير المصرح به

5. Answer: C. To provide alerts and tools for responding to data breach incidents

Explanation: The role of incident response in DLP is to provide alerts and tools for responding to data breach incidents.

دور الاستجابة للحوادث هو توفير تنبيهات وأدوات للاستجابة لحوادث خرق البيانات

---

9. Asset Assessment and Review تقييم الأصول ومراجعتها

• Asset Assessment تقييم الأصول

Asset assessment involves evaluating the value, risk, and security posture of information assets.

يشمل تقييم الأصول تقييم قيمة الأصول والمخاطر ووضع الأمان.

-Example: Assessing the security measures in place for critical databases.

تقييم التدابير الأمنية المتبعة لقواعد البيانات الحيوية

• Regular Audits المراجعات الدورية

Conducting regular audits to ensure compliance with security policies and standards.

إجراء المراجعات الدورية لضمان الامتثال مع السياسات والمعايير الأمنية

Example:Performing annual security audits to review the effectiveness of data protection measures.

إجراء مراجعات أمنية سنوية لمراجعة فعالية تدابير حماية البيانات

• Risk Assessment تقييم المخاطر

Identifying and evaluating risks to information assets and implementing controls to mitigate them.

تحديد وتقييم المخاطر على الأصول المعلوماتية وتنفيذ الضوابط لتخفيفها

Example: Conducting a risk assessment to identify vulnerabilities in the network infrastructure.

إجراء تقييم للمخاطر لتحديد الثغرات في بنية الشبكة التحتية

• Asset Review مراجعة الأصول

Periodically reviewing asset inventories and classifications to ensure they are up to date and accurate.

مراجعة قوائم جرد الأصول وتصنيفاتها بشكل دوري للتأكد من أنها محدثة ودقيقة

Example: Reviewing and updating the inventory of software applications used in the organization.

مراجعة وتحديث جرد تطبيقات البرامج المستخدمة في المنظمة

• Continuous Monitoring المراقبة المستمرة

Implementing continuous monitoring tools and processes to detect and respond to security incidents in real-time.

تنفيذ أدوات وعمليات المراقبة المستمرة لاكتشاف والاستجابة لحوادث الأمان في الوقت الفعلي.

-Example: Using a Security Information and Event Management (SIEM) system to monitor network activity.

استخدام نظام إدارة معلومات الأمان والأحداث لمراقبة نشاط الشبكة

Multiple Choice Questions:

1. What is the primary purpose of asset assessment in asset management?

A. To generate revenue from assets

B. To evaluate the value, risk, and security posture of information assets

C. To sell assets to external parties

D. To remove assets from the inventory

2. Which process involves conducting regular audits to ensure compliance with security policies and standards?

A. Asset assessment

B. Risk assessment

C. Regular audits

D. Continuous monitoring

3. What is an example of asset review in asset management?

A. Selling obsolete equipment

B. Reviewing and updating the inventory of software applications

C. Conducting a risk assessment to identify vulnerabilities

D. Using a SIEM system to monitor network activity

4. Why is risk assessment important in asset management?

A. To categorize assets based on sensitivity

B. To assign responsibility for the protection and management of an asset

C. To identify and evaluate risks to information assets

D. To generate revenue from assets

5. What is the role of continuous monitoring in asset management?

A. To sell assets to external parties

B. To define criteria for categorizing assets

C. To detect and respond to security incidents in real-time

D. To remove data from the system

Answers and Explanations:

1. Answer: B. To evaluate the value, risk, and security posture of information assets

Explanation: The primary purpose of asset assessment in asset management is to evaluate the value, risk, and security posture of information assets.

الهدف الرئيسي من تقييم الأصول في إدارة الأصول هو تقييم قيمة الأصول والمخاطر ووضع الأمان

2. Answer: C. Regular audits

Explanation: Regular audits involve conducting periodic reviews to ensure compliance with security policies and standards.

تشمل المراجعات الدورية إجراء مراجعات دورية لضمان الامتثال للسياسات والمعايير الأمنية

3. Answer: B. Reviewing and updating the inventory of software applications

Explanation: An example of asset review in asset management is periodically reviewing and updating the inventory of software applications used in the organization.

مثال على مراجعة الأصول في إدارة الأصول هو مراجعة وتحديث جرد تطبيقات البرامج المستخدمة في المنظمة بشكل دوري

4. Answer: C. To identify and evaluate risks to information assets

Explanation: Risk assessment is important in asset management because it helps identify and evaluate risks to information assets and implement controls to mitigate them.

تقييم المخاطر مهم في إدارة الأصول لأنه يساعد في تحديد وتقييم المخاطر على الأصول المعلوماتية وتنفيذ الضوابط لتخفيفها

5. Answer: C. To detect and respond to security incidents in real-time

Explanation: The role of continuous monitoring in asset management is to detect and respond to security incidents in real-time.

دور المراقبة المستمرة في إدارة الأصول هو اكتشاف والاستجابة لحوادث الأمان في الوقت الفعلي

Conclusion

Effective asset management ensures that information assets are adequately protected and managed throughout their lifecycle. By implementing robust asset inventory processes, classifying data based on its value, and employing appropriate protection measures, organizations can mitigate risks and ensure compliance with regulatory requirements. Regular audits, risk assessments, and continuous monitoring are essential practices to maintain the security and integrity of information assets.

إدارة الأصول الفعالة تضمن حماية وإدارة الأصول المعلوماتية بشكل كافٍ طوال دورة حياتها. من خلال تنفيذ عمليات جرد الأصول القوية، وتصنيف البيانات بناءً على قيمتها، واستخدام تدابير الحماية المناسبة، يمكن للمنظمات تخفيف المخاطر وضمان الامتثال للمتطلبات التنظيمية. تعد المراجعات الدورية وتقييمات المخاطر والمراقبة المستمرة ممارسات أساسية للحفاظ على أمان وسلامة الأصول المعلوماتية

CISSP Resources fo Module 2

1- **Official (ISC)² CISSP Study Guide**

2- **CISSP (ISC)² Official Practice Tests**

3- **CISSP All-in-One Exam Guide by Shon Harris**

4- **Cybrary – CISSP Training by Kelly Handerhan**

https://www.cybrary.it/course/cissp

5- **Oreilly – CISSP Training by Sari Greene**

https://www.oreilly.com/library/view/cissp-4th-edition/9780135328613/?_gl=1*jwhz1z*_ga*MTgyMDY2NDI5LjE3MTczNzAwMDI.*_ga_092EL089CH*MTcxNzM3MDAwMi4xLjEuMTcxNzM3MDEwNi41OC4wLjA.

6- **CISSP bundles by Thor Pedersen**

https://thorteaches.com/cissp/

7- **CISSP MindMaps YouTube Playlist from Destination Certification**

https://www.youtube.com/playlist?list=PLZKdGEfEyJhLd-pJhAD7dNbJyUgpqI4pu

Mahmoud Abdelmonem 1mo
Information Security Analyst | SOC Analyst | eCIR |Threat Hunting | Vulnerability Management| GRC|

شرح أكثر من رائع جزاك الله خيرا

Like · Reply | 1 Reaction

Mohamed Mawia 2mo
Senior IT Specialist at Saudi Xerox

شكرا على الشرح القيم،جزاك الله خير

Like · Reply

Mena Makram 2mo
HSE Manager @ Elsewedy Electric Infrastructure, ASP, NASP Trainer, NEBOSH and ISO 45001,14001 Lead Auditor

Abdelkader Ahmed check that

Like · Reply | 1 Reaction

Mena Makram 2mo
HSE Manager @ Elsewedy Electric Infrastructure, ASP, NASP Trainer, NEBOSH and ISO 45001,14001 Lead Auditor

perfect 👏👏👏

Like · Reply | 1 Reaction

Hesham Hamad 2mo
Network & Security Team Leader @ MADKOUR |CyberSecurity |NSE 4, NSE 6, NSE 7, FCA, FCF, FCP، FCSS Certifed |...

جزاك الله خيرا

Like · Reply | 1 Reaction

See more comments

To view or add a comment, sign in

More articles by this author

Module 7: Security Operations / إدارة عمليات...
Aug 5, 2024

Module 6: Security Assessment and Testing...
Jul 28, 2024

CISSP Module 5: Identi and Access Manageme
Jul 8, 2024

See all

Insights from the community

Information Security Management System (ISMS)

How do you leverage asset inventory to improve your ISMS performance and maturity?

IT Management

How can you manage risks associated with outdated technology?

Business Administration

How can EPM software help you manage risk effectively?

Information Security Management System (ISMS)

How do you update and maintain your asset inventory for ISMS?

Risk Management

What are the latest IT risk management innovations and how can you apply them?

Facility Management (FM)

How can FM risk management tools be integrated with other FM systems?

Show more

Others also viewed

How your IT inventory of assets can help you achieve ISO 27001

Noam Birnbaum · 3y

Take It To The Next Level: Insights from Our ISO 27001 Recertification Audit

Tom Vogel · 5mo

How Do "Management Systems" Fit Together?

Andrew Summers · 9y

Secure Digital Asset Management is a Boardroom Discussion

Ken Linscott · 5y

Loss Prevention Through Effective ITAM Processes and Reporting

Rennie Rollinson · 5y

TOP 5 REASONS: Why Cybersecurity Asset Management Platform Is A Must Have

Bill Kiani · 3y

Show more

Explore topics

Sales

Marketing

Business Administration

HR Management

Content Management

Engineering

Soft Skills

See All

الهندسة المعمارية والهندسة الأمنية
Security Architecture and Engineering

Emad M. Abdelhamid • 2nd
Technical Leader | SME IT Security Design @ Cisco - CX EMEA . ...
View my portfolio

+ Follow ...

3w • Edited •

السلام عليكم ورحمه الله وبركاته
اليوم بإذن الله سنقوم بشرح الفصل الثالث من شهادة ال
CISSP
وهو من الفصول الدسمة والصعبة ويحتوى على الكثير من المصطلحات التي ستوسع افق الدارس لمجالات عدة ومواضيع شيقة ويتحدث الفصل عن الهندسة المعمارية والهندسة الأمنية (Security Architecture and Engineering)

و يغطي هذا الفصل المبادئ الأساسية لأرشفة الأمان والهندسة. ويشمل نماذج الأمان المختلفة، وخدمات التشفير، وقواعد الحوسبة الموثوقة، والحوسبة السحابية، والتوقيعات الرقمية، وثغرات الأنظمة، وتحليل الشفرات، والأمن الفيزيائي. ويهدف إلى توفير فهم شامل لكيفية البحث، وتنفيذ، وإدارة عمليات الهندسة باستخدام مبادئ التصميم الآمن.

ويحتوي على 11 جزء :
It contains 11 parts :

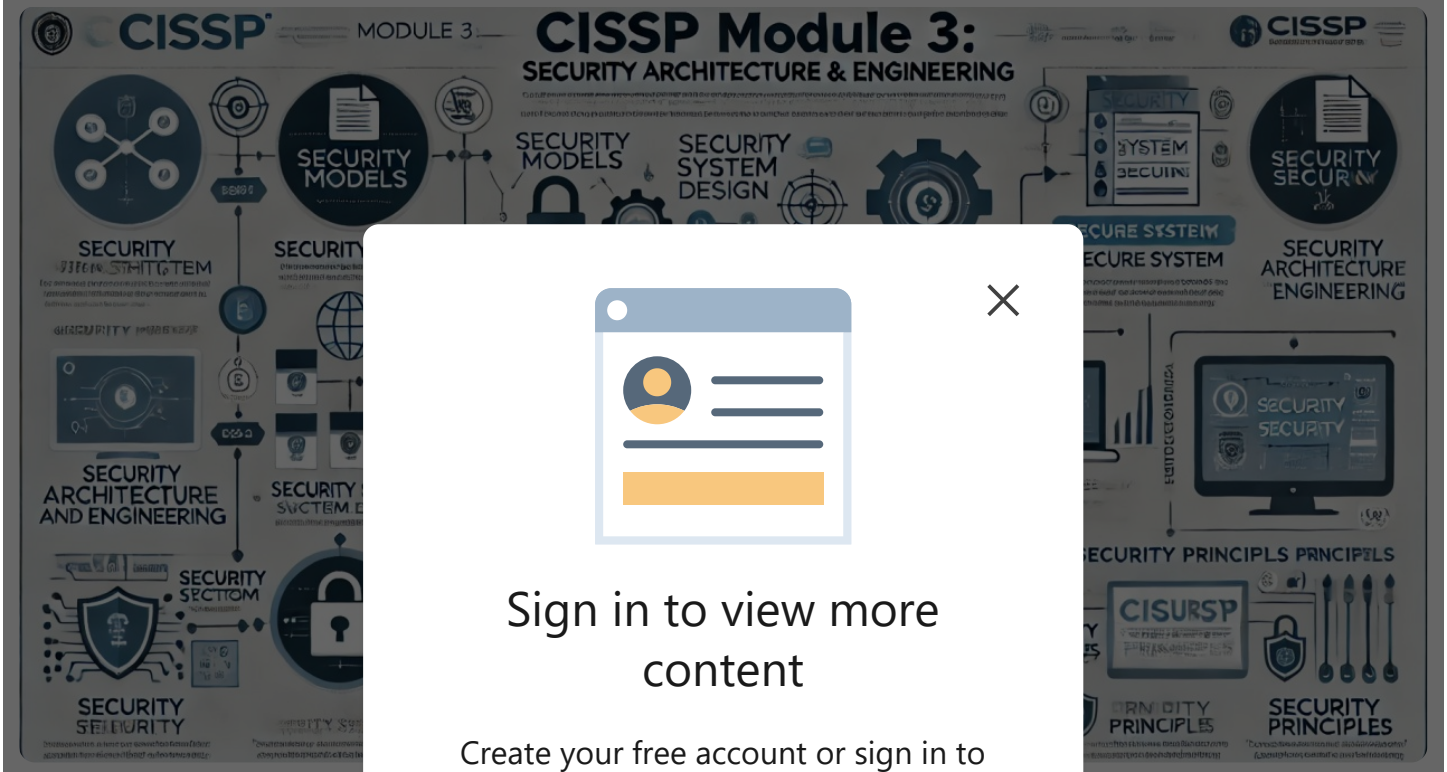
1. Research, Implement, and Manage Engineering Processes Using Secure Design Principles
البحث عن عمليات الهندسة وتنفيذها وإدارتها باستخدام مبادئ التصميم الآمن
2. Understand the Fundamental Concepts of Security Models
فهم المفاهيم الأساسية لنماذج الأمان
3. Select Controls Based Upon Systems Security Requirements
اختيار الضوابط بناءً على متطلبات أمان الأنظمة
4. Understand Security Capabilities of Information Systems
فهم قدرات الأمان لأنظمة المعلومات
5. Assess and Mitigate the Vulnerabilities of Security Architectures, Designs, and Solution Elements
تقييم وتخفيف الثغرات في هياكل الأمان والتصاميم وعناصر الحلول
6. Select and Determine Cryptographic Solutions
اختيار وتحديد الحلول التشفيرية
7. Understand Methods of Cryptanalytic Attacks
فهم طرق الهجمات التحليلية التشفيرية
8. Apply Security Principles to Site and Facility Design
تطبيق مبادئ الأمان على تصميم المواقع والمرافق
9. Design Site and Facility Security Controls
تصميم ضوابط أمان المواقع والمرافق
10. Manage the Information System Lifecycle
إدارة دورة حياة نظام المعلومات
11. Vulnerabilities in Systems
الثغرات في الأنظمة

المقالات

For Module 1 : https://lnkd.in/dkkyFGdW
For Module 2 : https://lnkd.in/dNUWhiJs
For Module 3: https://lnkd.in/dsqBXhEc
For Module 4: https://lnkd.in/d_DBAm4h
For Module 5: https://lnkd.in/dGPDeKWF
For Module 6: https://lnkd.in/dZHHJKJx
For Module 7: https://lnkd.in/d_JswW5W
For Module 8: https://lnkd.in/dQsQHqgR

Resources - المصادر

1- Official (ISC)² CISSP Study Guide
2- CISSP (ISC)² Official Practice Tests
3- CISSP All-in-One Exam Guide by Shon Harris
4- Cybrary – CISSP Training by Kelly Handerhan https://lnkd.in/d4zrAkJz
5- Oreilly – CISSP Training by Sari Greene https://lnkd.in/dANS-hVc.
6- CISSP bundles by Thor Pedersen https://lnkd.in/d2tpqaJk
7- CISSP MindMaps YouTube Playlist from Destination Certification https://lnkd.in/deJM44xX



CISSP Mod ure and Engineerin ال الأمنية

Emad M. Ab
Technical Lead
CCIE#58413 |
ISO27001 LA |

Published Jun 22, 2024

Introduction

This module covers the foundational principles of security architecture and engineering. It includes various security models, cryptographic services, trusted computing bases, cloud computing, digital signatures, system vulnerabilities,

using secure design principles.

يغطي هذا المقرر المبادئ الأساسية لأرشفة الأمان والهندسة. ويشمل نماذج الأمان المختلفة، وخدمات التشفير، وقواعد الحوسبة الموثوقة، والحوسبة السحابية، والتوقيعات الرقمية، وثغرات الأنظمة، وتحليل الشفرات، والأمن الفيزيائي. يهدف إلى توفير فهم شامل لكيفية البحث، وتنفيذ، وإدارة عمليات الهندسة باستخدام مبادئ التصميم الآمن

Module Brief

1. Research, Implement, and Manage Engineering Processes Using Secure Design Principles

This section covers various principles and practices for designing secure systems, including threat modeling, least privilege, defense in depth, secure defaults, fail securely, segregation of duties, keeping systems simple and small, zero trust or trust but verify, privacy by design, shared responsibility, and secure access service edge.

يتناول هذا القسم المبادئ والممارسات المختلفة لتصميم الأنظمة الآمنة، بما في ذلك نمذجة التهديدات، وأقل امتياز، والدفاع في العمق، والافتراضات الآمنة، والفشل الآمن، وفصل الواجبات، وإبقاء الأنظمة بسيطة وصغيرة، والثقة الصفرية أو الثقة مع التحقق، والخصوصية حسب التصميم، والمسؤولية المشتركة، وحافة خدمة الوصول الآمن.

2. Understand the Fundamental Concepts of Security Models

This section explains the foundational concepts of security models, such as enterprise security architecture frameworks and different types of security models including lattice-based and rule-based models.

يوضح هذا القسم المفاهيم الأساسية لنماذج الأمان، مثل أطر أرشفة أمان المؤسسة، وأنواع نماذج الأمان المختلفة بما في ذلك النماذج القائمة على الشبكة والنماذج القائمة على القواعد.

3. Select Controls Based Upon Systems Security Requirements

This section discusses how to select appropriate security controls based on specific system security requirements and evaluation criteria.

يتناول هذا القسم كيفية اختيار الضوابط الأمنية المناسبة بناءً على متطلبات أمان النظام المحددة ومعايير التقييم.

4. Understand Security Capabilities of Information Systems

This section explores the security capabilities of various information systems, including memory protection, Trusted Platform Modules (TPM), and encryption/decryption methods.

يستكشف هذا القسم قدرات الأمان لأنظمة المعلومات المختلفة، بما في ذلك حماية الذاكرة، ووحدات النظام الأساسي الموثوق بها، وطرق التشفير وفك التشفير.

5. Assess and Mitigate the Vulnerabilities of Security Architectures, Designs, and Solution Elements

This section covers how to assess and mitigate vulnerabilities in security architectures, designs, and solution elements, including client-based systems, server-based systems, database systems, and cloud-based systems.

يغطي هذا القسم كيفية تقييم وتخفيف الثغرات في أرشفة الأمان، والتصميم، وعناصر الحلول، بما في ذلك الأنظمة المستندة إلى العميل، والأنظمة المستندة إلى الخادم، وأنظمة قواعد البيانات، والأنظمة السحابية.

6. Select and Determine Cryptographic Solutions

This section provides an overview of selecting and determining cryptographic solutions, including cryptographic life cycles, methods, public key infrastructure (PKI), and key management practices.

يقدم هذا القسم نظرة عامة على اختيار وتحديد حلول التشفير، بما في ذلك دورات حياة التشفير، والطرق، والبنية التحتية للمفاتيح العامة، وممارسات إدارة المفاتيح.

7. Understand Methods of Cryptanalytic Attacks

This section delves into various methods of cryptanalytic attacks and how to defend against them.

يتعمق هذا القسم في طرق هجمات تحليل الشفرات المختلفة وكيفية الدفاع ضدها.

8. Apply Security Principles to Site and Facility Design

This section explains how to apply security principles to the design of physical sites and facilities to ensure their security.

يوضح هذا القسم كيفية تطبيق مبادئ الأمان على تصميم المواقع والمنشآت الفيزيائية لضمان

أمانها.

9. Design Site and Facility Security Controls

This section discusses the design of security controls for sites and facilities, including wiring closets, server rooms, and data centers.

يتناول هذا القسم تصميم ضوابط الأمان للمواقع والمنشآت، بما في ذلك غرف الأسلاك، وغرف الخوادم، ومراكز البيانات.

10. Manage the Information System Lifecycle

This section covers managing the information system lifecycle, from stakeholder needs and requirements through to retirement and disposal.

يغطي هذا القسم إدارة دورة حياة نظام المعلومات من احتياجات ومتطلبات أصحاب المصلحة إلى التقاعد والتخلص منها.

11. Vulnerabilities in Systems

This section identifies vulnerabilities in systems, including those in mobile devices, web-based applications, and general system vulnerabilities.

يحدد هذا القسم الثغرات في الأنظمة، بما في ذلك تلك الموجودة في الأجهزة المحمولة، وتطبيقات الويب، وثغرات النظام العامة.

---

1. Research, Implement, and Manage Engineering Processes Using Secure Design Principles

1.1 Threat Modeling

Definition: The process of identifying potential threats and designing controls to mitigate them. عملية تحديد التهديدات المحتملة وتصميم الضوابط لتخفيفها

Example: Conducting a threat modeling session during the design phase of a new application to identify and address potential security issues. إجراء جلسة نمذجة التهديدات خلال مرحلة تصميم تطبيق جديد لتحديد ومعالجة المشكلات الأمنية المحتملة

Threat Modeling Process: Identifying assets, identifying threats, defining security controls, and validating controls. عملية نمذجة التهديدات تحديد الأصول تحديد التهديدات

تحديد الضوابط الأمنية والتحقق من الضوابط

Detailed Process:

1. Identify Assets: Determine what assets need protection (e.g., data, applications, systems). تحديد الأصول تحديد الأصول التي تحتاج إلى الحماية مثل البيانات والتطبيقات والأنظمة

2. Identify Threats: Determine potential threats to the assets (e.g., hackers, malware, insider threats). تحديد التهديدات تحديد التهديدات المحتملة للأصول مثل المتسللين والبرامج الضارة والتهديدات الداخلية

3. Define Security Controls: Identify and design security measures to protect the assets. تحديد الضوابط الأمنية تحديد وتصميم التدابير الأمنية لحماية الأصول

4. Validate Controls: Test the security controls to ensure they effectively mitigate the identified threats. التحقق من الضوابط اختبار الضوابط الأمنية لضمان فعاليتها في تخفيف التهديدات المحددة

1.2 Least Privilege

Definition: Ensuring users have only the permissions necessary to perform their jobs. ضمان أن المستخدمين لديهم فقط الأذونات اللازمة لأداء وظائفهم

Example: Configuring database access controls so that users can only access the data they need to perform their job functions. تكوين ضوابط الوصول إلى قاعدة البيانات بحيث يمكن للمستخدمين الوصول فقط إلى البيانات التي يحتاجونها لأداء وظائفهم

Implementation: Role-based access control (RBAC), enforcing the principle of least privilege. التحكم في الوصول المستند إلى الدور وتطبيق مبدأ أقل امتياز

Detailed Steps:

1. Role Identification: Identify different roles within the organization and their required access levels. تحديد الأدوار تحديد الأدوار المختلفة داخل المنظمة ومستويات الوصول المطلوبة لكل منها

2. Assign Permissions: Assign permissions to each role based on the principle of least privilege. تعيين الأذونات تعيين الأذونات لكل دور بناءً على مبدأ أقل امتياز

3. Regular Reviews: Conduct regular reviews of permissions to ensure they are still

appropriate. المراجعات الدورية إجراء مراجعات دورية للأذونات لضمان أنها لا تزال مناسبة

4. Adjust as Necessary: Adjust permissions as roles and job functions change within the organization. التعديل حسب الحاجة تعديل الأذونات حسب تغير الأدوار والوظائف داخل المنظمة

1.3 Defense in Depth

Definition: Implementing multiple layers of security controls to protect systems and data. تنفيذ طبقات متعددة من الضوابط الأمنية لحماية الأنظمة والبيانات

Example: Using firewalls, intrusion detection systems, and antivirus software together to protect a network. استخدام الجدران النارية وأنظمة كشف التسلل وبرامج مكافحة الفيروسات معًا لحماية الشبكة

Layers of Defense: Physical, technical, and administrative controls. طبقات الدفاع ضوابط مادية وتقنية وإدارية

Detailed Layers:

1. Physical Controls: Security measures to protect physical access to systems (e.g., locks, security guards, surveillance cameras). الضوابط المادية التدابير الأمنية لحماية الوصول الفيزيائي إلى الأنظمة مثل الأقفال وحراس الأمن وكاميرات المراقبة

2. Technical Controls: Security measures implemented through technology (e.g., firewalls, encryption, intrusion detection systems). الضوابط التقنية التدابير الأمنية التي تنفذ من خلال التكنولوجيا مثل الجدران النارية والتشفير وأنظمة كشف التسلل

3. Administrative Controls: Policies and procedures to manage security (e.g., security training, incident response plans). الضوابط الإدارية السياسات والإجراءات لإدارة الأمان مثل التدريب على الأمان وخطط الاستجابة للحوادث

1.4 Secure Defaults

Definition: Designing systems with default settings that are secure. تصميم الأنظمة بإعدادات افتراضية آمنة

Example: Requiring users to change default passwords upon first login to a new system. طلب تغيير المستخدمين لكلمات المرور الافتراضية عند تسجيل الدخول لأول مرة إلى

نظام جديد

Implementation: Secure configurations, disabling unnecessary features, and services by default. تكوينات آمنة وتعطيل الميزات والخدمات غير الضرورية بشكل افتراضي

Detailed Implementation:

1. Default Configurations: Set default configurations to the most secure settings. الإعدادات الافتراضية تعيين الإعدادات الافتراضية إلى الإعدادات الأكثر أمانًا

2. Disable Unnecessary Features: Disable features and services that are not needed by default. تعطيل الميزات غير الضرورية تعطيل الميزات والخدمات التي لا تكون ضرورية بشكل افتراضي

3. User Awareness: Educate users on the importance of maintaining secure settings. توعية المستخدمين تثقيف المستخدمين حول أهمية الحفاظ على الإعدادات الآمنة

4. Regular Audits: Conduct regular audits to ensure systems remain configured securely. إجراء تدقيقات دورية إجراء تدقيقات دورية لضمان بقاء الأنظمة مهيأة بشكل آمن

1.5 Fail Securely

Definition: Designing systems to deny all access if they fail. تصميم الأنظمة لرفض جميع الوصول إذا فشلت

Example: Configuring a firewall to block all traffic if it experiences an error. تكوين جدار ناري لحظر جميع الحركة إذا واجه خطأ

Implementation: Default to secure state, error handling, and logging. افتراض الحالة الآمنة ومعالجة الأخطاء والتسجيل

Detailed Implementation:

1. Default to Secure State: Ensure that systems revert to a secure state in case of failure. افتراض الحالة الآمنة ضمان أن الأنظمة تعود إلى حالة آمنة في حالة الفشل

2. Error Handling: Implement robust error handling to manage unexpected failures. معالجة الأخطاء تنفيذ معالجة الأخطاء القوية لإدارة حالات الفشل غير المتوقعة

3. Logging: Maintain logs of system failures and security events for analysis and response. التسجيل الحفاظ على سجلات حالات فشل النظام والأحداث الأمنية للتحليل والاستجابة

1.6 Segregation of Duties (SoD)

Definition: Dividing tasks and responsibilities among multiple users to reduce the risk of fraud and error. تقسيم المهام والمسؤوليات بين عدة مستخدمين لتقليل خطر الاحتيال والخطأ

Example: Separating the duties of system administrators and auditors to prevent conflicts of interest. فصل واجبات مسؤولي النظام والمدققين لمنع تضارب المصالح

Implementation: Role separation, least privilege, and independent verification. فصل الأدوار وأقل امتياز والتحقق المستقل

Detailed Implementation:

1. Role Separation: Define and separate roles within the organization to ensure no single user has control over all aspects of a critical process. فصل الأدوار تعريف وفصل الأدوار داخل المنظمة لضمان عدم وجود مستخدم واحد يتحكم في جميع جوانب عملية حاسمة

2. Least Privilege: Ensure that users only have access to the resources necessary for their role. أقل امتياز ضمان أن المستخدمين لديهم فقط الوصول إلى الموارد الضرورية لدورهم

3. Independent Verification: Implement independent checks and audits to verify that duties are being properly segregated. التحقق المستقل تنفيذ عمليات التحقق والتدقيق المستقلة للتحقق من أن الواجبات يتم فصلها بشكل صحيح

1.7 Keep It Simple and Small

Definition: Designing systems to be as simple as possible to reduce the risk of vulnerabilities. تصميم الأنظمة لتكون بسيطة قدر الإمكان لتقليل خطر الثغرات الأمنية

Example: Using a minimal number of software components to reduce the attack surface of an application. استخدام أقل عدد من مكونات البرامج لتقليل سطح الهجوم في التطبيق

Detailed Implementation:

1. Simplify Design: Keep system design as simple as possible to minimize potential vulnerabilities. تبسيط التصميم الحفاظ على تصميم النظام بسيطًا قدر الإمكان لتقليل

الثغرات المحتملة

2. Limit Features: Only include necessary features and functions to avoid unnecessary complexity. تحديد الميزات تضمين الميزات والوظائف الضرورية فقط لتجنب التعقيد غير الضروري

3. Regular Review: Regularly review systems to identify and remove unnecessary complexity. مراجعة منتظمة مراجعة الأنظمة بانتظام لتحديد وإزالة التعقيد غير الضروري

1.8 Zero Trust or Trust but Verify

Definition: Implementing security controls that do not automatically trust any user or system. تنفيذ الضوابط الأمنية التي لا تثق تلقائيًا في أي مستخدم أو نظام

Example: Requiring multi-factor authentication for all users accessing a sensitive system. طلب المصادقة متعددة العوامل لجميع المستخدمين الذين يصلون إلى نظام حساس

Detailed Implementation:

1. Continuous Monitoring: Monitor all network traffic and user activities continuously. المراقبة المستمرة مراقبة جميع حركة المرور على الشبكة وأنشطة المستخدمين باستمرار

2. Strong Authentication: Implement multi-factor authentication to verify user identities. المصادقة القوية تنفيذ المصادقة متعددة العوامل للتحقق من هويات المستخدمين

3. Access Controls: Use granular access controls to limit user access based on their roles and activities. ضوابط الوصول استخدام ضوابط وصول دقيقة لتحديد وصول المستخدم بناءً على أدوارهم وأنشطتهم

1.9 Privacy by Design

Definition: Incorporating privacy considerations into the design and architecture of systems. إدراج اعتبارات الخصوصية في تصميم وهندسة الأنظمة

Example: Implementing data anonymization techniques to protect user privacy in a new analytics system. تنفيذ تقنيات إخفاء الهوية لحماية خصوصية المستخدم في نظام تحليلات جديد

Principles: Proactive not reactive, privacy as default, and privacy embedded into design. مبادئ استباقي وليس تفاعلي الخصوصية كإعداد افتراضي والخصوصية مدمجة في التصميم

Detailed Principles:

1. Proactive not Reactive: Anticipate and prevent privacy issues before they occur. استباقي وليس تفاعلي توقع ومنع مشكلات الخصوصية قبل حدوثها

2. Privacy as Default: Ensure that privacy is the default setting for all systems and processes. الخصوصية كإعداد افتراضي ضمان أن الخصوصية هي الإعداد الافتراضي لجميع الأنظمة والعمليات

3. Privacy Embedded into Design: Integrate privacy measures into the design and architecture of systems from the beginning. الخصوصية مدمجة في التصميم دمج تدابير الخصوصية في تصميم وهندسة الأنظمة من البداية

1.10 Shared Responsibility

Definition: Recognizing that security is a shared responsibility between the organization and its users. الاعتراف بأن الأمان هو مسؤولية مشتركة بين المنظمة ومستخدميها

Example: Providing security awareness training to employees to help them understand their role in protecting the organization's information. توفير تدريب على الوعي الأمني للموظفين لمساعدتهم على فهم دورهم في حماية معلومات المنظمة

Implementation: Security policies, user training, and collaboration between stakeholders. سياسات الأمان وتدريب المستخدم والتعاون بين أصحاب المصلحة

Detailed Implementation:

1. Security Policies: Develop and enforce comprehensive security policies. سياسات الأمان تطوير وتنفيذ سياسات أمان شاملة

2. User Training: Conduct regular security awareness training for all employees. تدريب المستخدم إجراء تدريب منتظم على الوعي الأمني لجميع الموظفين

3. Collaboration: Foster collaboration between different departments and stakeholders to ensure a unified security approach. التعاون تعزيز التعاون بين الأقسام المختلفة وأصحاب المصلحة لضمان نهج أمني موحد

1.11 Secure Access Service Edge (SASE)

Definition: Combining network security functions with wide-area network (WAN) capabilities to support secure access needs. الجمع بين وظائف أمان الشبكة وقدرات الشبكة واسعة النطاق لدعم احتياجات الوصول الآمن

Example: Implementing SASE solutions to provide secure access to cloud applications for remote workers. تنفيذ حلول لتوفير الوصول الآمن إلى التطبيقات السحابية للعاملين عن بُعد

Components: Secure web gateways, cloud access security brokers, firewalls, and zero-trust network access. بوابات الويب الآمنة وسماسرة أمان الوصول إلى السحابة والجدران النارية والوصول إلى الشبكة بدون ثقة

Detailed Components:

1. Secure Web Gateways: Protect against web-based threats by filtering internet traffic. بوابات الويب الآمنة الحماية من التهديدات المستندة إلى الويب عن طريق تصفية حركة المرور على الإنترنت

2. Cloud Access Security Brokers (CASB): Monitor and control access to cloud applications and services. سماسرة أمان الوصول إلى السحابة مراقبة والتحكم في الوصول إلى التطبيقات والخدمات السحابية

3. Firewalls: Protect networks by monitoring and controlling incoming and outgoing traffic. الجدران النارية حماية الشبكات عن طريق مراقبة والتحكم في حركة المرور الواردة والصادرة

4. Zero-Trust Network Access: Ensure that no user or system is trusted by default. الوصول إلى الشبكة بدون ثقة ضمان عدم الثقة بأي مستخدم أو نظام بشكل افتراضي

Multiple Choice Questions

1. Which of the following is a principle of least privilege?

A. Providing users with all permissions

B. Assigning permissions based on the principle of least privilege

C. Allowing users to access all data in the system

D. Granting administrative access to all users

2. What does 'Defense in Depth' refer to in security design?

A. A single layer of security control

B. Multiple layers of security controls

C. Only physical security measures

D. Disabling security features by default

3. What is the purpose of Secure Defaults in system design?

A. Allowing default settings to be easily changed

B. Ensuring default settings are secure

C. Disabling all default features

D. Allowing users to bypass security settings

4. In threat modeling, what is the first step?

A. Identifying threats

B. Defining security controls

C. Identifying assets

D. Validating controls

5. What is an example of Shared Responsibility in security?

A. Only the IT department is responsible for security

B. Employees are not required to understand security policies

C. Providing security awareness training to employees

D. Ignoring user roles in security

Answers and Explanations

1. B.

The principle of least privilege ensures that users have only the permissions necessary to perform their jobs, reducing the risk of unauthorized access and potential security breaches.

يضمن مبدأ أقل امتياز أن المستخدمين لديهم فقط الأذونات اللازمة لأداء وظائفهم، مما يقلل من خطر الوصول غير المصرح به والثغرات الأمنية المحتملة.

2. B.

Defense in Depth involves implementing multiple layers of security controls (physical, technical, and administrative) to protect systems and data from various threats.

يتضمن الدفاع في العمق تنفيذ طبقات متعددة من الضوابط الأمنية (مادية وتقنية وإدارية) لحماية الأنظمة والبيانات من التهديدات المختلفة.

3. B.

Secure Defaults involve designing systems with default settings that are secure, reducing the risk of security breaches by ensuring that systems are secure from the start.

تتضمن الافتراضات الآمنة تصميم الأنظمة بإعدادات افتراضية آمنة، مما يقلل من خطر الثغرات الأمنية عن طريق ضمان أن الأنظمة آمنة من البداية.

4. C.

The first step in threat modeling is to identify the assets that need protection, such as data, applications, and systems, which helps in understanding what needs to be secured.

الخطوة الأولى في نمذجة التهديدات هي تحديد الأصول التي تحتاج إلى الحماية، مثل البيانات والتطبيقات والأنظمة، مما يساعد في فهم ما يجب تأمينه.

5. C.

Shared Responsibility in security means recognizing that security is a shared responsibility between the organization and its users, which includes providing security awareness training to employees.

المسؤولية المشتركة في الأمن تعني الاعتراف بأن الأمن هو مسؤولية مشتركة بين المنظمة ومستخدميها، ويتضمن ذلك توفير تدريب على الوعي الأمني للموظفين

---

2. Understand the Fundamental Concepts of Security Models

2.1 Enterprise Security Architecture

Definition: A framework for aligning IT and security with business goals and regulatory requirements. إطار عمل لمواءمة تقنية المعلومات والأمان مع أهداف العمل والمتطلبات التنظيمية

Components:

1. **Zachman Framework**
2. **Sabsa Framework**
3. **TOGAF (The Open Group Architecture Framework)**

Detailed Frameworks:

1- Zachman Framework: **Description**: Provides a formal and structured way of viewing and defining an enterprise's architecture. It uses a 6x6 matrix to organize the architecture artifacts. .يوفر طريقة رسمية ومنظمة لعرض وتعريف هندسة المؤسسة يستخدم مصفوفة 6*6 لتنظيم المصنوعات المعمارية

Components: Data, Function, Network, People, Time, Motivation. البيانات، الوظيفة، الشبكة، الأشخاص، الوقت، الدافع

Details:

1. **Data**: What data is processed? ؟البيانات: ما البيانات التي تتم معالجتها

2. **Function**: How do the processes work? الوظيفة: كيف تعمل العمليات؟

3. **Network**: Where are the data and processes located? الشبكة: أين توجد البيانات والعمليات؟

4. **People**: Who performs the processes? الأشخاص: من ينفذ العمليات؟

5. **Time**: When are processes performed? الوقت: متى يتم تنفيذ العمليات؟

6. **Motivation**: Why are processes performed? الدافع: لماذا يتم تنفيذ العمليات؟

2- Sabsa Framework: **Description**: A security architecture methodology that is risk-driven and focuses on the creation and maintenance of security architectures aligned with business needs. منهجية هندسة الأمان المدفوعة بالمخاطر والتي تركز على إنشاء وصيانة هندسة الأمان المتوافقة مع احتياجات العمل

Components: Contextual, Conceptual, Logical, Physical, Component, and Operational layers. المكونات الطبقات السياقية والمفهومية والمنطقية والفيزيائية والمكونة والتشغيلية

Details:

1. **Contextual Layer**: Defines business requirements and the context for the architecture. الطبقة السياقية: تحدد متطلبات العمل والسياق للمعمارية.

2. **Conceptual Layer**: Establishes high-level security concepts and principles. الطبقة المفهومية: تؤسس مفاهيم ومبادئ الأمان عالية المستوى.

3. **Logical Layer**: Defines logical security services and processes. الطبقة المنطقية: تحدد الخدمات والعمليات الأمنية المنطقية.

4. **Physical Layer**: Specifies physical implementations of security controls. الطبقة الفيزيائية: تحدد تنفيذات الفيزيائية للضوابط الأمنية.

5. **Component Layer**: Details specific components that provide security services. طبقة المكونات: تفاصيل المكونات المحددة التي توفر الخدمات الأمنية.

6. **Operational Layer**: Defines how security services are operated and managed. الطبقة التشغيلية: تحدد كيفية تشغيل وإدارة الخدمات الأمنية.

3- TOGAF: **Description**: Provides a detailed method and set of supporting tools for developing an enterprise architecture. يقدم طريقة مفصلة ومجموعة من الأدوات الداعمة لتطوير هندسة المؤسسة

Components: Architecture Development Method (ADM), Enterprise Continuum, TOGAF Reference Models. المكونات طريقة تطوير الهندسة، استمرارية المؤسسة، نماذج مرجعية

Details:

1. **Architecture Development Method (ADM)**: A step-by-step approach to developing an enterprise architecture. طريقة تطوير الهندسة: نهج خطوة بخطوة لتطوير هندسة المؤسسة.
2. **Enterprise Continuum**: Provides a framework for categorizing architectural artifacts. استمرارية المؤسسة: يوفر إطارًا لتصنيف المصنوعات المعمارية.
3. **TOGAF Reference Models**: Standardized models for developing architectures. نماذج مرجعية نماذج قياسية لتطوير المعماريات

2.2 Security Models

Definition: Theoretical frameworks to describe how to implement security policies and controls to protect information. الأطر النظرية لوصف كيفية تنفيذ السياسات والضوابط الأمنية لحماية المعلومات

2.2.1 Lattice-Based Models

-Bell-LaPadula Model:

- **Definition**: A model focused on maintaining the confidentiality of information. نموذج يركز على الحفاظ على سرية المعلومات
- **Components**:

Simple Security Property: No read-up. خاصية الأمان البسيطة عدم القراءة لأعلى

Star Property: No write-down. خاصية النجم عدم الكتابة لأسفل

Strong Star Property: No read-up or write-down. خاصية النجم القوي عدم القراءة لأعلى أو الكتابة لأسفل

-Biba Model:

- **Definition**: A model focused on maintaining the integrity of information. نموذج يركز على الحفاظ على سلامة المعلومات
- **Components**:

Simple Integrity Property: No read-down. خاصية السلامة البسيطة عدم القراءة لأسفل

Star Integrity Property: No write-up. خاصية السلامة النجمية عدم الكتابة لأعلى

-Lipner Implementation:

- **Description**: Combines elements of both Bell-LaPadula and Biba models to enforce both confidentiality and integrity. يجمع بين عناصر من النموذجين لفرض كل من السرية والسلامة

2.2.2 Rule-Based Models

-Clark-Wilson Model:

- **Definition**: A model designed to ensure data integrity through well-formed transactions and separation of duties. نموذج مصمم لضمان سلامة البيانات من خلال المعاملات المكونة جيدًا وفصل الواجبات
- **Goals of Integrity**: Ensuring well-formed transactions, internal consistency, and external consistency. أهداف السلامة ضمان المعاملات المكونة جيدًا الاتساق الداخلي الاتساق الخارجي
- **Clark-Wilson Rules**: Separation of duties, well-formed transactions, and certification and enforcement rules. قواعد كلارك-ويلسون فصل الواجبات المعاملات المكونة جيدًا قواعد التصديق والإنفاذ

-Brewer-Nash Model:

- **Definition**: Also known as the Chinese Wall Model, it aims to prevent conflicts of interest by ensuring that access controls change dynamically based on user actions. يُعرف أيضًا

باسم نموذج الجدار الصيني، ويهدف إلى منع تضارب المصالح من خلال ضمان أن تتغير ضوابط الوصول ديناميكيًا بناءً على تصرفات المستخدمين

- **Components**: Company datasets, conflict of interest classes, and dynamic rules for access control. المكونات مجموعات بيانات الشركة، فئات تضارب المصالح، والقواعد الديناميكية لضوابط الوصول

-Graham-Denning Model:

- **Definition**: A model for securely managing the creation and deletion of subjects and objects in a computer system. نموذج لإدارة آمنة لإنشاء وحذف الموضوعات والكائنات في نظام الكمبيوتر

- **Components**: Eight primary protection rights (e.g., create object, delete object, read, write). ثمانية حقوق حماية رئيسية مثل إنشاء كائن حذف كائن قراءة كتابة.

-Harrison-Ruzzo-Ullman Model:

- **Definition**: A model that extends the Graham-Denning model by adding a set of rules for changing access rights. نموذج يوسع نموذج Graham-Denning من خلال إضافة مجموعة من القواعد لتغيير حقوق الوصول

- **Components**: Set of rules for creating, deleting, and modifying subjects and objects. مجموعة من القواعد لإنشاء وحذف وتعديل الموضوعات والكائنات

2.3 Security Frameworks

-ISO 27001:

- **Description**: A standard providing requirements for an information security management system (ISMS). معيار يوفر متطلبات نظام إدارة أمن المعلومات.

-ISO 27002:

- **Description**: Provides guidelines and best practices for initiating, implementing, maintaining, and improving information security management. يقدم إرشادات وأفضل الممارسات لبدء وتنفيذ وصيانة وتحسين إدارة أمن المعلومات

-NIST 800-53:

- **Description**: A catalog of security and privacy controls for federal information systems and organizations. كتالوج لضوابط الأمان والخصوصية لأنظمة المعلومات والمنظمات الفيدرالية

-COBIT:

- **Description**: A framework for developing, implementing, monitoring, and improving IT governance and management practices. إطار لتطوير وتنفيذ ومراقبة وتحسين ممارسات حوكمة وإدارة تقنية المعلومات

-ITIL:

- **Description**: A set of practices for IT service management that focuses on aligning IT services with the needs of business. مجموعة من الممارسات لإدارة خدمات تقنية المعلومات التي تركز على مواءمة خدمات تقنية المعلومات مع احتياجات العمل

-HIPAA:

- **Description**: The Health Insurance Portability and Accountability Act, which sets the standard for protecting sensitive patient data. قانون التأمين الصحي القابلية للنقل والمساءلة الذي يحدد المعيار لحماية البيانات الحساسة للمرضى

-SOX:

- **Description**: The Sarbanes-Oxley Act, which mandates strict reforms to improve financial disclosures and prevent accounting fraud. قانون ساربانيس أوكسلي الذي يفرض إصلاحات صارمة لتحسين الإفصاحات المالية ومنع الاحتيال المحاسبي

-FedRAMP:

- **Description**: The Federal Risk and Authorization Management Program, which provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. برنامج إدارة المخاطر والتفويض الفيدرالي الذي يوفر نهجًا موحدًا لتقييم الأمان والتفويض والمراقبة المستمرة للمنتجات والخدمات السحابية

-FISMA:

- **Description**: The Federal Information Security Management Act, which requires federal agencies to develop, document, and implement an information security and protection program. قانون إدارة أمن المعلومات الفيدرالي الذي يتطلب من الوكالات الفيدرالية تطوير وتوثيق وتنفيذ برنامج لحماية وأمن المعلومات

-Cyber Kill Chain:

- **Description**: A model developed by Lockheed Martin to describe the stages of a cyber

attack and help in understanding and defending against them. نموذج طورته شركة لوكهيد مارتن لوصف مراحل الهجوم السيبراني والمساعدة في فهمها والدفاع ضدها

Multiple Choice Questions

1. What does the Zachman Framework primarily focus on?

A. Risk Management

B. Enterprise Architecture

C. Network Security

D. Software Development

2. The Clark-Wilson model ensures data integrity through:

A. Confidentiality and privacy

B. Well-formed transactions and separation of duties

C. Access control and encryption

D. Monitoring and auditing

3. Which security model is also known as the Chinese Wall Model?

A. Bell-LaPadula

B. Biba

C. Clark-Wilson

D. Brewer-Nash

4. Which framework is used to align IT services with business needs?

A. COBIT

B. ITIL

C. ISO 27001

D. NIST 800-53

5. What is the main purpose of the Cyber Kill Chain model?

A. To improve financial disclosures

B. To describe the stages of a cyber attack

C. To implement IT governance practices

D. To protect patient data

Answers and Explanations

1. B.

The Zachman Framework provides a structured way of viewing and defining an enterprise's architecture. يوفر إطار زاكمان طريقة منظمة لعرض وتعريف هندسة المؤسسة.

2. B.

The Clark-Wilson model ensures data integrity through well-formed transactions and separation of duties. يضمن نموذج كلارك-ويلسون سلامة البيانات من خلال المعاملات المكونة جيدًا وفصل الواجبات.

3. D.

The Brewer-Nash model, also known as the Chinese Wall Model, aims to prevent conflicts of interest. يُعرف النموذج أيضًا باسم نموذج الجدار الصيني، ويهدف إلى منع تضارب المصالح.

4. B.

ITIL is a set of practices for IT service management that focuses on aligning IT services with the needs of business. هي مجموعة من الممارسات لإدارة خدمات تقنية المعلومات التي تركز على مواءمة خدمات تقنية المعلومات مع احتياجات العمل.

5. B.

The Cyber Kill Chain model describes the stages of a cyber attack to help in understanding and defending against them. يصف النموذج مراحل الهجوم السيبراني للمساعدة في فهمها والدفاع ضدها.

---

3. Select Controls Based Upon Systems Security Requirements

3.1 Evaluation Criteria

Definition: The standards and benchmarks used to assess the security controls and overall security posture of a system. المعايير والمعايير المستخدمة لتقييم الضوابط الأمنية والوضع الأمني العام للنظام

Certification: The process of evaluating and validating that a system meets specified security requirements. عملية تقييم والتحقق من أن النظام يلبي متطلبات الأمان المحددة

-TCSEC (Orange Book): Trusted Computer System Evaluation Criteria, focused on assessing the security of computer systems. معايير تقييم نظام الكمبيوتر الموثوق، تركز على تقييم أمان أنظمة الكمبيوتر

Levels:

- **D1** – Failed or Not Tested فشل أو لم يتم اختباره
- **C1** – Weak Protection Mechanisms آليات حماية ضعيفة
- **C2** – Strict Login Procedures إجراءات تسجيل دخول صارمة
- **B1** – Security Labels تسميات الأمان
- **B2** – Security Labels and Verification of No Covert Channels تسميات الأمان والتحقق من عدم وجود قنوات سرية
- **B3** – Security Labels, Verification of No Covert Channels, Stay Secure During Start-Up تسميات الأمان، والتحقق من عدم وجود قنوات سرية، والبقاء آمنًا أثناء بدء التشغيل

- **A1** – Verified Design and Tested تصميم تم التحقق منه واختباره

-ITSEC: Information Technology Security Evaluation Criteria, includes confidentiality and integrity. معايير تقييم أمان تقنية المعلومات، تشمل السرية والسلامة.

Levels:

- **E0** – Inadequate غير كاف
- **E1** – Minimal الحد الأدنى
- **E2** – Standard قياسي
- **E3** – Enhanced محسّن
- **E4** – High عالي
- **E5** – Very High عالي جدًا
- **E6** – Extreme متطرف

-Common Criteria: An international standard for computer security certification (ISO/IEC 15408). معيار دولي لشهادة أمان الكمبيوتر

-Evaluation Assurance Levels (EAL):

- **EAL1** – Functionally Tested اختبار وظيفي
- **EAL2** – Structurally Tested اختبار هيكلي
- **EAL3** – Methodically Tested and Checked اختبار منهجي وفحص
- **EAL4** – Methodically Designed, Tested, and Reviewed تصميم واختبار ومراجعة منهجية
- **EAL5** – Semi-Formally Designed and Tested تصميم واختبار شبه رسمي
- **EAL6** – Semi-Formally Verified, Designed, and Tested التحقق شبه الرسمي والتصميم والاختبار
- **EAL7** – Formally Verified, Designed, and Tested التحقق الرسمي والتصميم والاختبار

Multiple Choice Questions

1. What is the primary purpose of TCSEC (Orange Book)?

A. Evaluate financial systems

B. Assess the security of computer systems

C. Manage network traffic

D. Secure physical premises

2. Which level in ITSEC is considered the highest assurance?

A. E1

B. E4

C. E6

D. E7

3. Which of the following is NOT a component of Common Criteria?

A. Protection Profile

B. Target of Evaluation

C. Enterprise Continuum

D. Security Targets

4. What does EAL4 in Common Criteria signify?

A. Functionally Tested

B. Methodically Designed, Tested, and Reviewed

C. Semi-Formally Designed and Tested

D. Formally Verified, Designed, and Tested

5. What is the focus of ITSEC?

A. Confidentiality only

B. Confidentiality and integrity

C. Availability only

D. Financial accuracy

Answers and Explanations

1. B.

TCSEC (Orange Book) is focused on assessing the security of computer systems to ensure they meet specified security requirements.

يركز (الكتاب البرتقالي) على تقييم أمان أنظمة الكمبيوتر لضمان أنها تلبي متطلبات الأمان المحددة

2. C.

E6 is the highest assurance level in ITSEC, indicating extremely rigorous security evaluation.

هو أعلى مستوى تأكيد في ، مما يشير إلى تقييم أمني صارم للغاية

3. C.

Enterprise Continuum is a component of TOGAF, not Common Criteria. Common Criteria includes Protection Profile, Target of Evaluation, and Security Targets.

استمرارية المؤسسة هي أحد مكونات ، وليست من المعايير العامة. تشمل المعايير العامة ملف الحماية، وهدف التقييم، والأهداف الأمنية

4. B.

EAL4 in Common Criteria signifies that a system has been methodically designed, tested, and reviewed.

يشير في المعايير العامة إلى أن النظام قد تم تصميمه واختباره ومراجعته بطريقة منهجية

5. B.

ITSEC focuses on evaluating the confidentiality and integrity of information technology systems.

يركز على تقييم سرية وسلامة أنظمة تكنولوجيا المعلومات

---

4. Understand Security Capabilities of Information Systems

4.1 Memory Protection

Definition: Techniques to protect memory from unauthorized access and corruption. تقنيات لحماية الذاكرة من الوصول غير المصرح به والفساد.

Methods:

- **Access Control Lists (ACLs)**: Restrict access to memory regions based on user roles and permissions. قوائم التحكم في الوصول تقييد الوصول إلى مناطق الذاكرة بناءً على أدوار المستخدم والأذونات.
- **Data Execution Prevention (DEP)**: Prevents execution of code from non-executable memory regions. منع تنفيذ البيانات يمنع تنفيذ الكود من مناطق الذاكرة غير القابلة للتنفيذ.
- **Address Space Layout Randomization (ASLR)**: Randomizes memory addresses to make it difficult for attackers to predict where code will be loaded. عشوائية تخطيط مساحة العناوين يقوم بعشوائية عناوين الذاكرة لجعل من الصعب على المهاجمين التنبؤ بمكان تحميل الكود

4.2 Trusted Platform Module (TPM)

Definition: A hardware-based security feature that provides secure cryptographic operations. ميزة أمان تعتمد على الأجهزة توفر عمليات تشفير آمنة.

Capabilities:

- **Secure Generation and Storage of Cryptographic Keys**: Generates and stores

cryptographic keys in a secure environment. توليد وتخزين آمن للمفاتيح التشفيرية يولد ويخزن المفاتيح التشفيرية في بيئة آمنة

- **Remote Attestation**: Verifies the integrity of the system remotely. التحقق عن بعد التحقق من سلامة النظام عن بعد

- **Sealing and Binding**: Ensures that data can only be accessed if the system is in a specific state. الإغلاق والربط يضمن أن البيانات لا يمكن الوصول إليها إلا إذا كان النظام في حالة معينة

4.3 Encryption/Decryption

Definition: The process of converting plaintext into ciphertext (encryption) and converting ciphertext back into plaintext (decryption). عملية تحويل النص العادي إلى نص مشفر التشفير وتحويل النص المشفر مرة أخرى إلى نص عادي فك التشفير

Types:

- **Symmetric Encryption**: Uses the same key for encryption and decryption. التشفير المتماثل يستخدم نفس المفتاح للتشفير وفك التشفير

- **Asymmetric Encryption**: Uses a pair of keys, a public key for encryption and a private key for decryption. التشفير غير المتماثل يستخدم زوجًا من المفاتيح مفتاحًا عامًا للتشفير ومفتاحًا خاصًا لفك التشفير

Algorithms:

- **Symmetric**:

DES: Data Encryption Standard. معيار تشفير البيانات

AES: Advanced Encryption Standard. معيار التشفير المتقدم

- **Asymmetric**:

RSA: Rivest-Shamir-Adleman. ريفيست شامير عدلمان

ECC: Elliptic Curve

Multiple Choice Questions

1. What is the primary function of Access Control Lists (ACLs) in memory

protection?

A. To encrypt data

B. To restrict access based on roles and permissions

C. To execute code from non-executable regions

D. To randomize memory addresses

2. What does Data Execution Prevention (DEP) aim to prevent?

A. Unauthorized access to memory

B. Execution of code from non-executable memory regions

C. Memory address randomization

D. Generation of cryptographic keys

3. Which capability is provided by Trusted Platform Module (TPM)?

A. Sealing and binding

B. Access control

C. Data encryption

D. Memory randomization

4. Which type of encryption uses the same key for both encryption and decryption?

A. Asymmetric

B. Public key

C. Symmetric

D. Elliptic curve

5. What is a key feature of Address Space Layout Randomization (ASLR)?

A. Generates cryptographic keys

B. Verifies system integrity

C. Randomizes memory addresses

D. Encrypts data

Answers and Explanations

1. B.

Access Control Lists (ACLs) restrict access to memory regions based on user roles and permissions, ensuring that only authorized users can access specific areas of memory.

قوائم التحكم في الوصول تقييد الوصول إلى مناطق الذاكرة بناءً على أدوار المستخدم والأذونات، مما يضمن أن المستخدمين المصرح لهم فقط يمكنهم الوصول إلى مناطق معينة من الذاكرة.

2. B.

Data Execution Prevention (DEP) prevents the execution of code from non-executable memory regions, protecting systems from certain types of attacks.

منع تنفيذ البيانات يمنع تنفيذ الكود من مناطق الذاكرة غير القابلة للتنفيذ، مما يحمي الأنظمة من أنواع معينة من الهجمات.

3. A.

Trusted Platform Module (TPM) provides the capability of sealing and binding, ensuring that data can only be accessed if the system is in a specific state.

الإغلاق والربط يضمن أن البيانات لا يمكن الوصول إليها إلا إذا كان النظام في حالة معينة.

4. C.

Symmetric encryption uses the same key for both encryption and decryption, making it simpler but requiring secure key management.

التشفير المتماثل يستخدم نفس المفتاح للتشفير وفك التشفير، مما يجعله أبسط ولكنه يتطلب إدارة آمنة للمفاتيح.

5. C.

Address Space Layout Randomization (ASLR) randomizes memory addresses, making it difficult for attackers to predict where code will be loaded, enhancing system security.

عشوائية تخطيط مساحة العناوين يقوم بعشوائية عناوين الذاكرة، مما يجعل من الصعب على المهاجمين التنبؤ بمكان تحميل الكود، مما يعزز أمان النظام.

---

5. Assess and Mitigate the Vulnerabilities of Security Architectures, Designs, and Solution Elements

5.1 Client-Based Systems

Definition: Systems that rely on client devices for processing and data storage.
أنظمة تعتمد على أجهزة العميل للمعالجة وتخزين البيانات

Vulnerabilities:

- **Malware**: Malicious software that can compromise client systems. البرامج الضارة برامج خبيثة يمكن أن تعرض أنظمة العميل للخطر
- **Phishing**: Social engineering attacks that trick users into providing sensitive information. الهجمات الهندسية الاجتماعية التي تخدع المستخدمين لتقديم معلومات حساسة

Mitigation:

- **Antivirus Software**: Detect and remove malware. برنامج مكافحة الفيروسات اكتشاف وإزالة البرامج الضارة
- **User Education**: Train users to recognize phishing attempts. تدريب المستخدمين على التعرف على محاولات التصيد الاحتيالي

5.2 Server-Based Systems

Definition: Systems that rely on servers for processing and data storage. أنظمة تعتمد على الخوادم للمعالجة وتخزين البيانات

Vulnerabilities:

- **SQL Injection**: An attack that allows attackers to execute arbitrary SQL code. هجوم يسمح للمهاجمين بتنفيذ كود تعسفي
- **DDoS Attacks**: Distributed Denial of Service attacks that overwhelm servers with traffic. هجمات حجب الخدمة الموزعة التي تغمر الخوادم بحركة المرور

Mitigation:

- **Input Validation**: Ensure that all user inputs are validated before processing. ضمان التحقق من جميع مدخلات المستخدم قبل المعالجة
- **DDoS Mitigation Services**: Use services to detect and mitigate DDoS attacks. استخدام الخدمات لاكتشاف وتخفيف هجمات

5.3 Database Systems

Definition: Systems that store and manage data. أنظمة تخزن وتدير البيانات

Vulnerabilities:

- **Data Breaches**: Unauthorized access to sensitive data. الوصول غير المصرح به إلى البيانات الحساسة
- **SQL Injection**: An attack that allows attackers to execute arbitrary SQL code. هجوم يسمح للمهاجمين بتنفيذ كود تعسفي

Mitigation:

- **Encryption**: Encrypt sensitive data to protect it from unauthorized access. تشفير البيانات الحساسة لحمايتها من الوصول غير المصرح به
- **Access Controls**: Implement strong access controls to limit who can access the database. تنفيذ ضوابط وصول قوية لتحديد من يمكنه الوصول إلى قاعدة البيانات

5.4 Cryptographic Systems

Definition: Systems that use cryptographic methods to secure data. أنظمة تستخدم طرق التشفير لتأمين البيانات

Vulnerabilities:

- **Weak Algorithms**: Using outdated or weak cryptographic algorithms. استخدام الخوارزميات التشفيرية القديمة أو الضعيفة
- **Key Management**: Poor management of cryptographic keys. إدارة سيئة للمفاتيح التشفيرية

Mitigation:

- **Use Strong Algorithms**: Use modern and strong cryptographic algorithms. استخدام الخوارزميات التشفيرية الحديثة والقوية
- **Key Management Practices**: Implement best practices for key management. تنفيذ أفضل الممارسات لإدارة المفاتيح

5.5 Operational Technology/Industrial Control Systems (ICS)

Definition: Systems used to control industrial processes and operations. أنظمة تستخدم للتحكم في العمليات الصناعية والتشغيلية

Vulnerabilities:

- **Legacy Systems**: Older systems that may not have modern security features. أنظمة قديمة قد لا تحتوي على ميزات الأمان الحديثة
- **Physical Access**: Unauthorized physical access to control systems. الوصول الفيزيائي غير المصرح به إلى أنظمة التحكم

Mitigation:

- **Upgrade Systems**: Upgrade legacy systems with modern security features. ترقية الأنظمة القديمة بميزات الأمان الحديثة
- **Physical Security**: Implement strong physical security controls to protect systems. تنفيذ ضوابط أمان فيزيائية قوية لحماية الأنظمة

5.6 Cloud-Based Systems

5.6.1 Characteristics:

- **On-Demand Self Service**: Users can provision computing capabilities as needed automatically. يمكن للمستخدمين توفير قدرات الحوسبة حسب الحاجة تلقائيًا.
- **Broad Network Access**: Capabilities are available over the network and accessed through standard mechanisms. القدرات متاحة عبر الشبكة ويتم الوصول إليها من خلال آليات قياسية.
- **Resource Pooling**: Provider's computing resources are pooled to serve multiple consumers. يتم تجميع موارد الحوسبة لمقدم الخدمة لخدمة عدة مستهلكين.
- **Rapid Elasticity**: Capabilities can be rapidly and elastically provisioned to scale with demand. يمكن توفير القدرات بسرعة ومرونة لتتناسب مع الطلب.
- **Measured Service**: Resource usage can be monitored, controlled, and reported. يمكن مراقبة واستخدام الموارد والتحكم فيها والإبلاغ عنها

5.6.2 Service Models:

- **IaaS (Infrastructure as a Service)**: Provides virtualized computing resources over the internet. توفير موارد الحوسبة الافتراضية عبر الإنترنت.
- **PaaS (Platform as a Service)**: Provides a platform allowing customers to develop, run, and manage applications. توفير منصة تسمح للعملاء بتطوير وتشغيل وإدارة التطبيقات.
- **SaaS (Software as a Service)**: Provides software applications over the internet. توفير تطبيقات البرامج عبر الإنترنت

5.6.3 Deployment Models:

- **Public Cloud**: Services are delivered over the public internet and shared across multiple organizations. تقديم الخدمات عبر الإنترنت العام ومشاركتها بين عدة منظمات.
- **Private Cloud**: Services are maintained on a private network and used exclusively by one organization. تقديم الخدمات عبر شبكة خاصة وتستخدم حصريًا من قبل منظمة واحدة.
- **Community Cloud**: Services are shared by several organizations and support a specific community. تقديم الخدمات وتستخدم من قبل عدة منظمات وتدعم مجتمعًا معينًا.

- **Hybrid Cloud**: Combines public and private clouds, bound together by technology that allows data and applications to be shared between them. يجمع بين السحابة العامة والخاصة ويرتبط بتكنولوجيا تسمح بمشاركة البيانات والتطبيقات بينهما

5.6.4 Virtualized Compute:

- **Virtual Machine**: Emulates a computer system, providing the functionality of a physical computer. يحاكي نظام الكمبيوتر ويقدم وظيفة الكمبيوتر الفعلي

- **Containers**: Packages software and its dependencies into a single unit that can run anywhere. تغليف البرامج واعتمادياتها في وحدة واحدة يمكن تشغيلها في أي مكان

- **Serverless**: Allows developers to build and run applications without managing servers. يسمح للمطورين ببناء وتشغيل التطبيقات دون إدارة الخوادم

5.6.5 Identity Provider:

- **Local**: Managed within the organization. إدارة داخل المنظمة

- **Cloud**: Managed by a third-party cloud service. إدارة من قبل خدمة سحابية تابعة لجهة خارجية

5.6.6 Cloud Identity:

- **Linked**: Identities are linked between the local and cloud providers. ترتبط الهويات بين المزودين المحليين والسحابيين

- **Synced**: Identities are synchronized between the local and cloud providers. تتم مزامنة الهويات بين المزودين المحليين والسحابيين

- **Federated**: Identities are federated, allowing for single sign-on (SSO) across multiple systems. الفيدرالية تسمح بالوصول الموحد عبر أنظمة متعددة

5.6.7 Roles:

- **Accountable**:

-Cloud Consumer: Uses cloud services. المستهلك السحابي يستخدم خدمات السحابة

-**Owner**: Owns the data or application in the cloud. يمتلك البيانات أو التطبيق في السحابة

- **Responsible**:

-Controller: Manages the data within the cloud. يدير البيانات داخل السحابة

-Cloud Provider: Provides cloud services. يقدم خدمات السحابة

-Processor: Processes data on behalf of the controller. يعالج البيانات نيابة عن المتحكم

-Cloud Broker: Manages the use, performance, and delivery of cloud services. يدير استخدام وأداء وتسليم خدمات السحابة

-Cloud Auditor: Conducts independent assessments of cloud services. يجري تقييمات مستقلة لخدمات السحابة

5.6.8 Protocols:

- **SPML**: Service Provisioning Markup Language. لغة توصيف توفير الخدمة
- **SAML**: Security Assertion Markup Language. لغة توصيف تأكيد الأمان
- **OpenID**: An open standard for decentralized authentication. معيار مفتوح للمصادقة اللامركزية
- **OAuth**: Open standard for access delegation. معيار مفتوح لتفويض الوصول

5.6.9 Migration:

- **Data Centric**: Focuses on the secure migration of data to the cloud. يركز على نقل البيانات إلى السحابة بأمان

5.6.10 Forensics: Techniques and procedures for investigating cloud-based incidents. تقنيات وإجراءات التحقيق في الحوادث المستندة إلى السحابة

5.6.11 Data Destruction:

- **Snapshot, Virtual Disk, Image**: Methods for securely destroying data. طرق لتدمير البيانات بأمان
- **Crypto Shredding / Crypto Erase**: Uses cryptographic techniques to securely delete data. يستخدم تقنيات التشفير لحذف البيانات بأمان

5.7 Distributed Systems

Definition: Systems in which components located on networked computers communicate and coordinate their actions by passing messages. أنظمة تكون فيها المكونات الموجودة على أجهزة الكمبيوتر المتصلة بالشبكة تتواصل وتنسق أفعالها عن طريق تمرير الرسائل

Vulnerabilities:

- **Communication Failures**: Issues with network communication can disrupt system functionality. مشاكل الاتصال بالشبكة يمكن أن تعطل وظائف النظام
- **Inconsistent States**: Different parts of the system may have different views of the state of data. قد تكون لدى أجزاء مختلفة من النظام وجهات نظر مختلفة لحالة البيانات
-

Mitigation:

- **Redundant Communication Channels**: Implement multiple communication paths to ensure reliability. تنفيذ مسارات اتصال متعددة لضمان الموثوقية
- **Consistency Protocols**: Use protocols to ensure data consistency across the system. استخدام بروتوكولات لضمان اتساق البيانات عبر النظام

5.8 Internet of Things (IoT)

Definition: The network of physical objects that contain embedded technology to communicate and interact with their internal states or the external environment. شبكة من الكائنات الفيزيائية التي تحتوي على تقنية مدمجة للتواصل والتفاعل مع حالاتها

الداخلية أو البيئة الخارجية

Vulnerabilities:

- **Insecure Devices**: Many IoT devices have weak or no security features. العديد من أجهزة إنترنت الأشياء لديها ميزات أمان ضعيفة أو معدومة
- **Data Privacy**: Sensitive data can be exposed if not properly secured. يمكن أن تتعرض البيانات الحساسة إذا لم تكن مؤمنة بشكل صحيح

Mitigation:

- **Secure Device Management**: Implement strong authentication and encryption for device communication. تنفيذ المصادقة القوية والتشفير لتواصل الجهاز
- **Data Privacy Measures**: Use encryption and access controls to protect data. استخدام التشفير وضوابط الوصول لحماية البيانات

5.9 Microservices (e.g., API)

Definition: An architectural style that structures an application as a collection of loosely coupled services. أسلوب معماري ينظم التطبيق كمجموعة من الخدمات المترابطة بشكل فضفاض

Vulnerabilities:

- **API Security**: APIs can be targeted for attacks, leading to data breaches. يمكن استهداف واجهات برمجة التطبيقات للهجمات مما يؤدي إلى تسرب البيانات
- **Service Dependencies**: Interdependencies between services can lead to cascading failures. يمكن أن تؤدي التبعيات بين الخدمات إلى إخفاقات متتالية

Mitigation:

- **API Gateway**: Use an API gateway to manage and secure API traffic. استخدام بوابة لإدارة وتأمين حركة مرور
- **Resilience Engineering**: Design services to handle failures gracefully. تصميم الخدمات للتعامل مع الإخفاقات بشكل سلس

5.10 Containerization

Definition: A lightweight form of virtualization that packages an application and its dependencies into a single unit. شكل خفيف من الافتراضية يعبئ التطبيق واعتمادياته في وحدة واحدة

Vulnerabilities:

- **Isolation Issues**: Poor isolation between containers can lead to security breaches. العزل الضعيف بين الحاويات يمكن أن يؤدي إلى خروقات الأمان
- **Image Security**: Insecure container images can introduce vulnerabilities. يمكن أن تؤدي صور الحاويات غير الآمنة إلى إدخال ثغرات أمنية

Mitigation:

- **Strong Isolation**: Use container orchestration tools to ensure strong isolation. استخدام أدوات تنظيم الحاويات لضمان العزل القوي
- **Image Scanning**: Regularly scan container images for vulnerabilities. مسح صور الحاويات بانتظام للكشف عن الثغرات الأمنية

5.11 Serverless

Definition: A cloud computing model where the cloud provider manages the infrastructure and dynamically allocates resources. نموذج حوسبة سحابية حيث يدير مزود السحابة البنية التحتية ويخصص الموارد ديناميكيًا

Vulnerabilities:

- **Execution Environment**: Limited visibility into the execution environment can obscure security issues. الرؤية المحدودة في بيئة التنفيذ يمكن أن تخفي مشكلات الأمان
- **Function Overloading**: Overloaded functions can lead to performance and security issues. يمكن أن تؤدي الوظائف المحملة بشكل زائد إلى مشاكل في الأداء والأمان

Mitigation:

- **Monitoring**: Implement robust monitoring to track function execution. تنفيذ المراقبة القوية لتتبع تنفيذ الوظائف
- **Resource Management**: Use resource management tools to prevent function

overloading. استخدام أدوات إدارة الموارد لمنع تحميل الوظائف بشكل زائد

5.12 Embedded Systems

Definition: Special-purpose computer systems designed to perform dedicated functions within a larger system. أنظمة كمبيوتر مخصصة مصممة لأداء وظائف مخصصة ضمن نظام أكبر

Vulnerabilities:

- **Firmware Attacks**: Attacks targeting the firmware can compromise the system. الهجمات التي تستهدف البرامج الثابتة يمكن أن تعرض النظام للخطر
- **Insecure Interfaces**: Weak or unsecured interfaces can be exploited. الواجهات الضعيفة أو غير الآمنة يمكن استغلالها

Mitigation:

- **Firmware Updates**: Regularly update firmware to address vulnerabilities. تحديث البرامج الثابتة بانتظام لمعالجة الثغرات الأمنية
- **Secure Interfaces**: Implement secure communication protocols for interfaces. تنفيذ بروتوكولات الاتصال الآمنة للواجهات

5.13 High-Performance Computing Systems

Definition: Systems designed to provide high levels of computational power. أنظمة مصممة لتوفير مستويات عالية من القوة الحاسوبية

Vulnerabilities:

- **Resource Exhaustion**: High demand can lead to resource exhaustion and system crashes. الطلب العالي يمكن أن يؤدي إلى استنزاف الموارد وتعطل النظام
- **Parallel Execution Issues**: Bugs in parallel execution can lead to security vulnerabilities. الأخطاء في التنفيذ المتوازي يمكن أن تؤدي إلى ثغرات أمنية

Mitigation:

- **Resource Management**: Implement resource management strategies to prevent

exhaustion. تنفيذ استراتيجيات إدارة الموارد لمنع الاستنزاف

- **Parallel Execution Testing**: Regularly test parallel execution code for vulnerabilities. اختبار كود التنفيذ المتوازي بانتظام للكشف عن الثغرات الأمنية

5.14 Edge Computing Systems

Definition: Systems that process data at the edge of the network, close to the source of the data. أنظمة تعالج البيانات على حافة الشبكة بالقرب من مصدر البيانات

Vulnerabilities:

- **Physical Security**: Devices at the edge are more vulnerable to physical tampering. الأجهزة على الحافة أكثر عرضة للتلاعب الفيزيائي
- **Data Privacy**: Sensitive data processed at the edge can be exposed. يمكن أن تتعرض البيانات الحساسة المعالجة على الحافة للخطر

Mitigation:

- **Secure Enclosures**: Use secure enclosures to protect edge devices from tampering. استخدام أغلفة آمنة لحماية الأجهزة الطرفية من العبث
- **Data Encryption**: Encrypt data processed at the edge to protect privacy. تشفير البيانات المعالجة على الحافة لحماية الخصوصية

5.15 Virtualized Systems

Definition: Systems that use virtualization technology to create virtual versions of physical resources. أنظمة تستخدم تقنية الافتراضية لإنشاء نسخ افتراضية من الموارد الفيزيائية

Vulnerabilities:

- **Hypervisor Attacks**: Attacks targeting the hypervisor can compromise multiple virtual machines. الهجمات التي تستهدف المشرف الفائق يمكن أن تعرض عدة أجهزة افتراضية للخطر
- **Isolation Issues**: Poor isolation between virtual machines can lead to security breaches. العزل الضعيف بين الأجهزة الافتراضية يمكن أن يؤدي إلى خروقات الأمان

Mitigation:

- **Secure Hypervisors**: Use secure hypervisors and keep them updated. استخدام المشرفين الفائقين الآمنين والحفاظ على تحديثهم
- **Strong Isolation**: Ensure strong isolation between virtual machines. ضمان العزل القوي بين الأجهزة الافتراضية

5.16 Trusted Computing Base (TCB)

Definition: The totality of protection mechanisms within a computer system, including hardware, firmware, and software. مجموعة كاملة من آليات الحماية داخل نظام الكمبيوتر بما في ذلك الأجهزة والبرامج الثابتة والبرامج

Components:

- **Reference Monitor Concept**: Ensures that all access to system resources is authorized. مفهوم المراقب المرجعي يضمن أن جميع الوصول إلى موارد النظام مصرح به **Subject**: The active entity (e.g., user, process). الكيان النشط مثل المستخدم العملية **Mediation**: The process of checking access rights. عملية التحقق من حقوق الوصول **Object**: The passive entity (e.g., file, database). الكيان السلبي مثل الملف قاعدة البيانات **Rules**: Policies that define access controls. السياسات التي تحدد ضوابط الوصول **Logging & Monitoring**: Recording and analyzing access attempts. تسجيل وتحليل محاولات الوصول

Hardware Components:

- **Processor**: The central processing unit that executes instructions. المعالج وحدة المعالجة المركزية التي تنفذ التعليمات
- **Storage**: **Primary**: RAM and cache. التخزين الأساسي ذاكرة الوصول العشوائي وذاكرة التخزين المؤقت **Secondary**: Hard drives and SSDs. التخزين الثانوي محركات الأقراص الصلبة و SSD

Software Components:

- **System Kernel**: The core part of the operating system that manages system resources. النواة النظامية الجزء الأساسي من نظام التشغيل الذي يدير موارد النظام
- **Firmware**: Software that provides low-level control for the device's specific hardware. البرامج الثابتة برامج توفر تحكمًا منخفض المستوى في الأجهزة الخاصة بالجهاز
- **Middleware**: Software that provides common services and capabilities to applications.

البرمجيات الوسيطة برامج توفر خدمات وقدرات مشتركة للتطبيقات

Protection Mechanisms:

- **Operating System Modes**: **User Mode**: Limited access to system resources. وضع المستخدم الوصول المحدود إلى موارد النظام **Kernel Mode**: Full access to system resources. وضع النواة الوصول الكامل إلى موارد النظام
- **Ring Protection Model**: **Ring 3**: User programs. الحلقة 3 برامج المستخدم **Ring 0**: System kernel. الحلقة 0 نواة النظام
- **Secure Memory Management**: Techniques to protect memory from unauthorized access. تقنيات لحماية الذاكرة من الوصول غير المصرح به
- **Data Hiding**: Concealing data to prevent unauthorized access. إخفاء البيانات لمنع الوصول غير المصرح به
- **Defense in Depth**: Multiple layers of security controls. طبقات متعددة من الضوابط الأمنية
- **Memory Segmentation**: Dividing memory into segments to protect different types of data. تقسيم الذاكرة إلى مقاطع لحماية أنواع مختلفة من البيانات
- **Time Division Multiplexing**: Sharing a resource by dividing time into slots. مشاركة مورد عن طريق تقسيم الوقت إلى فترات زمنية
- **Problem States**: Different states of system operation. حالات النظام التشغيلية المختلفة
- **Supervisor States**: States in which the system has higher privileges. حالات المشرف التي يكون فيها النظام لديه امتيازات أعلى

Multiple Choice Questions

1. What is a common mitigation strategy for malware on client-based systems?

A. Input validation

B. Antivirus software

C. Data encryption

D. Secure hypervisors

2. Which attack involves overwhelming a server with traffic?

A. Phishing

B. SQL injection

C. DDoS attack

D. Side channel attack

3. What is the purpose of using encryption in database systems?

A. To increase processing speed

B. To protect sensitive data from unauthorized access

C. To enhance user experience

D. To improve data retrieval times

4. What is a key feature of Trusted Platform Module (TPM)?

A. Provides data randomization

B. Ensures secure key generation and storage

C. Monitors network traffic

D. Manages user access controls

5. What is the function of Address Space Layout Randomization (ASLR)?

A. To prevent code execution from non-executable memory regions

B. To randomize memory addresses

C. To control user access

D. To encrypt data

Answers and Explanations

1. B.

Antivirus software is a common mitigation strategy for malware on client-based systems, as it detects and removes malicious software.

برنامج مكافحة الفيروسات هو استراتيجية شائعة لتخفيف البرامج الضارة على الأنظمة المستندة إلى العميل، حيث يكتشف ويزيل البرامج الضارة.

2. C.

A DDoS attack involves overwhelming a server with traffic, causing it to become unavailable to legitimate users.

يتضمن هجوم إغراق الخادم بحركة المرور، مما يجعله غير متاح للمستخدمين الشرعيين.

3. B.

Encryption in database systems is used to protect sensitive data from unauthorized access, ensuring data confidentiality and security.

يتم استخدام التشفير في أنظمة قواعد البيانات لحماية البيانات الحساسة من الوصول غير المصرح به، مما يضمن سرية البيانات وأمانها.

4. B.

A key feature of Trusted Platform Module (TPM) is secure key generation and storage, providing a hardware-based method to protect cryptographic keys.

ميزة رئيسية لوحدة النظام الأساسي الموثوق بها هي توليد وتخزين المفاتيح بشكل آمن، مما يوفر طريقة تعتمد على الأجهزة لحماية المفاتيح التشفيرية.

5. B.

Address Space Layout Randomization (ASLR) randomizes memory addresses, making it difficult for attackers to predict where code will be loaded, thereby enhancing system security.

يقوم تخطيط مساحة العناوين العشوائي بعشوائية عناوين الذاكرة، مما يجعل من الصعب على المهاجمين التنبؤ بمكان تحميل الكود، وبالتالي يعزز أمان النظام

---

6. Select and Determine Cryptographic Solutions

6.1 Cryptographic Life Cycle

Definition: The stages through which cryptographic keys and algorithms pass, from creation to destruction. المراحل التي تمر بها المفاتيح والخوارزميات التشفيرية من الإنشاء إلى التدمير

Stages:

1. Key Generation: Creating cryptographic keys. توليد المفاتيح التشفيرية

Example: Using a random number generator to create a key for AES encryption. استخدام مولد أرقام عشوائي لإنشاء مفتاح لتشفير

2. Key Distribution: Distributing keys to users securely. توزيع المفاتيح للمستخدمين بأمان

Example: Using Diffie-Hellman key exchange to securely distribute keys over a public channel. استخدام تبادل المفاتيح لتوزيع المفاتيح بأمان عبر قناة عامة

3. Key Storage: Storing keys securely. تخزين المفاتيح بأمان

Example: Storing cryptographic keys in a Hardware Security Module (HSM). تخزين المفاتيح التشفيرية في وحدة أمان الأجهزة

4. Key Usage: Using keys for cryptographic operations. استخدام المفاتيح للعمليات التشفيرية

Example: Using a key to encrypt data for secure communication. استخدام مفتاح لتشفير البيانات للاتصال الآمن

5. Key Rotation: Regularly changing keys to maintain security. تغيير المفاتيح بانتظام للحفاظ على الأمان

Example: Rotating encryption keys every 90 days. تدوير مفاتيح التشفير كل 90 يومًا

6. Key Destruction: Securely destroying keys when no longer needed. تدمير المفاتيح بأمان عندما لم تعد هناك حاجة إليها

Example: Overwriting the key storage area with random data before deletion. الكتابة

فوق منطقة تخزين المفتاح ببيانات عشوائية قبل الحذف

6.2 Cryptographic Methods

-Symmetric Encryption:

- **Definition**: Uses the same key for both encryption and decryption. يستخدم نفس المفتاح للتشفير وفك التشفير
- **Algorithms**:

1. DES: Data Encryption Standard. معيار تشفير البيانات

Example: Encrypting a 64-bit block of data using a 56-bit key. تشفير كتلة بيانات 64 بت باستخدام مفتاح 56 بت

2. 3DES: Triple Data Encryption Standard. معيار التشفير الثلاثي للبيانات

Example: Applying DES encryption three times with different keys for added security. تطبيق تشفير ثلاث مرات بمفاتيح مختلفة لزيادة الأمان

3. AES: Advanced Encryption Standard. معيار التشفير المتقدم

Example: Encrypting data with a 128-bit, 192-bit, or 256-bit key. تشفير البيانات بمفتاح 128 بت أو 192 بت أو 256 بت

4. CAST-128

5. SAFER

6. Blowfish

7. Twofish

8. RC5/RC6

-Asymmetric Encryption:

• **Definition:** Uses a pair of keys, one for encryption and one for decryption. يستخدم زوجًا من المفاتيح واحد للتشفير والآخر لفك التشفير

• **Algorithms:**

1. RSA: Rivest-Shamir-Adleman. ريفيست شامير عدلمان

Example: Encrypting data with a public key and decrypting it with a private key. تشفير البيانات بمفتاح عام وفك تشفيرها بمفتاح خاص

2. Diffie-Hellmann: Key exchange protocol. بروتوكول تبادل المفاتيح

Example: Securely exchanging cryptographic keys over a public channel. تبادل المفاتيح التشفيرية بأمان عبر قناة عامة

3. Elliptic Curve (ECC): Uses elliptic curve mathematics. يستخدم الرياضيات المنحنية البيضاوية

Example: Encrypting data with shorter keys while maintaining high security. تشفير البيانات بمفاتيح أقصر مع الحفاظ على الأمان العالي

4. El Gamal

5. DSA: Digital Signature Algorithm. خوارزمية التوقيع الرقمي

Example: Signing a message to ensure its authenticity and integrity. توقيع رسالة لضمان أصالتها وسلامتها

-Digital Certificates:

- **Definition**: Electronic documents used to prove the ownership of a public key. وثائق إلكترونية تستخدم لإثبات ملكية مفتاح عام

-Digital Signatures:

- **Definition**: Provide authenticity, integrity, and non-repudiation for electronic messages. توفير الأصالة والنزاهة وعدم الإنكار للرسائل الإلكترونية

-Substitution:

- **Caesar Cipher**: A substitution cipher where each letter is shifted a certain number of

places. تشفير قيصر شفرة الاستبدال حيث يتم تحريك كل حرف عددًا معينًا من الأماكن

- **Monoalphabetic**: Uses a single substitution alphabet. يستخدم أبجدية استبدال واحدة
- **Polyalphabetic**: Uses multiple substitution alphabets. يستخدم عدة أبجديات استبدال
- **Running**: Uses a running key from a predetermined text. يستخدم مفتاح تشغيل من نص محدد مسبقًا
- **One-Time Pads**: Uses a single-use key that is as long as the message. يستخدم مفتاح استخدام واحد بطول الرسالة

-Transposition:

- **Spartan Scytale**: Uses a cylinder and a strip of leather to encrypt messages. يستخدم أسطوانة وشريطًا جلديًا لتشفير الرسائل
- **Rail Fence (Zigzag)**: Writes the message in a zigzag pattern. يكتب الرسالة في نمط متعرج

6.3 Public Key Infrastructure (PKI)

Definition: A system for the creation, storage, and distribution of digital certificates and public keys. نظام لإنشاء وتخزين وتوزيع الشهادات الرقمية والمفاتيح العامة.

Components:

1. **Certificate Authority (CA)**: Issues and verifies digital certificates. يصدر ويحقق في الشهادات الرقمية ***Example:*** Verisign providing a digital certificate to a website. Verisign تقدم شهادة رقمية لموقع ويب
2. **Registration Authority (RA)**: Verifies the identity of entities requesting certificates. يتحقق من هوية الكيانات التي تطلب الشهادات ***Example:*** An RA validating the identity of a company before issuing a certificate. تحقق من هوية شركة قبل إصدار الشهادة
3. **Certificate Database**: Stores issued certificates and their statuses. يخزن الشهادات الصادرة وحالاتها ***Example:*** A database tracking the expiration dates of digital certificates. قاعدة بيانات تتبع تواريخ انتهاء الشهادات الرقمية
4. **Certificate Store**: Local storage of certificates on a device. تخزين الشهادات المحلية على جهاز

Example: Storing a digital certificate in a browser's certificate store. تخزين شهادة رقمية في مخزن الشهادات في المتصفح

6.4 Key Management Practices

Definition: Practices for securely handling cryptographic keys throughout their lifecycle. ممارسات للتعامل بأمان مع المفاتيح التشفيرية طوال دورة حياتها

Practices:

1. **Key Generation**: Securely generating cryptographic keys. توليد المفاتيح التشفيرية بأمان ***Example:*** Using a hardware random number generator for key creation. استخدام مولد أرقام عشوائي للأجهزة لإنشاء المفتاح

2. **Key Distribution**: Securely distributing keys to intended recipients. توزيع المفاتيح بأمان للمستلمين المقصودين ***Example:*** Sending keys through an encrypted email. إرسال المفاتيح عبر بريد إلكتروني مشفر

3. **Key Storage**: Storing keys in secure environments. تخزين المفاتيح في بيئات آمنة ***Example:*** Using an HSM to store keys securely. استخدام وحدة أمان الأجهزة لتخزين المفاتيح بأمان

4. **Key Rotation**: Regularly updating keys to maintain security. تحديث المفاتيح بانتظام للحفاظ على الأمان **Example**: Changing encryption keys every 90 days. تغيير مفاتيح التشفير كل 90 يومًا

5. **Key Destruction**: Securely destroying keys when no longer needed. تدمير المفاتيح بأمان عندما لم تعد هناك حاجة إليها **Example**: Overwriting keys with random data before deletion. الكتابة فوق المفاتيح ببيانات عشوائية قبل الحذف

6.5 Digital Signatures and Digital Certificates

Digital Signatures:

- **Definition**: Provide authenticity, integrity, and non-repudiation for electronic messages. توفير الأصالة والنزاهة وعدم الإنكار للرسائل الإلكترونية

Example: Signing an email with a digital signature to ensure the recipient knows it is authentic. توقيع بريد إلكتروني بتوقيع رقمي لضمان أن المستلم يعرف أنه أصلي

Digital Certificates:

- **Definition**: Electronic documents used to prove the ownership of a public key. وثائق إلكترونية تستخدم لإثبات ملكية مفتاح عام

Example: Using an SSL certificate to establish a secure connection between a web server and a browser. استخدام شهادة لإنشاء اتصال آمن بين خادم ويب ومتصفح

6.6 Cryptographic Services

Definition: Services that use cryptographic methods to ensure the security of information. الخدمات التي تستخدم طرق التشفير لضمان أمان المعلومات

Services:

1. **Confidentiality**: Ensuring that information is only accessible to those authorized to view it. ضمان أن المعلومات يمكن الوصول إليها فقط من قبل الأشخاص المخولين ***Example:*** Encrypting emails to prevent unauthorized access. تشفير رسائل البريد الإلكتروني لمنع الوصول غير المصرح به

2. **Integrity**: Ensuring that information has not been altered. ضمان عدم تغيير المعلومات ***Example:*** Using hash functions to verify file integrity. استخدام وظائف التجزئة للتحقق من سلامة الملفات

3. **Authenticity**: Verifying the identity of a user or system. التحقق من هوية المستخدم أو النظام ***Example:*** Using digital signatures to authenticate users. استخدام التوقيعات الرقمية لمصادقة المستخدمين

4. **Non-Repudiation**: Ensuring that a user cannot deny having performed a particular action. ضمان أن المستخدم لا يمكنه إنكار القيام بإجراء معين ***Example:*** Digital signatures providing proof of the sender's identity and action. التوقيعات الرقمية توفر دليلًا على هوية المرسل والإجراء

5. **Access Control**: Restricting access to information based on user roles. تقييد الوصول إلى المعلومات بناءً على أدوار المستخدمين ***Example:*** Implementing role-based access control in a database. تنفيذ التحكم في الوصول المستند إلى الدور في قاعدة البيانات

6. **Origin**: Verifying the origin of a message or data. التحقق من أصل الرسالة أو البيانات ***Example:*** Ensuring an email is from the claimed sender using SPF records. ضمان أن البريد الإلكتروني من المرسل المزعوم باستخدام سجلات

7. **Delivery**: Ensuring that information is delivered to the correct recipient. ضمان تسليم المعلومات إلى المستلم الصحيح ***Example:*** Encrypting messages to ensure they are only

readable by the intended recipient. تشفير الرسائل لضمان قراءتها فقط من قبل المستلم المقصود

6.7 Cryptographic Terminology

- **Plaintext**: The original unencrypted data. النص العادي البيانات الأصلية غير المشفرة
- **Encrypt**: Converting plaintext into ciphertext. تحويل النص العادي إلى نص مشفر
- **Key / Crypto Variable**: The secret value used in the encryption and decryption process. القيمة السرية المستخدمة في عملية التشفير وفك التشفير
- **Decrypt**: Converting ciphertext back into plaintext. تحويل النص المشفر مرة أخرى إلى نص عادي
- **Key Clustering**: When two different keys produce the same ciphertext from the same plaintext. عندما تنتج مفتاحان مختلفان نفس النص المشفر من نفس النص العادي
- **Work Factor**: The estimated time and resources needed to break a cryptographic algorithm. الوقت والموارد المقدرة اللازمة لكسر خوارزمية التشفير
- **Initialization Vector / Nonce**: A random value used to ensure that the same plaintext encrypts to different ciphertexts. قيمة عشوائية تستخدم لضمان أن نفس النص العادي يتم تشفيره إلى نصوص مشفرة مختلفة
- **Confusion**: Making the relationship between the key and ciphertext as complex as possible. جعل العلاقة بين المفتاح والنص المشفر معقدة قدر الإمكان
- **Diffusion**: Spreading the plaintext characters over the ciphertext to hide patterns. نشر أحرف النص العادي عبر النص المشفر لإخفاء الأنماط
- **Avalanche**: A small change in the plaintext or key should result in a significant change in the ciphertext. يجب أن يؤدي تغيير صغير في النص العادي أو المفتاح إلى تغيير كبير في النص المشفر

6.8 Secret Writing

Hidden:

• Steganography: Hiding information within other non-secret text or data. إخفاء

المعلومات داخل نصوص أو بيانات غير سرية أخرى

• Null Cipher: Hiding the plaintext within a larger non-secret text. إخفاء النص العادي داخل نص غير سري أكبر

Scrambled (Cryptography):

• **One-Way:**

o Hashing: Converting data into a fixed-size string of characters. تحويل البيانات إلى سلسلة أحرف بحجم ثابت

o MD5: Message Digest Algorithm 5. خوارزمية التجزئة

o SHA-1: Secure Hash Algorithm 1. 1 خوارزمية التجزئة الآمنة

o SHA-2: Secure Hash Algorithm 2. 2 خوارزمية التجزئة الآمنة

o SHA-3: Secure Hash Algorithm 3. 3 خوارزمية التجزئة الآمنة

• **Two-Way:**

o Symmetric:

 DES: Data Encryption Standard. معيار تشفير البيانات

 3DES: Triple Data Encryption Standard. معيار التشفير الثلاثي للبيانات

 AES: Advanced Encryption Standard. معيار التشفير المتقدم

 CAST-128

 SAFER

 Blowfish

 Twofish

 RC5/RC6

o Asymmetric:

 RSA: Rivest-Shamir-Adleman. ريفيست شامير عدلمان

 Diffie-Hellmann: Key exchange protocol. بروتوكول تبادل المفاتيح

 Elliptic Curve (ECC): Uses elliptic curve mathematics. يستخدم الرياضيات المنحنية البيضاوية

 El Gamal

 DSA: Digital Signature Algorithm. خوارزمية التوقيع الرقمي

Digital Certificates:

• Electronic documents used to prove the ownership of a public key. وثائق إلكترونية تستخدم لإثبات ملكية مفتاح عام

Digital Signatures:

• Provide authenticity, integrity, and non-repudiation of electronic messages. توفير الأصالة والنزاهة وعدم الإنكار للرسائل الإلكترونية

Substitution:

• *Caesar Cipher:* A substitution cipher where each letter is shifted a certain number of places. تشفير قيصر شفرة الاستبدال حيث يتم تحريك كل حرف عددًا معينًا من الأماكن

• *Monoalphabetic:* Uses a single substitution alphabet. يستخدم أبجدية استبدال واحدة

• *Polyalphabetic:* Uses multiple substitution alphabets. يستخدم عدة أبجديات استبدال

• *Running:* Uses a running key from a predetermined text. يستخدم مفتاح تشغيل من نص محدد مسبقًا

• *One-Time Pads:* Uses a single-use key that is as long as the message. يستخدم مفتاح استخدام واحد بطول الرسالة

Transposition:

• *Spartan Scytale:* Uses a cylinder and a strip of leather to encrypt messages. يستخدم

أسطوانة وشريطًا جلديًا لتشفير الرسائل

• *Rail Fence (Zigzag):* Writes the message in a zigzag pattern. يكتب الرسالة في نمط متعرج

Multiple Choice Questions

1. What is the purpose of key rotation in the cryptographic life cycle?

A. To encrypt data

B. To update keys regularly for maintaining security

C. To store keys securely

D. To destroy keys when no longer needed

2. Which algorithm is used in symmetric encryption?

A. RSA

B. Diffie-Hellmann

C. DES

D. DSA

3. What is a function of the Certificate Authority (CA) in PKI?

A. Generating keys

B. Encrypting data

C. Issuing and verifying digital certificates

D. Storing certificates

4. Which of the following ensures non-repudiation in electronic messages?

A. Symmetric encryption

B. Digital certificates

C. Hashing

D. Digital signatures

5. What does a one-time pad provide in cryptography?

A. A fixed-size hash

B. A single-use key as long as the message

C. A substitution cipher

D. A transposition cipher

Answers and Explanations

1. B.

Key rotation involves regularly updating keys to maintain security, ensuring that old keys do not compromise the system if they are exposed.

يتضمن تغيير المفاتيح تحديث المفاتيح بانتظام للحفاظ على الأمان، مما يضمن أن المفاتيح القديمة لا تعرض النظام للخطر إذا تم كشفها.

2. C.

DES (Data Encryption Standard) is an algorithm used in symmetric encryption, where the same key is used for both encryption and decryption.

هو خوارزمية تستخدم في التشفير المتماثل، حيث يتم استخدام نفس (معيار تشفير البيانات) المفتاح لكل من التشفير وفك التشفير.

3. C.

The Certificate Authority (CA) in PKI is responsible for issuing and verifying digital certificates, ensuring the authenticity of public keys.

السلطة المصادقة في البنية التحتية للمفتاح العام مسؤولة عن إصدار والتحقق من الشهادات

الرقمية، وضمان أصالة المفاتيح العامة.

4. D.

Digital signatures provide non-repudiation in electronic messages, ensuring that the sender cannot deny having sent the message.

التوقيعات الرقمية توفر عدم الإنكار في الرسائل الإلكترونية، مما يضمن أن المرسل لا يمكنه إنكار إرسال الرسالة.

5. B.

A one-time pad provides a single-use key that is as long as the message, ensuring that the encryption is theoretically unbreakable.

يوفر مفتاح الاستخدام الواحد مفتاحًا للاستخدام الفردي بطول الرسالة، مما يضمن أن التشفير لا يمكن كسره نظريًا

---

7. Understand Methods of Cryptanalytic Attacks

7.1 Cryptanalytic Attacks

Brute Force:

- **Definition**: Trying all possible keys until the correct one is found. محاولة جميع المفاتيح الممكنة حتى يتم العثور على المفتاح الصحيح

Example: Attempting every possible key combination to decrypt a message. محاولة كل تركيبة مفتاح ممكنة لفك تشفير رسالة

Ciphertext Only:

- **Definition**: Attacking based on the analysis of ciphertexts. الهجوم بناءً على تحليل النصوص المشفرة

Example: Analyzing patterns in intercepted encrypted messages to decipher them. تحليل الأنماط في الرسائل المشفرة المعترضة لفك تشفيرها

Known Plaintext:

- **Definition**: Using known plaintext and its corresponding ciphertext to find the key. استخدام النص العادي المعروف والنص المشفر المقابل له للعثور على المفتاح

Example: If the plaintext "HELLO" and its ciphertext are known, using them to find the encryption key. إذا كان النص العادي ونصه المشفر معروفين ، استخدمهما للعثور على مفتاح التشفير

Chosen Plaintext:

- **Definition**: Choosing plaintexts to be encrypted and analyzing the ciphertexts. اختيار النصوص العادية لتشفيرها وتحليل النصوص المشفرة

Example: An attacker sends chosen plaintext to be encrypted and then analyzes the resulting ciphertext. يرسل المهاجم النص العادي المختار ليتم تشفيره ثم يحلل النص المشفر الناتج

Chosen Ciphertext:

- **Definition**: Choosing ciphertexts to be decrypted and analyzing the resulting plaintexts. اختيار النصوص المشفرة لفك تشفيرها وتحليل النصوص العادية الناتجة

Example: An attacker chooses specific ciphertexts, has them decrypted, and studies the resulting plaintexts. يختار المهاجم نصوصًا مشفرة محددة ، ويفك تشفيرها ، ويدرس النصوص العادية الناتجة

Linear & Differential:

- **Definition**: Statistical methods used to attack block ciphers. طرق إحصائية تستخدم للهجوم على الشفرات الكتلية

Example: Using differential cryptanalysis to find differences in the encryption process. استخدام التحليل التفاضلي للعثور على اختلافات في عملية التشفير

Factoring:

- **Definition**: Breaking cryptographic keys based on the difficulty of factoring large numbers. كسر المفاتيح التشفيرية بناءً على صعوبة تحليل الأعداد الكبيرة

Example: Factoring the product of two large prime numbers used in RSA encryption. تحليل ناتج ضرب عددين أوليين كبيرين مستخدمين في تشفي.

7.2 Cryptographic Attacks

Man-in-the-Middle:

- **Definition**: Intercepting communication between two parties and altering it. اعتراض الاتصالات بين طرفين وتغييرها

Example: Intercepting and modifying messages between two communicating parties. اعتراض الرسائل وتعديلها بين طرفين متواصلين

Replay:

- **Definition**: Reusing a valid data transmission to fraudulently repeat or delay the transmission. إعادة استخدام نقل البيانات الصالح لتكرار النقل أو تأخيره بشكل احتيالي.

Example: Capturing a login request and replaying it to gain unauthorized access. التقاط طلب تسجيل الدخول وإعادة تشغيله للحصول على وصول غير مصرح به

Pass the Hash:

- **Definition**: Using hashed credentials to authenticate without knowing the actual password. استخدام بيانات الاعتماد المشفرة للمصادقة دون معرفة كلمة المرور الفعلية.

Example: Capturing a hashed password and using it to authenticate to a system. التقاط كلمة مرور مشفرة واستخدامها للمصادقة على نظام

Temporary Files:

- **Definition**: Exploiting temporary files that may contain sensitive data. استغلال الملفات المؤقتة التي قد تحتوي على بيانات حساسة

Example: Recovering sensitive data from temporary files created by applications. استرداد البيانات الحساسة من الملفات المؤقتة التي أنشأتها التطبيقات

Implementation:

- **Definition**: Attacks targeting the implementation of cryptographic algorithms. الهجمات التي تستهدف تنفيذ الخوارزميات التشفيرية

Example: Exploiting weaknesses in the implementation of an encryption algorithm. استغلال نقاط الضعف في تنفيذ خوارزمية التشفير

Side Channel:

- **Power**: Analyzing power consumption patterns. تحليل أنماط استهلاك الطاقة

Example: Measuring power consumption during encryption to deduce keys. قياس استهلاك الطاقة أثناء التشفير لاستخلاص المفاتيح

- **Timing**: Analyzing the time taken to execute cryptographic algorithms. تحليل الوقت المستغرق لتنفيذ الخوارزميات التشفيرية

Example: Observing time variations to find cryptographic keys. مراقبة التباين في الوقت للعثور على المفاتيح التشفيرية

- **Radiation Emissions**: Analyzing electromagnetic emissions. تحليل الانبعاثات الكهرومغناطيسية

Example: Capturing electromagnetic emissions to extract keys. التقاط الانبعاثات الكهرومغناطيسية لاستخراج المفاتيح

Dictionary Attack:

- **Definition**: Trying a list of commonly used passwords. محاولة قائمة من كلمات المرور الشائعة الاستخدام

Example: Using a dictionary of common passwords to guess a user's password. استخدام قاموس لكلمات المرور الشائعة لتخمين كلمة مرور المستخدم

Rainbow Tables:

- **Definition**: Using precomputed hash chains to reverse cryptographic hashes. استخدام سلاسل التجزئة المحسوبة مسبقًا لعكس التجزئة التشفيرية

Example: Using a rainbow table to find the original password from its hash. استخدام جدول قوس قزح للعثور على كلمة المرور الأصلية من تجزئتها

Birthday Attack:

- **Definition**: Exploiting the birthday paradox to find hash collisions. استغلال مفارقة عيد الميلاد للعثور على تصادمات التجزئة

Example: Finding two different inputs that produce the same hash value. العثور على مدخلين مختلفين ينتجان نفس قيمة التجزئة

Social Engineering:

- **Definition**: Manipulating individuals to gain unauthorized access. التلاعب بالأفراد للحصول على الوصول غير المصرح به

Example: Convincing an employee to reveal their password over the phone. إقناع موظف بالكشف عن كلمة المرور الخاصة به عبر الهاتف

Purchase Key:

- **Definition**: Buying cryptographic keys from individuals or organizations. شراء المفاتيح التشفيرية من الأفراد أو المنظمات

Example: Paying for stolen cryptographic keys on the dark web. الدفع مقابل المفاتيح التشفيرية المسروقة على الويب المظلم

Rubber Hose:

- **Definition**: Physically coercing someone to disclose cryptographic keys. إكراه شخص ماديًا للكشف عن المفاتيح التشفيرية

Example: Forcing an individual to reveal their encryption keys under threat. إجبار شخص على الكشف عن مفاتيحه التشفيرية تحت التهديد

Multiple Choice Questions

1. What is the primary goal of a brute force attack?

A. To analyze ciphertexts

B. To try all possible keys until the correct one is found

C. To reuse valid data transmissions

D. To manipulate individuals for unauthorized access

2. Which type of attack involves intercepting communication between two parties and altering it?

A. Replay

B. Pass the Hash

C. Man-in-the-Middle

D. Dictionary Attack

3. What is a side channel attack?

A. Analyzing power consumption patterns

B. Reusing valid data transmissions

C. Trying all possible keys

D. Buying cryptographic keys

4. Which attack exploits temporary files that may contain sensitive data?

A. Rainbow Tables

B. Temporary Files

C. Brute Force

D. Social Engineering

5. What is the focus of a birthday attack?

A. Finding hash collisions

B. Intercepting communications

C. Reusing valid data transmissions

D. Analyzing timing patterns

Answers and Explanations

1. B.

The primary goal of a brute force attack is to try all possible keys until the correct one is found, eventually breaking the encryption.

الهدف الأساسي لهجوم القوة الغاشمة هو محاولة جميع المفاتيح الممكنة حتى يتم العثور على المفتاح الصحيح، مما يؤدي في النهاية إلى كسر التشفير.

2. C.

A Man-in-the-Middle attack involves intercepting communication between two parties and altering it, potentially compromising the integrity and confidentiality of the communication.

هجوم الرجل في المنتصف يتضمن اعتراض الاتصالات بين طرفين وتغييرها، مما قد يعرض سلامة وسرية الاتصال للخطر.

3. A.

A side channel attack involves analyzing indirect information such as power consumption patterns to extract cryptographic keys or other sensitive information.

يتضمن هجوم القناة الجانبية تحليل المعلومات غير المباشرة مثل أنماط استهلاك الطاقة لاستخراج المفاتيح التشفيرية أو المعلومات الحساسة الأخرى.

4. B.

Temporary files attacks exploit temporary files that may contain sensitive data, potentially exposing confidential information if not properly managed.

هجمات الملفات المؤقتة تستغل الملفات المؤقتة التي قد تحتوي على بيانات حساسة، مما قد يعرض المعلومات السرية للخطر إذا لم تتم إدارتها بشكل صحيح.

5. A.

A birthday attack focuses on finding hash collisions, exploiting the mathematical principle that collisions are more likely than one might intuitively expect.

يركز هجوم عيد الميلاد على العثور على تصادمات التجزئة، مستغلاً المبدأ الرياضي أن التصادمات أكثر احتمالية مما قد يتوقعه المرء.

---

8. Apply Security Principles to Site and Facility Design

8.1 Safety of People

- **Definition:** Ensuring the physical safety of personnel. ضمان السلامة الفيزيائية للأفراد
- **Measures:**

1. Emergency Exits: Clearly marked and accessible exits. مخارج الطوارئ المحددة بوضوح والمتاحة

Example: Regularly inspecting emergency exits to ensure they are not blocked. فحص مخارج الطوارئ بانتظام للتأكد من عدم انسدادها

2. Fire Drills: Regularly conducted fire drills. تمارين الحريق التي يتم إجراؤها بانتظام

Example: Conducting fire drills every six months to ensure everyone knows the evacuation procedure. إجراء تمارين الحريق كل ستة أشهر لضمان معرفة الجميع بإجراءات الإخلاء

3. First Aid Kits: Easily accessible first aid kits. حقائب الإسعافات الأولية المتاحة بسهولة

Example: Ensuring that first aid kits are fully stocked and accessible in multiple locations. التأكد من أن حقائب الإسعافات الأولية مليئة ومتاحة في مواقع متعددة

8.2 Layered Defense

- **Definition:** Implementing multiple layers of security controls. تنفيذ طبقات متعددة من الضوابط الأمنية
- **Layers:**

1. Perimeter Security: First layer of defense, includes fences, walls, and gates. الأمن المحيطي الطبقة الأولى من الدفاع تشمل الأسوار والجدران والبوا

Example: Installing a tall fence with barbed wire around the facility. تركيب سياج عالٍ بأسلاك شائكة حول المنشأة

2. Internal Security: Security within the facility, includes security guards and surveillance. الأمن الداخلي الأمان داخل المنشأة يشمل الحراس الأمنيين والمراقبة

Example: Employing security guards to patrol the premises and monitor surveillance cameras. توظيف حراس أمنيين لدوريات على المبنى ومراقبة كاميرات المراقبة

3. Data Security: Protecting data through encryption and access controls. أمان البيانات حماية البيانات من خلال التشفير وضوابط الوصول

Example: Encrypting sensitive data stored on servers and restricting access to authorized personnel. تشفير البيانات الحساسة المخزنة على الخوادم وتقييد الوصول إلى الموظفين المصرح لهم

8.3 Categories of Controls

1. Deter: Measures to discourage attacks (e.g., warning signs). تدابير لردع الهجمات مثل

علامات التحذير

Example: Placing visible security cameras to deter potential intruders. وضع كاميرات أمنية مرئية لردع المتسللين المحتملين

2. Delay: Measures to slow down attackers (e.g., locks, barriers). تدابير لتأخير المهاجمين مثل الأقفال والحواجز

Example: Installing strong locks on doors to delay unauthorized access. تركيب أقفال قوية على الأبواب لتأخير الوصول غير المصرح به

3. Detect: Measures to identify attacks (e.g., alarms, sensors). تدابير لتحديد الهجمات مثل الإنذارات وأجهزة الاستشعار

Example: Using motion sensors to detect unauthorized movement within the facility. استخدام أجهزة استشعار الحركة للكشف عن الحركة غير المصرح بها داخل المنشأة

4. Assess: Measures to evaluate the nature of the attack (e.g., CCTV). تدابير لتقييم طبيعة الهجوم مثل الكاميرات

Example: Monitoring CCTV footage to assess the nature and extent of a security breach. مراقبة لقطات الكاميرات لتقييم طبيعة ونطاق خرق أمني

5. Respond: Measures to address the attack (e.g., security personnel). تدابير لمعالجة الهجوم مثل الأفراد الأمنيين

Example: Deploying security personnel to respond to an active security incident. نشر أفراد الأمن للاستجابة لحادث أمني نشط

8.4 Perimeter

1. Landscape: Designing the landscape to enhance security. تصميم المناظر الطبيعية لتعزيز الأمان

Example: Using thorny bushes under windows to deter entry. استخدام الشجيرات الشائكة تحت النوافذ لردع الدخول

2. Grading: Adjusting the terrain to prevent unauthorized access. تعديل التضاريس لمنع الوصول غير المصرح به

Example: Creating steep embankments around the facility. إنشاء ضفاف شديدة الانحدار حول المنشأة

3. Mechanical:

• **Locks:** Using secure locks to prevent unauthorized access. استخدام الأقفال الآمنة لمنع الوصول غير المصرح به

Example: Installing high-security locks on all external doors. تركيب أقفال عالية الأمان على جميع الأبواب الخارجية

• **Doors / Mantraps:** Installing secure doors and mantraps. تركيب الأبواب الآمنة والفخاخ

Example: Using mantraps to control access to sensitive areas. استخدام الفخاخ للتحكم في الوصول إلى المناطق الحساسة

• **Windows:** Using secure windows to prevent unauthorized entry. استخدام النوافذ الآمنة لمنع الدخول غير المصرح به

Example: Installing shatter-resistant windows. تركيب نوافذ مقاومة للكسر

• **Walls:** Building secure walls to protect the facility. بناء الجدران الآمنة لحماية المنشأة

Example: Constructing high, reinforced walls around the perimeter. بناء جدران عالية معززة حول المحيط

• **Skimming:** Preventing skimming attacks on electronic locks. منع الهجمات على الأقفال الإلكترونية

Example: Using anti-skimming devices on card readers. استخدام أجهزة منع السرقة على قارئات البطاقات

4. Digital: Implementing digital security measures (e.g., electronic access control). تنفيذ تدابير الأمن الرقمي مثل التحكم في الوصول الإلكتروني

Example: Using electronic access control systems to manage entry points. استخدام أنظمة التحكم في الوصول الإلكترونية لإدارة نقاط الدخول

5. Shock: Using shock sensors to detect unauthorized access. استخدام أجهزة استشعار الصدمة للكشف عن الوصول غير المصرح به

Example: Installing shock sensors on doors and windows. تركيب أجهزة استشعار الصدمة على الأبواب والنوافذ

6. Glassbreak: Using sensors to detect broken glass. استخدام أجهزة الاستشعار للكشف

عن الزجاج المكسور

Example: Installing glassbreak sensors on windows. تركيب أجهزة استشعار الزجاج المكسور على النوافذ

7. Cameras: Installing surveillance cameras to monitor the perimeter. تركيب كاميرات المراقبة لمراقبة المحيط

Example: Setting up security cameras to cover all entry points. إعداد كاميرات الأمان لتغطية جميع نقاط الدخول

8. Passive Infrared Devices: Using infrared devices to detect movement. استخدام الأجهزة تحت الحمراء للكشف عن الحركة

Example: Deploying passive infrared sensors in hallways. نشر أجهزة استشعار تحت الحمراء السلبية في الممرات

9. Lighting: Implementing security lighting to deter and detect intruders. تنفيذ إضاءة الأمان لردع واكتشاف المتسللين

Example: Installing motion-activated lights around the facility. تركيب أضواء تعمل بالحركة حول المنشأة

10. Card Readers / Badges: Using card readers and badges for secure access. استخدام قارئات البطاقات والشارات للوصول الآمن

Example: Issuing ID badges to employees and using card readers for entry. إصدار شارات الهوية للموظفين واستخدام قارئات البطاقات للدخول

8.5 Infrastructure

1. Power:

• **UPS:** Uninterruptible Power Supply. إمداد الطاقة غير المنقطع

Example: Installing UPS systems to ensure continuous power supply during outages. تركيب أنظمة لضمان إمداد الطاقة المستمر خلال الانقطاعات

• **Generator:** Backup power generator. مولد الطاقة الاحتياطية

Example: Using a backup generator to provide power during extended outages. استخدام مولد احتياطي لتوفير الطاقة خلال الانقطاعات الطويلة

• **Power Outages:** Measures to handle power outages. تدابير للتعامل مع انقطاع التيار الكهربائي

Example: Developing a plan to ensure critical systems remain operational during outages. تطوير خطة لضمان بقاء الأنظمة الحيوية تعمل خلال الانقطاعات.

• **Power Degradation:** Measures to handle power degradation. تدابير للتعامل مع تدهور الطاقة

Example: Installing voltage regulators to manage power fluctuations. تركيب منظمات الجهد لإدارة تقلبات الطاقة

2. HVAC:

• **Temperature:** Maintaining optimal temperature for equipment. الحفاظ على درجة الحرارة المثلى للمعدات

Example: Using air conditioning to keep server rooms cool. استخدام تكييف الهواء للحفاظ على برودة غرف الخوادم

• **Humidity:** Controlling humidity levels. التحكم في مستويات الرطوبة

Example: Installing dehumidifiers to maintain proper humidity levels. تركيب مزيلات الرطوبة للحفاظ على مستويات الرطوبة المناسبة

• **Air Quality:** Ensuring good air quality. ضمان جودة الهواء الجيدة

Example: Using air filters to remove contaminants from the air. استخدام مرشحات الهواء لإزالة الملوثات من الهواء

3. Network: Implementing network security measures. تنفيذ تدابير أمان الشبكة

Example: Using firewalls and intrusion detection systems to protect the network. استخدام الجدران النارية وأنظمة كشف التسلل لحماية الشبكة

8.6 Fire Detection

1. Smoke: Using smoke detectors. استخدام كاشفات الدخان

Example: Installing smoke detectors in all rooms and hallways. تركيب كاشفات الدخان في جميع الغرف والممرات

2. Heat (Thermal): Using heat detectors. استخدام كاشفات الحرارة

Example: Placing heat detectors near high-risk areas like kitchens. وضع كاشفات الحرارة بالقرب من المناطق عالية الخطورة مثل المطابخ

3. Flame (Infrared): Using infrared flame detectors. استخدام كاشفات اللهب تحت الحمراء

Example: Installing flame detectors in large open areas like warehouses. تركيب كاشفات اللهب في المناطق المفتوحة الكبيرة مثل المستودعات

4. Ionization: Using ionization detectors. استخدام كاشفات التأين

Example: Installing ionization smoke detectors in offices. تركيب كاشفات الدخان التأينية في المكاتب

5. Photo-Electric: Using photo-electric detectors. استخدام كاشفات كهروضوئية

Example: Using photo-electric smoke detectors in data centers. استخدام كاشفات الدخان الكهروضوئية في مراكز البيانات

6. Dual: Using dual-sensor detectors. استخدام كاشفات ثنائية المستشعر

Example: Installing dual-sensor detectors that detect both smoke and heat. تركيب كاشفات ثنائية المستشعر تكتشف كل من الدخان والحرارة

8.7 Fire Suppression

1. Water:

• **Wet:** Using wet pipe sprinkler systems. استخدام أنظمة رش الأنابيب الرطبة

Example: Installing wet pipe sprinkler systems in office buildings. تركيب أنظمة رش الأنابيب الرطبة في المباني المكتبية

• **Dry:** Using dry pipe sprinkler systems. استخدام أنظمة رش الأنابيب الجافة

Example: Installing dry pipe systems in areas prone to freezing. تركيب أنظمة الأنابيب الجافة في المناطق المعرضة للتجميد

• **Pre-Action:** Using pre-action sprinkler systems. استخدام أنظمة رش ما قبل العمل

Example: Using pre-action systems in data centers to avoid accidental discharge. استخدام أنظمة ما قبل العمل في مراكز البيانات لتجنب التفريغ العرضي

• **Deluge:** Using deluge sprinkler systems. استخدام أنظمة رش الفيضانات

Example: Installing deluge systems in industrial facilities. تركيب أنظمة الفيضانات في المنشآت الصناعية

2. Gas:

• **INERGEN:** Gas fire suppression system. نظام إخماد الحرائق بالغاز

Example: Using INERGEN in server rooms. استخدام في غرف الخوادم

• **Argonite:** Gas fire suppression system. نظام إخماد الحرائق بالغاز

Example: Installing Argonite systems in archives and libraries. تركيب أنظمة في الأرشيفات والمكتبات

• **FM-200:** Gas fire suppression system. نظام إخماد الحرائق بالغاز

Example: Using FM-200 in data centers. استخدام في مراكز البيانات

• **Aero-K:** Gas fire suppression system. نظام إخماد الحرائق بالغاز

Example: Installing Aero-K systems in critical infrastructure. تركيب أنظمة في البنية التحتية الحيوية

3. Extinguisher:

• **CO2:** Carbon dioxide fire extinguisher. مطفأة حريق ثاني أكسيد الكربون

Example: Using CO2 extinguishers for electrical fires. استخدام مطفأة حريق ثاني أكسيد الكربون للحرائق الكهربائية

Multiple Choice Questions

1. What is a primary measure for ensuring the physical safety of personnel in a

facility?

A. Data encryption

B. First aid kits

C. Digital certificates

D. Key rotation

2. Which category of control is aimed at slowing down attackers?

A. Deter

B. Delay

C. Detect

D. Assess

3. What is the purpose of using secure locks on doors and windows?

A. To enhance network security

B. To prevent unauthorized access

C. To monitor power consumption

D. To manage data encryption

4. Which type of fire detection system uses infrared sensors?

A. Smoke detectors

B. Ionization detectors

C. Flame detectors

D. Photo-electric detectors

5. What is the role of an Uninterruptible Power Supply (UPS) in a facility?

A. To detect intruders

B. To provide backup power

C. To control access

D. To suppress fires

Answers and Explanations

1. B.

First aid kits are a primary measure for ensuring the physical safety of personnel, providing essential medical supplies in case of emergencies.

حقائب الإسعافات الأولية هي تدبير أساسي لضمان السلامة الفيزيائية للأفراد، حيث توفر الإمدادات الطبية الأساسية في حالات الطوارئ.

2. B.

The delay category of controls aims at slowing down attackers, giving security personnel more time to respond to incidents.

فئة التحكم في التأخير تهدف إلى إبطاء المهاجمين، مما يمنح أفراد الأمن المزيد من الوقت للاستجابة للحوادث.

3. B.

Secure locks on doors and windows are used to prevent unauthorized access, enhancing the physical security of the facility.

تُستخدم الأقفال الآمنة على الأبواب والنوافذ لمنع الوصول غير المصرح به، مما يعزز الأمان الفيزيائي للمنشأة.

4. C.

Flame detectors use infrared sensors to detect flames, providing early warning of fire.

تستخدم كاشفات اللهب أجهزة استشعار تحت الحمراء للكشف عن اللهب، مما يوفر إنذارًا مبكرًا

بالحريق.

5. B.

An Uninterruptible Power Supply (UPS) provides backup power, ensuring that critical systems remain operational during power outages.

يوفر إمداد الطاقة غير المنقطع طاقة احتياطية، مما يضمن بقاء الأنظمة الحيوية قيد التشغيل أثناء انقطاع التيار الكهربائي

---

9. Design Site and Facility Security Controls

9.1 Wiring Closets/Intermediate Distribution Frame

Definition: Secure areas for housing networking equipment. مناطق آمنة لإيواء معدات الشبكات

Example: Locking wiring closets to prevent unauthorized access to network equipment. قفل غرف الأسلاك لمنع الوصول غير المصرح به إلى معدات الشبكة.

9.2 Server Rooms/Data Centers

Definition: Secure rooms for housing servers and other critical IT infrastructure. غرف آمنة لإيواء الخوادم والبنية التحتية الحيوية الأخرى لتقنية المعلومات

Example: Using biometric access controls to restrict entry to server rooms. استخدام ضوابط الوصول البيومترية لتقييد الدخول إلى غرف الخوادم

9.3 Media Storage Facilities

Definition: Secure storage for backup media and other sensitive materials. التخزين الآمن لوسائط النسخ الاحتياطي والمواد الحساسة الأخرى

Example: Storing backup tapes in a fireproof safe. تخزين أشرطة النسخ الاحتياطي في خزنة مقاومة للحريق

9.4 Evidence Storage

Definition: Secure storage for evidence in investigations and audits. التخزين الآمن للأدلة في التحقيقات والتدقيق

Example: Using tamper-evident seals on evidence storage containers. استخدام أختام تظهر العبث على حاويات تخزين الأدلة

9.5 Restricted and Work Area Security

Definition: Measures to secure restricted and work areas. تدابير لتأمين المناطق المحظورة ومناطق العمل

Example: Implementing access controls to restrict entry to sensitive areas. تنفيذ ضوابط الوصول لتقييد الدخول إلى المناطق الحساسة

9.6 Utilities and Heating, Ventilation, and Air Conditioning (HVAC)

Definition: Securing utilities and HVAC systems. تأمين المرافق وأنظمة التدفئة والتهوية وتكييف الهواء

Example: Using locks and access controls on HVAC systems. استخدام الأقفال وضوابط الوصول على أنظمة التدفئة والتهوية وتكييف الهواء

1. Power:

• **Power Lines:** Securing power lines to prevent tampering. تأمين خطوط الطاقة لمنع التلاعب

• **Electrical Panels:** Securing electrical panels to prevent unauthorized access. تأمين اللوحات الكهربائية لمنع الوصول غير المصرح به

• **Power Circuits:** Ensuring power circuits are secure and protected. ضمان تأمين وحماية دوائر الطاقة

• **Backup Power:** Implementing backup power solutions. تنفيذ حلول الطاقة الاحتياطية

2. Water:

• **Water Lines:** Securing water lines to prevent tampering. تأمين خطوط المياه لمنع التلاعب

• **Fire Suppression Systems:** Ensuring fire suppression systems are operational. ضمان أنظمة إخماد الحرائق التشغيلية

• **Flood Barriers:** Installing flood barriers to protect against water damage. تركيب حواجز الفيضانات لحماية من أضرار المياه

3. Gas:

• **Gas Lines:** Securing gas lines to prevent tampering. تأمين خطوط الغاز لمنع التلاعب

• **Gas Detection:** Installing gas detection systems. تركيب أنظمة الكشف عن الغاز

4. HVAC:

• **Air Conditioning:** Ensuring air conditioning systems are secure. ضمان أنظمة تكييف الهواء الآمنة

• **Heating:** Ensuring heating systems are secure. ضمان أنظمة التدفئة الآمنة

• **Ventilation:** Ensuring ventilation systems are secure. ضمان أنظمة التهوية الآمنة

5. Cabling:

• **Ethernet:** Securing Ethernet cabling. تأمين كابلات إيثرنت

• **Fiber Optic:** Securing fiber optic cabling. تأمين كابلات الألياف البصرية

• **Copper:** Securing copper cabling. تأمين كابلات النحاس

9.7 Environmental Issues

Definition: Measures to address environmental risks (e.g., natural disasters). تدابير لمعالجة المخاطر البيئية مثل الكوارث الطبيعية

Example: Building facilities to withstand earthquakes and floods. بناء المنشآت لتحمل

الزلازل والفيضانات

9.8 Fire Prevention, Detection, and Suppression

Definition: Implementing fire prevention, detection, and suppression measures. تنفيذ تدابير الوقاية من الحرائق والكشف عنها وإخمادها

Example: Installing fire suppression systems in data centers. تركيب أنظمة إخماد الحرائق في مراكز البيانات

9.9 Power

Definition: Ensuring reliable power supply and backup. ضمان إمدادات الطاقة الموثوقة والنسخ الاحتياطي

Example: Using backup generators to provide power during outages. استخدام مولدات النسخ الاحتياطية لتوفير الطاقة خلال الانقطاعات

Multiple Choice Questions

1. What is the primary purpose of a wiring closet?

A. To store backup media

B. To house networking equipment

C. To preserve digital evidence

D. To secure electrical panels

2. Which facility is used for housing servers and critical IT infrastructure?

A. Media storage facilities

B. Evidence storage

C. Server rooms

D. Restricted areas

3. What is a key security measure for power lines?

A. Securing Ethernet cabling

B. Securing power lines to prevent tampering

C. Installing gas detection systems

D. Using flood barriers

4. Which system is essential for maintaining the air quality in a secure facility?

A. Gas detection

B. Air conditioning

C. Fire suppression

D. Backup power

5. What is the primary use of media storage facilities?

A. Housing networking equipment

B. Storing backup media and sensitive data

C. Preserving digital evidence

D. Securing power circuits

Answers and Explanations

1. B.

The primary purpose of a wiring closet is to house networking equipment, ensuring secure and organized network infrastructure.

الهدف الأساسي من غرفة الأسلاك هو إيواء معدات الشبكات، مما يضمن بنية تحتية آمنة

ومنظمة للشبكة.

2. C.

Server rooms are used for housing servers and critical IT infrastructure, providing a secure environment for essential systems.

تُستخدم غرف الخوادم لإيواء الخوادم والبنية التحتية الحيوية لتقنية المعلومات، مما يوفر بيئة آمنة للأنظمة الأساسية.

3. B.

A key security measure for power lines is securing them to prevent tampering, ensuring a stable and secure power supply.

تدبير أمان رئيسي لخطوط الطاقة هو تأمينها لمنع التلاعب، مما يضمن إمدادًا كهربائيًا مستقرًا وآمنًا.

4. B.

Air conditioning is essential for maintaining the air quality in a secure facility, ensuring that equipment operates within optimal temperature and humidity ranges.

تكييف الهواء ضروري للحفاظ على جودة الهواء في منشأة آمنة، مما يضمن أن المعدات تعمل ضمن نطاقات درجة الحرارة والرطوبة المثلى.

5. B.

The primary use of media storage facilities is to store backup media and sensitive data securely, protecting them from unauthorized access and physical damage.

الاستخدام الأساسي لمنشآت تخزين الوسائط هو تخزين وسائط النسخ الاحتياطي والبيانات الحساسة بأمان، مما يحميها من الوصول غير المصرح به والأضرار الفيزيائية.

---

10. Manage the Information System Lifecycle

10.1 Stakeholders Needs and Requirements

Definition: Identifying and understanding stakeholder needs and requirements.
تحديد وفهم احتياجات ومتطلبات أصحاب المصلحة

Example: Conducting interviews with stakeholders to gather requirements for a new system. إجراء مقابلات مع أصحاب المصلحة لجمع المتطلبات لنظام جديد

Process:

• **Stakeholder Identification:** Identifying all parties involved or affected by the project. تحديد جميع الأطراف المشاركة أو المتأثرة بالمشروع

• **Requirement Gathering:** Collecting detailed requirements from stakeholders through interviews, surveys, and workshops. جمع المتطلبات التفصيلية من أصحاب المصلحة من خلال المقابلات والاستبيانات وورش العمل

• **Documentation:** Clearly documenting all requirements to ensure they are understood and agreed upon. توثيق جميع المتطلبات بوضوح لضمان فهمها والموافقة عليها

10.2 Requirements Analysis

Definition: Analyzing requirements to ensure they are clear, complete, and feasible. تحليل المتطلبات لضمان أنها واضحة وكاملة وقابلة للتنفيذ

Example: Creating detailed requirements documents that outline the functionality of the system. إنشاء مستندات متطلبات مفصلة توضح وظيفة النظام

Process:

• **Feasibility Study:** Assessing whether the requirements can be realistically achieved within the constraints of time, budget, and technology. تقييم ما إذا كانت المتطلبات يمكن تحقيقها بشكل واقعي ضمن قيود الوقت والميزانية والتكنولوجيا

• **Prioritization:** Determining the priority of requirements based on their importance and impact. تحديد أولويات المتطلبات بناءً على أهميتها وتأثيرها

• **Validation:** Ensuring that the requirements accurately reflect the needs of stakeholders. ضمان أن المتطلبات تعكس بدقة احتياجات أصحاب المصلحة

10.3 Architectural Design

Definition: Designing the system architecture to meet requirements. تصميم هندسة النظام لتلبية المتطلبات

Example: Developing a blueprint of the system's structure and components. تطوير مخطط هيكل النظام ومكوناته

Process:

• ***High-Level Design:*** Creating an overarching design that outlines the main components and their interactions. إنشاء تصميم شامل يحدد المكونات الرئيسية وتفاعلاتها.

• ***Detailed Design:*** Developing detailed plans for each component, including data flow diagrams, interface specifications, and hardware requirements. تطوير خطط تفصيلية لكل مكون، بما في ذلك مخططات تدفق البيانات، مواصفات الواجهات، ومتطلبات الأجهزة

10.4 Development/Implementation

Definition: Developing and implementing the system according to the design. تطوير وتنفيذ النظام وفقًا للتصميم

Example: Writing code and configuring hardware based on the architectural design. كتابة الكود وتكوين الأجهزة بناءً على التصميم المعماري

Process:

• **Coding:** Writing the actual code based on the design specifications. كتابة الكود الفعلي بناءً على مواصفات التصميم

• **Unit Testing:** Testing individual components to ensure they function correctly. اختبار المكونات الفردية لضمان أنها تعمل بشكل صحيح

• **Integration:** Combining all components and ensuring they work together seamlessly. دمج جميع المكونات وضمان أنها تعمل معًا بسلاسة.

10.5 Integration

Definition: Integrating the system components to work together. دمج مكونات النظام للعمل معًا

Example: Combining software modules and hardware components to form a complete system. دمج وحدات البرمجيات ومكونات الأجهزة لتشكيل نظام كامل

Process:

• **System Testing:** Testing the entire system to ensure all components work together as intended. اختبار النظام بالكامل لضمان أن جميع المكونات تعمل معًا كما هو مقصود

• **Interoperability Testing:** Ensuring the system can interact with other systems and components. ضمان أن النظام يمكنه التفاعل مع الأنظمة والمكونات الأخرى

10.6 Verification and Validation

Definition: Ensuring the system meets requirements and performs as expected. ضمان أن النظام يلبي المتطلبات ويعمل كما هو متوقع

Example: Conducting tests to verify that the system functions correctly. إجراء اختبارات للتحقق من أن النظام يعمل بشكل صحيح

Process:

• **Verification:** Confirming that the system is built correctly according to specifications. تأكيد أن النظام تم بناؤه بشكل صحيح وفقًا للمواصفات

• **Validation:** Ensuring the system fulfills its intended purpose and meets stakeholder expectations. ضمان أن النظام يفي بالغرض المقصود منه ويلبي توقعات أصحاب المصلحة

10.7 Transition/Deployment

Definition: Transitioning the system into the operational environment. نقل النظام إلى بيئة التشغيل

Example: Migrating data and users to the new system. ترحيل البيانات والمستخدمين إلى النظام الجديد

Process:

• **Deployment Planning:** Creating a detailed plan for deploying the system, including timelines and resource allocation. إنشاء خطة مفصلة لنشر النظام، بما في ذلك الجداول الزمنية وتخصيص الموارد

• **Training:** Training users and administrators on how to use and manage the system.

تدريب المستخدمين والمسؤولين على كيفية استخدام وإدارة النظام

• **Go-Live:** Making the system operational and available to users. جعل النظام قيد التشغيل ومتاحًا للمستخدمين

10.8 Operations and Maintenance/Sustainment

Definition: Maintaining the system to ensure continued operation and performance. صيانة النظام لضمان استمرار التشغيل والأداء

Example: Regularly updating software and performing routine maintenance on hardware. تحديث البرمجيات بانتظام وإجراء صيانة دورية على الأجهزة

Process:

• **Monitoring:** Continuously monitoring the system to detect and address issues. مراقبة النظام باستمرار لاكتشاف ومعالجة المشاكل

• **Patch Management:** Applying updates and patches to fix vulnerabilities and improve performance. تطبيق التحديثات والترقيعات لإصلاح الثغرات وتحسين الأداء

• **Support:** Providing ongoing support to users and administrators. تقديم الدعم المستمر للمستخدمين والمسؤولين

10.9 Retirement/Disposal

Definition: Retiring and securely disposing of the system when it is no longer needed. تقاعد النظام والتخلص منه بأمان عندما لم يعد هناك حاجة إليه

Example: Decommissioning old servers and securely erasing data. إيقاف تشغيل الخوادم القديمة ومسح البيانات بأمان

Process:

• **Decommissioning:** Shutting down the system and ensuring all data is securely archived or transferred. إيقاف تشغيل النظام وضمان أرشفة جميع البيانات بأمان أو نقلها

• **Data Destruction:** Securely destroying any sensitive data. تدمير البيانات الحساسة بأمان

• **Recycling:** Disposing of hardware in an environmentally responsible manner.

التخلص من الأجهزة بطريقة مسؤولة بيئيًا

Multiple Choice Questions

1. What is the primary goal of the requirement analysis phase?

A. To develop detailed design specifications

B. To ensure requirements are clear, complete, and feasible

C. To write and test code

D. To train users and administrators

2. What is the purpose of unit testing in the development phase?

A. To ensure all system components work together

B. To test individual components for correct functionality

C. To transition the system to the operational environment

D. To monitor and address system issues

3. Which process involves confirming that the system is built correctly according to specifications?

A. Validation

B. Verification

C. Integration

D. Deployment

4. What is the first step in the transition/deployment process?

A. Training users

B. Go-Live

C. Deployment Planning

D. System Testing

5. What is the primary focus during the operations and maintenance phase?

A. Developing the system

B. Retiring and disposing of the system

C. Monitoring and maintaining system performance

D. Gathering requirements

Answers and Explanations

1. B.

The primary goal of the requirement analysis phase is to ensure that all requirements are clear, complete, and feasible within the constraints of the project.

الهدف الرئيسي من مرحلة تحليل المتطلبات هو ضمان أن جميع المتطلبات واضحة وكاملة وقابلة للتنفيذ ضمن قيود المشروع.

2. B.

Unit testing focuses on testing individual components to ensure they function correctly before being integrated into the larger system.

يركز اختبار الوحدات على اختبار المكونات الفردية لضمان أنها تعمل بشكل صحيح قبل دمجها في النظام الأكبر.

3. B.

Verification is the process of confirming that the system is built correctly according to the specified design and requirements.

التحقق هو عملية تأكيد أن النظام تم بناؤه بشكل صحيح وفقًا للتصميم والمتطلبات المحددة.

4. C.

The first step in the transition/deployment process is creating a detailed deployment plan, outlining timelines and resource allocation.

الخطوة الأولى في عملية الانتقال / النشر هي إنشاء خطة نشر مفصلة، توضح الجداول الزمنية وتخصيص الموارد.

5. C.

During the operations and maintenance phase, the primary focus is on continuously monitoring and maintaining the system to ensure its ongoing performance and reliability.

خلال مرحلة العمليات والصيانة، يركز الجهد الرئيسي على مراقبة النظام باستمرار وصيانته لضمان استمرارية أدائه وموثوقيته

---

11. Vulnerabilities in Systems

11.1 Mobile Devices

OWASP Mobile Top 10:

1. M1: Improper Platform Usage: Incorrect use of platform features or failure to use security controls. الاستخدام غير السليم للنظام الأساسي أو الفشل في استخدام ضوابط الأمان

Example: An app that does not use secure storage APIs correctly. تطبيق لا يستخدم واجهات برمجة التطبيقات للتخزين الآمن بشكل صحيح

2. M2: Insecure Data Storage: Poor protection of data stored on the device. تخزين البيانات غير الآمن

Example: Storing sensitive data in plaintext on a mobile device. تخزين البيانات الحساسة كنص عادي على جهاز محمول

3. M3: Insecure Communication: Failure to protect network traffic. الاتصال غير الآمن

Example: Transmitting sensitive information over HTTP instead of HTTPS.

4. M4: Insecure Authentication: Weaknesses in authentication mechanisms.

المصادقة غير الآمنة

Example: Using simple PINs for authentication without additional security measures. استخدام رموز بسيطة للمصادقة دون تدابير أمان إضافية

5. M5: Insufficient Cryptography: Weak or improperly implemented encryption. التشفير غير الكافي

Example: Using outdated encryption algorithms like DES. استخدام خوارزميات التشفير القديمة مثل

6. M6: Insecure Authorization: Flaws in authorization mechanisms. التفويض غير الآمن

Example: An app that does not properly check user permissions. تطبيق لا يتحقق بشكل صحيح من أذونات المستخدم

7. M7: Client Code Quality: Poor code quality leading to vulnerabilities. جودة كود العميل

Example: Vulnerabilities due to unhandled exceptions or poor error handling. نقاط الضعف الناتجة عن الاستثناءات غير المعالجة أو معالجة الأخطاء السيئة

8. M8: Code Tampering: Risks of unauthorized code changes. التلاعب بالكود

Example: Modifying an app's code to bypass security checks. تعديل كود التطبيق لتجاوز الفحوصات الأمنية

9. M9: Reverse Engineering: Threats from analyzing app code to find vulnerabilities. الهندسة العكسية

Example: Using tools to decompile an app and find security flaws. استخدام الأدوات لفك تجميع تطبيق واكتشاف العيوب الأمنية

10. M10: Extraneous Functionality: Unintended, dangerous functionality in the code. الوظائف الزائدة

Example: Debug code left in the app that exposes sensitive information. كود التصحيح المتبقي في التطبيق الذي يكشف عن المعلومات الحساسة

11.2 Web-Based Vulnerabilities

1. Cross Site Scripting (XSS):

A. Stored (Persistent): Malicious script is permanently stored on the target server. المخزن الدائم النص الضار يتم تخزينه بشكل دائم على الخادم المستهدف

Example: An attacker injects a script into a forum post, affecting all who view it. مهاجم يحقن نصًا في منشور على المنتدى، مما يؤثر على جميع من يشاهده

B. Reflected (Most Common): Malicious script is reflected off a web application to the user's browser. المنعكس الأكثر شيوعًا النص الضار يتم عكسه عن تطبيق ويب إلى متصفح المستخدم

Example: An attacker includes a malicious script in a URL, and when a user clicks it, the script is executed. مهاجم يضمن نصًا ضارًا في رابط، وعندما ينقر المستخدم عليه، يتم تنفيذ النص

C. DOM: Modifies the Document Object Model environment in the victim's browser. تعدل بيئة نموذج الكائنات الوثائقية في متصفح الضحية

Example: An attacker manipulates the DOM structure to execute malicious code. مهاجم يتلاعب ببنية نموذج الكائنات الوثائقية لتنفيذ كود ضار

2. Cross Site Request Forgery (CSRF):

• **Definition:** Tricks the user into performing actions they did not intend. خداع المستخدم للقيام بإجراءات لم يقصدها

Example: An attacker tricks a user into submitting a malicious request to a website where the user is authenticated. مهاجم يخدع المستخدم لتقديم طلب ضار إلى موقع ويب يكون المستخدم مصدق عليه

3. SQL Injection:

• **Definition:** An attack that allows attackers to execute arbitrary SQL code. هجوم يسمح للمهاجمين بتنفيذ كود تعسفي

Example: An attacker injects a malicious SQL query into a website's input field. مهاجم يحقن استعلام ضار في حقل إدخال موقع ويب

4. Input Validation:

A. Client Side vs. Server Side: Validating input on the client side vs. the server side. التحقق من صحة الإدخال في جانب العميل مقابل جانب الخادم

Example: Ensuring input is validated on the server side to prevent tampering. ضمان التحقق من صحة الإدخال على جانب الخادم لمنع التلاعب

B. Allow Lists vs. Deny Lists: Allowing known good input vs. denying known bad input. قوائم السماح مقابل قوائم الرفض السماح بالإدخال الجيد المعروف مقابل رفض الإدخال السيئ المعروف

Example: Using an allow list to specify which input values are permitted. استخدام قائمة السماح لتحديد قيم الإدخال المسموح بها

11.3 General Vulnerabilities

1. Single Point of Failure:

• **Definition:** A single component whose failure can bring down the entire system. مكون واحد يمكن لفشله أن يعطل النظام بالكامل

Example: A single server that, if it fails, will disrupt the entire network. خادم واحد، إذا فشل، سيعطل الشبكة بالكامل

2. Bypass Controls:

• **Definition:** Methods to bypass security mechanisms. طرق لتجاوز آليات الأمان

Example: Exploiting a bug to gain unauthorized access despite security controls. استغلال خطأ للوصول غير المصرح به على الرغم من الضوابط الأمنية

3. TOCTOU (Race Conditions):

• **Definition:** Timing issues where changes occur between checking a condition and performing an action. مشاكل التوقيت حيث تحدث التغييرات بين فحص شرط وتنفيذ إجراء.

Example: A file is checked for permissions and then modified before access is granted. يتم فحص ملف للحصول على الأذونات ثم يتم تعديله قبل منح الوصول.

4. Emanations:

Definition: Electromagnetic emissions that can be exploited to gain information. الانبعاثات الكهرومغناطيسية التي يمكن استغلالها للحصول على المعلومات

• **Shielding (TEMPEST):** Protecting against eavesdropping by containing electronic emissions. الحماية من التنصت عن طريق احتواء الانبعاثات الإلكترونية

• **White Noise:** Using noise to mask signal transmissions. استخدام الضوضاء لإخفاء الإشارات

• **Control Zones:** Establishing controlled areas to limit electromagnetic leaks. إنشاء مناطق محكمة للحد من التسريبات الكهرومغناطيسية

Example: Capturing data from a monitor through its electromagnetic emissions. التقاط البيانات من شاشة من خلال انبعاثاتها الكهرومغناطيسية

5. Shielding (TEMPEST):

• **Definition:** Measures to protect against data leakage through electromagnetic emissions. تدابير لحماية من تسرب البيانات من خلال الانبعاثات الكهرومغناطيسية

Example: Using shielded cables and enclosures to protect sensitive equipment. استخدام الكابلات المغلفة والأغلفة لحماية المعدات الحساسة

6. White Noise:

• **Definition:** Noise added to an environment to mask electromagnetic emissions. الضوضاء المضافة إلى بيئة لإخفاء الانبعاثات الكهرومغناطيسية

Example: Generating white noise to prevent eavesdropping on conversations. توليد الضوضاء البيضاء لمنع التنصت على المحادثات

7. Control Zones:

• **Definition:** Designated areas where security controls are implemented. المناطق المخصصة حيث يتم تنفيذ ضوابط الأمان

Example: Creating secure zones within a facility to restrict access. إنشاء مناطق آمنة داخل المنشأة لتقييد الوصول

8. Covert Channels:

• **Definition:** Hidden methods of transferring information. الطرق الخفية لنقل المعلومات

Example: Using a low-bandwidth covert channel to leak sensitive information. استخدام قناة خفية منخفضة النطاق لتسريب المعلومات الحساسة

9. Aggregation & Inference:

• **Definition:** Collecting and inferring information to reveal sensitive data. جمع واستنتاج المعلومات لكشف البيانات الحساسة

Example: Combining non-sensitive data to infer sensitive information. جمع البيانات غير الحساسة لاستنتاج المعلومات الحساسة

10. Redundancy:

• **Definition:** Duplicating critical components to increase reliability. تكرار المكونات الحيوية لزيادة الموثوقية

Example: Using redundant servers to ensure availability. استخدام الخوادم المتكررة لضمان التوفر

11. Mitigating Controls:

• **Definition:** Measures to reduce the risk or impact of vulnerabilities. تدابير لتقليل المخاطر أو تأثير الثغرات

Example: Implementing additional firewalls to protect against network attacks. تنفيذ جدران نارية إضافية للحماية من الهجمات الشبكية

12. Increase Frequency of Reauthentication:

• **Definition:** Requiring users to authenticate more frequently to reduce the risk of unauthorized access. طلب إعادة المصادقة من المستخدمين بشكل أكثر تكرارًا لتقليل خطر الوصول غير المصرح به

Example: Requiring reauthentication after a certain period of inactivity. طلب إعادة المصادقة بعد فترة معينة من عدم النشاط

13. Analysis & Design:

• **Definition:** Analyzing and designing systems to address vulnerabilities. تحليل وتصميم الأنظمة لمعالجة الثغرات

Example: Conducting a thorough analysis to identify potential vulnerabilities in a new system. إجراء تحليل شامل لتحديد الثغرات المحتملة في نظام جديد

14. Polyinstantiation:

• **Definition:** Creating multiple instances of data to prevent unauthorized inference. إنشاء مثيلات متعددة من البيانات لمنع الاستدلال غير المصرح به

Example: Using different versions of a database for different security levels. استخدام إصدارات مختلفة من قاعدة البيانات لمستويات أمان مختلفة

15. Policy, Training & Procedures:

• **Definition:** Implementing policies, training, and procedures to address vulnerabilities. تنفيذ السياسات والتدريب والإجراءات لمعالجة الثغرات

Example: Providing regular security training for employees. تقديم تدريب أمني منتظم للموظفين

16. Remote Access Security:

• **Definition:** Securing remote access to systems and networks. تأمين الوصول عن بُعد إلى الأنظمة والشبكات

Example: Using VPNs and multi-factor authentication for remote access. استخدام الشبكات الخاصة الافتراضية والمصادقة متعددة العوامل للوصول عن بُعد

17. End-Point Security:

• **Definition:** Securing devices that connect to the network. تأمين الأجهزة التي تتصل بالشبكة

Example: Implementing antivirus software and encryption on all endpoint devices. تنفيذ برامج مكافحة الفيروسات والتشفير على جميع الأجهزة الطرفية

Multiple Choice Questions

1. What does M3 in the OWASP Mobile Top 10 refer to?

A. Improper Platform Usage

B. Insecure Data Storage

C. Insecure Communication

D. Insufficient Cryptography

2. What type of vulnerability is SQL Injection?

A. Web-based

B. Mobile-based

C. Physical

D. Network

3. Which type of XSS involves malicious scripts stored on the server?

A. Reflected

B. Stored

C. DOM

D. Persistent

4. What does 'TOCTOU' stand for?

A. Time of Check to Time of Use

B. Type of Check to Type of Use

C. Time of Check to Type of Use

D. Type of Check to Time of Use

5. What is the purpose of using white noise in security?

A. To prevent SQL Injection

B. To mask signal transmissions

C. To authenticate users

D. To prevent cross-site scripting

Answers and Explanations

1. C.

M3 in the OWASP Mobile Top 10 refers to insecure communication, which highlights the risks associated with unencrypted or improperly encrypted communications.

يشير في قائمة إلى الاتصال غير الآمن، مما يبرز المخاطر المرتبطة بالاتصالات غير المشفرة أو المشفرة بشكل غير صحيح.

2. A.

SQL Injection is a type of web-based vulnerability where malicious SQL code is injected into queries to manipulate the database.

الحقن هو نوع من الثغرات القائمة على الويب حيث يتم حقن الكود الخبيث في الاستعلامات للتلاعب بقاعدة البيانات.

3. B.

Stored (persistent) XSS involves malicious scripts that are stored on the server and executed when users access the compromised server.

يشمل المخزن (المستمر) النصوص الخبيثة المخزنة على الخادم والتي يتم تنفيذها عند وصول المستخدمين إلى الخادم المتضرر.

4. A.

TOCTOU stands for Time of Check to Time of Use, which refers to race conditions that occur when the system state changes between checking a condition and using the results of that check.

يشير إلى وقت الفحص إلى وقت الاستخدام، وهو يشير إلى حالات السباق التي تحدث عندما تتغير حالة النظام بين فحص شرط معين واستخدام نتائج هذا الفحص.

5. B.

White noise is used in security to mask signal transmissions, making it harder for attackers to intercept and interpret electronic emissions.

يتم استخدام الضوضاء البيضاء في الأمان لإخفاء الإشارات، مما يجعل من الصعب على المهاجمين اعتراض وفهم الانبعاثات الإلكترونية.

Conclusion

In this module, we covered the foundational principles of security architecture and engineering. We discussed secure design principles, fundamental security models, selecting controls based on system requirements, and understanding the security capabilities of information systems. Additionally, we explored methods to assess and mitigate vulnerabilities, cryptographic solutions, cryptanalytic attacks, site and facility security design, managing the information system lifecycle, and identifying system vulnerabilities.

في هذا المقرر، تناولنا المبادئ الأساسية لأرشفة الأمان والهندسة. ناقشنا مبادئ التصميم الآمن، والنماذج الأمنية الأساسية، واختيار الضوابط بناءً على متطلبات النظام، وفهم قدرات الأمان لأنظمة المعلومات. بالإضافة إلى ذلك، استكشفنا طرق تقييم وتخفيف الثغرات، وحلول التشفير، وهجمات تحليل الشفرات، وتصميم أمان المواقع والمنشآت، وإدارة دورة حياة نظام المعلومات، وتحديد ثغرات النظام

CISSP Resources

1. Official $(ISC)^2$ CISSP Study Guide
2. CISSP $(ISC)^2$ Official Practice Tests
3. Oreilly – CISSP Training by Sari Greene : **https://www.oreilly.com/library/view/cissp-4th-edition**
4. CISSP MindMaps YouTube Playlist from Destination Certification : **https://www.youtube.com/playlist?list=PLZKdGEfEyJhLd-pJhAD7dNbJyUgpqI4pu**

Mohammed Alfatih Altahir 1mo
Network Security Engineer/Cisco/Palo alto/Fortinet

شكرا مهندس جعله الله في ميزان حسناتك

Like · Reply

Gassim M. Abbas, MBA, PMP®, CISA, ITIL®, MCSA 2mo
IT Project Management | IT Auditing | IT Service Management

جزاك الله خير

Like · Reply | 1 Reaction

Dr. Saad Alqahtany 2mo
Dean, College of Computer Science and Information systems | Cyber Security & Digital forensics Consultant | Assis...

جزاك الله خير. عمل ابداعي يذكر ويشكر🌺

Like · Reply | 1 Reaction

Mohamed Goda 2mo
Infrastructure Engineer- Nutanix - Vmware - Backup solution

ما شاء الله يا عماد ربنا يجعله في ميزان حسناتك وشفيع للوالد والوالده

Like · Reply | 1 Reaction

Ahmed Sultan 2mo
Founder at Netriders Academy

شغل محترم يا عماد 🌹

Like · Reply | 3 Reactions

See more comments

To view or add a comment, sign in

More articles by this author

Module 7: Security Operations / إدارة عمليات...
Aug 5, 2024

Module 6: Security Assessment and Testing...
Jul 28, 2024

CISSP Module 5: Identi and Access Manageme
Jul 8, 2024

See all

Explore topics

- Sales
- Marketing
- Business Administration
- HR Management
- Content Management
- Engineering
- Soft Skills
- See All

المبادئ الأساسية للاتصال الآمن وأمان الشبكة

The fundamental principles of secure communication and network security

Emad M. Abdelhamid • 2nd
Technical Leader | SME IT Security Design @ Cisco - CX EMEA . ...
View my portfolio
+ Follow
3w • Edited •

لسلام عليكم ورحمه الله وبركاته
استكمالاً لما بدأناه سنقوم اليوم بتقديم مختصر عن الفصل الرابع من الشرح المختصر لشهادة ال
CISSP
و يغطي هذا الفصل المبادئ الأساسية للاتصال الآمن وأمان الشبكة, ويشمل تصميم هياكل الشبكة الآمنة, وفهم مكونات الشبكة الآمنة ,وتنفيذ قنوات الاتصال الآمنة ,وضمان الوصول الآمن عن بُعد ,وفهم تقسيم الشبكة وحساباته ,واستكشاف حلول الأمان المتقدمة
مثل جدران الحماية وحماية النقاط النهائية , وفهم الهجمات الشبكية المختلفة ووسائل التخفيف منها.
الهدف هو توفير فهم شامل لكيفية تأمين البنية التحتية للشبكة ضد التهديدات والثغرات المتوقعة.

ويحتوى على 5 أجزاء
It contains 5 parts

1. Apply Secure Design Principles in Network Architectures تطبيق مبادئ التصميم الآمن في هندسة الشبكات
2. Network Security and Defense أمن الشبكات والدفاع
3. Implement Secure Communication تنفيذ الاتصالات الآمنة
4. Remote Access الوصول عن بعد
5. Network Attacks هجمات الشبكة

المقالات، بإذن الله، ستكون مقدمة جيدة للتحضير للشهادة. ولكنها غير كافية وتحتاج للتحضير بالتفصيل من المصادر المذكورة في نهاية كل مقال.

These articles, once completed, will serve as a good introduction to preparing for the certification. However, they are not sufficient on their own and will require detailed preparation from the sources mentioned at the end of each article.

تابعونا في المقالات القادمة لاستكمال شرح باقي الفصول، مع مزيد من الأمثلة والأسئلة التوضيحية التي تساعدكم في التحضير للشهادة بشكل أفضل

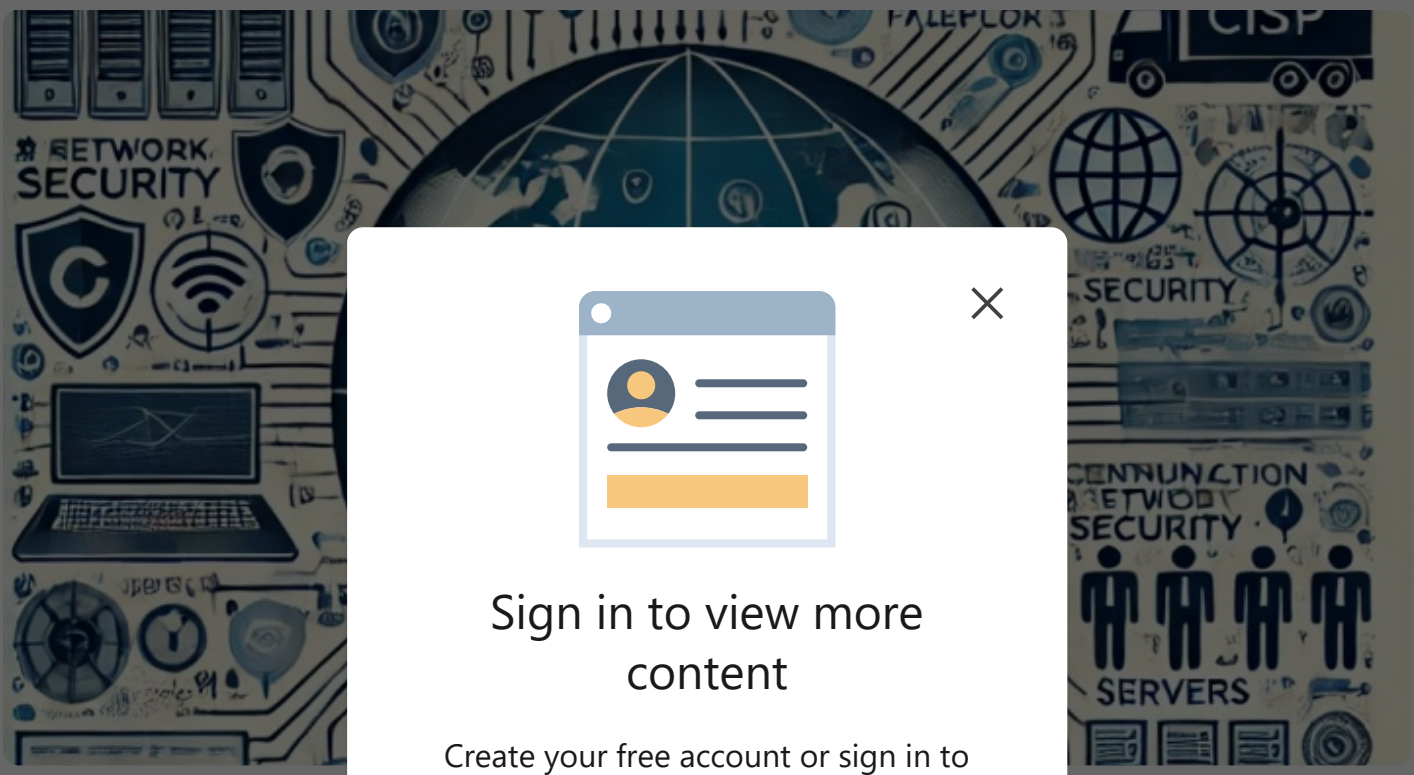
Follow us in the upcoming articles to complete the explanation of the remaining chapters, with more examples and clarifying questions that will help you better prepare for the CISSP certificate.

المقالات

For Module 1 : https://lnkd.in/dkkyFGdW
For Module 2 : https://lnkd.in/dNUWhiJs
For Module 3: https://lnkd.in/dsqBXhEc
For Module 4: https://lnkd.in/d_DBAm4h
For Module 5: https://lnkd.in/dGPDeKWF
For Module 6: https://lnkd.in/dZHHJKJx
For Module 7: https://lnkd.in/d_JswW5W
For Module 8: https://lnkd.in/dQsQHqgR

Resources - المصادر

1- Official (ISC)² CISSP Study Guide
2- CISSP (ISC)² Official Practice Tests
3- CISSP All-in-One Exam Guide by Shon Harris
4- Cybrary – CISSP Training by Kelly Handerhan https://lnkd.in/d4zrAkJz
5- Oreilly – CISSP Training by Sari Greene https://lnkd.in/dANS-hVc.
6- CISSP bundles by Thor Pedersen https://lnkd.in/d2tpqaJk
7- CISSP MindMaps YouTube Playlist from Destination Certification https://lnkd.in/deJM44xX



CISSP Mod ... Network S ...الاتص

Emad M. Ab
Technical Lead
CCIE#58413 | ™ |
ISO27001 LA |
Published Jul

Introduction

This module covers the fundamental principles of secure communication and network security. It includes designing secure network architectures, understanding secure network components, implementing secure communication channels, ensuring secure remote access, understanding subnetting and its calculations, exploring advanced security solutions like firewalls and endpoint protection, and

provide a comprehensive understanding of how to secure network infrastructures against emerging threats and vulnerabilities.

يغطي هذا الفصل المبادئ الأساسية للاتصال الآمن وأمان الشبكة ويشمل تصميم هياكل الشبكة الآمنة وفهم مكونات الشبكة الآمنة وتنفيذ قنوات الاتصال الآمنة وضمان الوصول الآمن عن بُعد وفهم تقسيم الشبكة وحساباته واستكشاف حلول الأمان المتقدمة مثل جدران الحماية وحماية النقاط النهائية وفهم الهجمات الشبكية المختلفة ووسائل التخفيف منها. الهدف هو توفير فهم شامل لكيفية تأمين البنية التحتية للشبكة ضد التهديدات والثغرات الناشئة

Module Brief

1. Apply Secure Design Principles in Network Architectures

This section covers the secure design principles necessary for creating robust network architectures, including understanding the OSI and TCP/IP models, secure protocols, converged protocols, physical and logical segmentation, and subnetting.

يتناول هذا القسم مبادئ التصميم الآمن اللازمة لإنشاء هياكل الشبكة القوية بما في ذلك فهم النماذج الاساسية والبروتوكولات الآمنة والبروتوكولات المتقاربة والتجزئة الفيزيائية والمنطقية وتقسيم الشبكة

2. Network Security and Defense

This section focuses on the operation and security of network infrastructure components, including transmission media, network access control systems, endpoint security, advanced endpoint protection solutions, defense in depth strategies, firewalls, IDS/IPS systems, and endpoint security solutions.

يركز هذا القسم على تشغيل وأمان مكونات البنية التحتية للشبكة بما في ذلك وسائل النقل وأنظمة التحكم في الوصول إلى الشبكة وأمان النقاط النهائية وحلول حماية النقاط النهائية المتقدمة واستراتيجيات الدفاع في العمق وجدران الحماية وأنظمة كشف ومنع التسلل وحلول أمان النقاط النهائية

3. Implement Secure Communication Channels According to Design

This section explains how to implement secure communication channels, including voice, video, collaboration, remote access, data communications, and third-party connectivity.

يوضح هذا القسم كيفية تنفيذ قنوات الاتصال الآمنة بما في ذلك الصوت والفيديو والتعاون

والوصول عن بعد واتصالات البيانات والاتصال بالأطراف الثالثة

4. Remote Access

This section covers the principles and technologies necessary for ensuring secure remote access, including tunneling, encryption, VPNs, and remote authentication.

يتناول هذا القسم المبادئ والتقنيات اللازمة لضمان الوصول الآمن عن بُعد بما في ذلك التشفير والشبكات الخاصة الافتراضية والمصادقة عن بُعد

5. Network Attacks

This section explores various types of network attacks, their phases, examples, and mitigation controls required to prevent them.

يستكشف هذا القسم أنواع الهجمات الشبكية المختلفة ومراحلها وأمثلة عنها ووسائل التخفيف المطلوبة لمنعها

---

1. Apply Secure Design Principles in Network Architectures

1.1 Open System Interconnection (OSI) Model

- **Definition:** Frameworks that standardize the functions of a telecommunication or computing system.

أطر عمل توحد وظائف نظام الاتصالات أو الحوسبة

- **The 7 Layers:**

1. Physical Layer
2. Datalink Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer

7. Application Layer

1.1.1 Physical Layer:

- **Media:**

Wired: Twisted Pair, Coaxial, Fiber Optic

Wireless: Radio Frequency, Infrared, Microwave

- **Topologies:**

Bus, Tree, Star, Mesh, Ring

- **Example:** Ethernet cables (Twisted Pair) used to connect computers in a network.

مثال كابلات إيثرنت زوج مجدول تُستخدم لتوصيل أجهزة الكمبيوتر في الشبكة

- **Use Case:** In a corporate office, Ethernet cables are used to connect desktop computers to the local network for reliable internet access and file sharing.

حالة استخدام في مكتب الشركة، يتم استخدام كابلات إيثرنت لتوصيل أجهزة الكمبيوتر المكتبية بالشبكة المحلية للوصول إلى الإنترنت ومشاركة الملفات بشكل موثوق

1.1.2 Datalink Layer:

- **Collisions:**

CSMA/CA, CSMA/CD

- **Devices:**

Hubs, Repeaters, Connectors

- **Protocols:**

802.1x

- **Example:** Switches use MAC addresses to forward data to the correct device.

مثال تستخدم المحولات عناوين ماك لتوجيه البيانات إلى الجهاز الصحيح

- **Use Case:** A network switch in a data center forwards traffic based on MAC addresses to ensure efficient data transmission between servers.

حالة استخدام يقوم مفتاح الشبكة في مركز البيانات بتوجيه حركة المرور بناءً على عناوين ماك لضمان نقل البيانات بكفاءة بين الخوادم

1.1.3 Network Layer:

- **Protocols:**

ARP, PPTP, PAP, CHAP, EAP

- **IP Addressing:**

ICMP (Ping), IPsec, IGMP

- **Devices:**

Routers, Packet Filtering Firewalls

- **Example:** Routers use IP addresses to forward packets to their destination.

مثال تستخدم الموجهات العناوين لتوجيه الحزم إلى وجهتها

- **Use Case:** A router in an enterprise network routes traffic between different subnets to manage network segmentation and improve security.

حالة استخدام يقوم جهاز توجيه في شبكة المؤسسة بتوجيه حركة المرور بين الشبكات الفرعية المختلفة لإدارة تقسيم الشبكة وتحسين الأمان

1.1.4 Transport Layer:

- **Ports = Services:**

Common Ports

- **Protocols:**

TCP/UDP, SSL/TLS, BGP

- **Example:** TCP ensures reliable data transfer between a client and server.

مثال يضمن البروتوكول نقل البيانات بشكل موثوق بين العميل والخادم

- **Use Case:** TCP is used in online banking transactions to ensure data integrity and reliability between the user's browser and the bank's server.

حالة استخدام يتم استخدام البروتوكول في المعاملات المصرفية عبر الإنترنت لضمان سلامة البيانات وموثوقيتها بين متصفح المستخدم وخادم البنك

_____

1.1.5 Session Layer:

- **Protocols:**

Circuit Proxy Firewall

- **Example:** RPC (Remote Procedure Call) allows a program to request a service from a program on another computer.

مثال يتيح (استدعاء الإجراء البعيد) للبرنامج طلب خدمة من برنامج على جهاز كمبيوتر آخر

- **Use Case:** RPC is used in a distributed application to allow different components to communicate and perform functions across different servers.

حالة استخدام يتم استخدام استدعاء الإجراء البعيد في تطبيق موزع للسماح للمكونات المختلفة بالتواصل وأداء الوظائف عبر الخوادم المختلفة

_____

1.1.6 Presentation Layer:

- **Devices:**

NetBIOS, RPC

- **Example:** SSL/TLS encrypts data to ensure secure communication.

مثال يقوم بتشفير البيانات لضمان الاتصال الآمن

- **Use Case:** SSL/TLS is implemented on e-commerce websites to encrypt sensitive

information such as credit card details during transactions.

حالة استخدام يتم تنفيذه على مواقع التجارة الإلكترونية لتشفير المعلومات الحساسة مثل تفاصيل بطاقة الائتمان أثناء المعاملات

1.1.7 Application Layer:

- **Protocols:**

HTTP/S, DNS, SSH, SNMP, LDAP, DHCP

- **Devices:**

Application Firewalls

- **Example:** HTTP/S is used for transmitting web pages over the internet.
- **Use Case:** HTTPS is used on social media platforms to ensure secure data exchange between users and the server.

1.2 Internet Protocol (IP) Version 4 and 6 (IPv6)

Definition: Protocols for addressing and routing packets of data so they can travel across networks and arrive at the correct destination.

بروتوكولات لمعالجة وتوجيه حزم البيانات بحيث يمكنها التنقل عبر الشبكات والوصول إلى الوجهة الصحيحة

Examples:

- **Unicast:** Sending data from one source to one destination. يونيكاست إرسال البيانات من مصدر واحد إلى وجهة واحدة
- **Broadcast:** Sending data from one source to all possible destinations in the network. البث إرسال البيانات من مصدر واحد إلى جميع الوجهات الممكنة في الشبكة
- **Use Case:** Unicast is used in video streaming services to send data from the server to a specific user's device.

حالة استخدام يتم استخدام يونيكاست في خدمات بث الفيديو لإرسال البيانات من الخادم إلى جهاز مستخدم معين

1.3 Secure Protocols

- **Definition:** Protocols that provide security services such as encryption and authentication for data in transit.

بروتوكولات توفر خدمات الأمان مثل التشفير والمصادقة للبيانات أثناء النقل

Examples:

- **IPSec:** Provides secure communication by encrypting and authenticating IP packets. بروتوكول أمان الإنترنت يوفر الاتصالات الآمنة عن طريق تشفير ومصادقة حزم آي بي
- **SSL/TLS:** Secures communications over a computer network. يؤمن الاتصالات عبر شبكة الكمبيوتر

- **Use Case:** IPSec is used in VPNs to ensure secure communication between remote employees and the corporate network.

يتم استخدامه في الشبكات الافتراضية الخاصة لضمان الاتصال الآمن بين الموظفين عن بُعد وشبكة الشركة

1.4 Implications of Multilayer Protocols

Definition: The use of protocols operating at multiple layers of the OSI model to provide comprehensive security.

استخدام البروتوكولات التي تعمل في طبقات متعددة من نموذج أوس أي لتوفير الأمان الشامل

Examples:

- Combining SSL/TLS (Layer 4) with IPSec (Layer 3) for enhanced security.

الطبقة الرابعة بروتوكول أمان الإنترنت مع الطبقة الثالثة لتعزيز الأمان

- **Use Case:** A financial institution combines SSL/TLS with IPSec to secure data transmissions across different layers for online banking services.

تقوم مؤسسة مالية بدمجهما لتأمين نقل البيانات عبر الطبقات المختلفة لخدمات الإنترنت المصرفية

1.5 Converged Protocols

Definition: Protocols that combine different types of network traffic (e.g., data, voice, video) over a single network infrastructure.

بروتوكولات تجمع بين أنواع مختلفة من حركة مرور الشبكة مثل البيانات والصوت والفيديو عبر بنية تحتية واحدة للشبكة

Examples:

- **VoIP:** Transmits voice data over IP networks. الصوت عبر بروتوكول الإنترنت ينقل بيانات الصوت عبر شبكات آي بي
- **iSCSI:** Transmits storage data over IP networks. ينقل بيانات التخزين عبر الشبكات

- **Use Case:** An enterprise uses VoIP for its internal communication system to reduce telephony costs and integrate with its data network.

تستخدم المؤسسة لبروتوكول الاتصال الداخلي لتقليل تكاليف الهاتف والدمج مع شبكة البيانات الخاصة بها

1.6 Transport Architecture

Definition: The design and structure of how data is transported within a network.

تصميم وهيكل كيفية نقل البيانات داخل الشبكة

Examples:

- **Topology:** The physical and logical arrangement of a network. الطوبولوجيا الترتيب الفيزيائي

والمنطقي للشبكة

- **Data/Control/Management Plane:** Different layers that handle data transfer, control functions, and network management. طبقة البيانات التحكم الإدارة طبقات مختلفة تتعامل مع نقل البيانات ووظائف التحكم وإدارة الشبكة

- **Use Case:** A data center uses a hierarchical network topology to manage traffic efficiently and ensure high availability.

يستخدم مركز البيانات طوبولوجيا شبكة هرمية لإدارة حركة المرور بكفاءة وضمان التوافر العالي

1.7 Performance Metrics

Definition: Measurements that indicate the performance and efficiency of a network.

القياسات التي تشير إلى أداء وكفاءة الشبكة

Examples:

- **Bandwidth:** The maximum rate of data transfer. النطاق الترددي معدل نقل البيانات الأقصى

- **Latency:** The delay before a transfer of data begins following an instruction. الكمون التأخير قبل بدء نقل البيانات بعد التعليمات

- **Use Case:** An ISP monitors bandwidth and latency to ensure optimal performance for its customers.

يقوم مزود خدمة الإنترنت بمراقبة النطاق الترددي والكمون لضمان الأداء الأمثل لعملائه

1.8 Traffic Flows

Definition: Patterns of data transfer within a network.

أنماط نقل البيانات داخل الشبكة

Examples:

- **North-South Traffic:** Data transfer between clients and servers. حركة المرور الشمالية الجنوبية نقل البيانات بين العملاء والخوادم

- **East-West Traffic:** Data transfer between servers within a data center. حركة المرور الشرقية الغربية نقل البيانات بين الخوادم داخل مركز البيانات

- **Use Case:** A cloud service provider optimizes East-West traffic within its data centers to enhance application performance.

يقوم مزود خدمة السحابة بتحسين حركة المرور الشرقية الغربية داخل مراكز البيانات لتعزيز أداء التطبيقات

1.9 Physical Segmentation

Definition: Separating network components physically to enhance security.

فصل مكونات الشبكة فيزيائيًا لتعزيز الأمان

Examples:

- **In-Band Management:** Managing network devices through the same channels used for regular data traffic. إدارة في النطاق إدارة أجهزة الشبكة من خلال نفس القنوات المستخدمة لحركة مرور البيانات العادية

- **Out-of-Band Management:** Using separate channels for network management traffic. إدارة خارج النطاق استخدام قنوات منفصلة لحركة مرور إدارة الشبكة

- **Use Case:** An IT department uses out-of-band management to ensure network devices can be accessed even during outages.

تستخدم قسم تكنولوجيا المعلومات إدارة خارج النطاق لضمان إمكانية الوصول إلى أجهزة الشبكة حتى أثناء الانقطاعات

1.10 Logical Segmentation

Definition: Separating network traffic logically using technologies like VLANs and

VPNs.

فصل حركة مرور الشبكة منطقيًا باستخدام تقنيات مثل الشبكات المحلية الافتراضية والشبكات الافتراضية الخاصة

Examples:

- **VLANs:** Separate broadcast domains within a network. الشبكات المحلية الافتراضية فصل نطاقات البث داخل الشبكة
- **VPNs:** Create secure connections over the internet. الشبكات الافتراضية الخاصة إنشاء اتصالات آمنة عبر الإنترنت
- **Use Case:** A university uses VLANs to separate student and staff network traffic for security and management purposes.

تستخدم جامعة الشبكات المحلية الافتراضية لفصل حركة مرور الشبكة بين الطلاب والموظفين لأغراض الأمان والإدارة

1.11 Micro-Segmentation

Definition: Dividing a network into smaller segments to improve security and control.

تقسيم الشبكة إلى أجزاء أصغر لتحسين الأمان والتحكم

Examples:

- **Distributed Firewalls:** Applying firewall policies at a granular level. الجدران النارية الموزعة تطبيق سياسات الجدار الناري على مستوى دقيق
- **Zero Trust:** An approach that assumes no implicit trust within the network. عدم الثقة نهج يفترض عدم وجود ثقة ضمنية داخل الشبكة
- **Use Case:** A healthcare organization implements micro-segmentation to protect patient data and comply with regulations.

تقوم منظمة الرعاية الصحية بتنفيذ التقسيم الصغير لحماية بيانات المرضى والامتثال للوائح

1.12 Edge Networks

Definition: Networks located at the edge of the enterprise network, managing ingress and egress traffic.

الشبكات الموجودة على حافة شبكة المؤسسة التي تدير حركة المرور الواردة والصادرة

Examples:

- **Ingress/Egress:** Managing data entering and leaving the network. إدارة الدخول الخروج البيانات التي تدخل وتغادر الشبكة
- **Peering:** Establishing direct network connections with other networks. نظير إنشاء اتصالات شبكية مباشرة مع الشبكات الأخرى
- **Use Case:** A content delivery network (CDN) uses edge networks to cache content closer to users, reducing latency.

تستخدم شبكة توصيل المحتوى شبكات الحافة لتخزين المحتوى مؤقتًا بالقرب من المستخدمين، مما يقلل التأخير

1.13 Wireless Networks

Definition: Networks that use wireless technologies for communication.

الشبكات التي تستخدم التقنيات اللاسلكية للاتصال

Examples:

- **Wi-Fi:** Wireless local area network technology. واي فاي تقنية الشبكة المحلية اللاسلكية
- **Bluetooth:** Short-range wireless technology for connecting devices. بلوتوث تقنية لاسلكية قصيرة المدى لتوصيل الأجهزة
- **Use Case:** An office uses Wi-Fi to provide internet access to employees without the need for physical cables.

يستخدم مكتب واي فاي لتوفير الوصول إلى الإنترنت للموظفين دون الحاجة إلى كابلات فيزيائية

1.14 Cellular/Mobile Networks

Definition: Networks that provide wireless communication over large areas through mobile devices.

الشبكات التي توفر الاتصال اللاسلكي عبر مناطق واسعة من خلال الأجهزة المحمولة

Examples:

- **4G:** Fourth generation of mobile network technology. الجيل الرابع الجيل الرابع من تكنولوجيا شبكات المحمول
- **5G:** Fifth generation of mobile network technology. الجيل الخامس الجيل الخامس من تكنولوجيا شبكات المحمول

- **Use Case:** A logistics company uses 4G and 5G networks to track and communicate with delivery vehicles in real-time.

تستخدم شركة الخدمات اللوجستية شبكات الجيل الرابع والخامس لتتبع والتواصل مع مركبات التوصيل في الوقت الفعلي

1.15 Content Distribution Networks (CDN)

Definition: Networks of servers that deliver web content to users based on their geographic location.

شبكات من الخوادم التي توفر محتوى الويب للمستخدمين بناءً على موقعهم الجغرافي

Examples:

- Reducing latency by serving content from a location closer to the user. تقليل التأخير من خلال تقديم المحتوى من موقع أقرب إلى المستخدم

- **Use Case:** An online streaming service uses a CDN to provide high-quality video content to users around the world.

تستخدم خدمة البث عبر الإنترنت شبكة توصيل المحتوى لتوفير محتوى فيديو عالي الجودة للمستخدمين حول العالم

1.16 Software Defined Networks (SDN)

Definition: An approach to network management that enables dynamic and programmatically efficient network configuration.

نهج لإدارة الشبكة يمكّن من التكوين الديناميكي والكفء للبرامج

Examples:

- **API:** Allows interaction with SDN controllers. واجهة برمجة التطبيقات تسمح بالتفاعل مع وحدات تحكم الشبكة المعرفة بالبرمجيات

- **Network Functions Virtualization:** Decouples network functions from hardware. افتراضية وظائف الشبكة فصل وظائف الشبكة عن الأجهزة

- **Use Case:** A telecom provider uses SDN to manage and optimize network traffic dynamically in response to changing demands.

يستخدم مزود الاتصالات لإدارة وتحسين حركة مرور الشبكة ديناميكيًا استجابة للطلبات المتغيرة

1.17 Virtual Private Cloud (VPC)

Definition: A private cloud within a public cloud infrastructure.

سحابة خاصة داخل بنية تحتية سحابية عامة

Examples:

- Providing isolated network environments within a public cloud. توفير بيئات شبكية معزولة داخل سحابة عامة

- **Use Case:** A startup uses a VPC to host its applications securely within a public cloud while maintaining control over its network environment.

تستخدم شركة ناشئة سحابة خاصة افتراضية لاستضافة تطبيقاتها بأمان داخل سحابة عامة مع الحفاظ على السيطرة على بيئة الشبكة الخاصة بها

1.18 Monitoring and Management

Definition: Tools and processes to observe and control network performance and health.

الأدوات والعمليات لمراقبة وأداء الشبكة وصحتها

Examples:

- **Traffic Flow/Shaping:** Managing data transfer to ensure network efficiency. تدفق حركة المرور إدارة نقل البيانات لضمان كفاءة الشبكة
- **Fault Detection and Handling:** Identifying and addressing network issues. الكشف عن الأعطال ومعالجتها تحديد ومعالجة مشاكل الشبكة

- **Use Case:** A network operations center (NOC) uses monitoring tools to detect and resolve network issues proactively.

يستخدم مركز عمليات الشبكة أدوات المراقبة لاكتشاف وحل مشاكل الشبكة بشكل استباقي

1.19 Subnetting

Definition: Dividing a network into smaller, more efficient sub-networks or subnets.

تقسيم الشبكة إلى شبكات فرعية أصغر وأكثر كفاءة

Purpose: To improve network performance and security by reducing congestion and isolating network segments.

الهدف تحسين أداء الشبكة وأمانها عن طريق تقليل الازدحام وعزل أجزاء الشبكة

Examples and Calculations:

Class A Network:

- Original Subnet: 10.0.0.0/8
- Subnet Mask: 255.0.0.0
- New Subnet Mask: 255.255.0.0
- Number of Subnets: 256
- Hosts per Subnet: 65,534

Class B Network:

- Original Subnet: 172.16.0.0/16
- Subnet Mask: 255.255.0.0
- New Subnet Mask: 255.255.255.0
- Number of Subnets: 256
- Hosts per Subnet: 254

Class C Network:

- Original Subnet: 192.168.1.0/24
- Subnet Mask: 255.255.255.0
- New Subnet Mask: 255.255.255.240
- Number of Subnets: 16
- Hosts per Subnet: 14

- **Use Case:** A company divides its network into smaller subnets to enhance security and

improve traffic management. تقوم شركة بتقسيم شبكتها إلى شبكات فرعية أصغر لتعزيز الأمان وتحسين إدارة حركة المرور

Multiple Choice Questions

1. What is the primary purpose of VLANs in network design?

a. Increase bandwidth

b. Reduce latency

c. Logical segmentation

d. Physical segmentation

2. Which layer of the OSI model is responsible for data encryption?

a. Physical

b. Presentation

c. Network

d. Application

3. What is a use case for SDN in a telecom provider's network?

a. Enhancing physical security

b. Dynamic traffic management

c. Increasing latency

d. Reducing bandwidth

4. How does micro-segmentation improve network security?

a. By increasing the number of routers

b. By dividing the network into smaller segments

c. By using only wireless connections

d. By enhancing the physical layer

5. What is the purpose of a DMZ in network architecture?

a. To provide a buffer zone between the internal network and external threats

b. To increase internal network speed

c. To reduce the number of firewalls needed

d. To enhance physical security

Answers and Explanations

1. c. Logical segmentation

Explanation: VLANs are used for logical segmentation of network traffic within a network. تستخدم لتقسيم حركة مرور الشبكة منطقيًا داخل الشبكة

2. b. Presentation

Explanation: The presentation layer of the OSI model is responsible for data encryption and decryption. الطبقة العرض في نموذج أوس أي مسؤولة عن تشفير وفك تشفير البيانات

3. b. Dynamic traffic management

Explanation: SDN enables dynamic and programmatically efficient network configuration, useful for managing traffic. يمكّن من تكوين الشبكة بشكل ديناميكي وبرمجي فعال، وهو مفيد لإدارة حركة المرور

4. b. By dividing the network into smaller segments

Explanation: Micro-segmentation improves security by creating smaller, isolated network segments. يحسن التقسيم الصغير الأمان بإنشاء أجزاء أصغر ومعزولة من الشبكة

5. a. To provide a buffer zone between the internal network and external

threats

Explanation: A DMZ creates a buffer zone to protect the internal network from external threats. تقوم المنطقة منزوعة السلاح بإنشاء منطقة عازلة لحماية الشبكة الداخلية من التهديدات الخارجية

---

2. Network Security and Defense

2.1 Secure Network Components

2.1.1 Operation of Infrastructure

Definition: Ensuring that network infrastructure operates efficiently and reliably.

ضمان أن تعمل البنية التحتية للشبكة بكفاءة وموثوقية

Examples:

- **Redundant Power:** Using backup power sources to prevent downtime. استخدام مصادر الطاقة الاحتياطية لمنع التوقف
- **Warranty and Support:** Ensuring hardware is covered by warranty and support services. ضمان تغطية الأجهزة بضمان وخدمات الدعم

- **Use Case:** A data center uses redundant power supplies to ensure continuous operation during power outages.

يستخدم مركز البيانات إمدادات الطاقة الاحتياطية لضمان التشغيل المستمر أثناء انقطاع التيار الكهربائي

2.1.2 Transmission Media

- Definition: Physical pathways that carry network data signals.

المسارات الفيزيائية التي تحمل إشارات بيانات الشبكة

- Physical Security: Protecting transmission media from physical damage and interference. حماية وسائل النقل من التلف الفيزيائي والتداخل
- **Signal Propagation Quality:** Ensuring high-quality transmission by minimizing signal loss. ضمان جودة النقل عن طريق تقليل فقدان الإشارة

Use Case: Fiber optic cables are used in long-distance communication to ensure minimal signal loss and high-speed data transfer.

يتم استخدام كابلات الألياف البصرية في الاتصالات لمسافات طويلة لضمان فقدان إشارة ضئيل ونقل بيانات عالي السرعة

2.1.3 Network Access Control (NAC) Systems

Definition: Solutions that control access to network resources.

حلول تتحكم في الوصول إلى موارد الشبكة

Examples:

- **Physical Solutions:** Using physical devices to restrict access. استخدام الأجهزة الفيزيائية لتقييد الوصول
- **Virtual Solutions:** Using software-based approaches to control access. استخدام الأساليب المستندة إلى البرمجيات للتحكم في الوصول

Use Case: An organization implements NAC systems to ensure only authorized devices can connect to its network.

لضمان أن الأجهزة المصرح بها فقط يمكنها الاتصال بشبكتها NAC تقوم منظمة بتنفيذ أنظمة

2.1.4 Endpoint Security

Definition: Protecting network endpoints, such as computers and mobile devices, from security threats.

حماية نقاط النهاية الشبكية مثل أجهزة الكمبيوتر والأجهزة المحمولة من التهديدات الأمنية

Examples:

- **Host-Based Security:** Implementing security measures directly on devices. تنفيذ تدابير الأمان مباشرة على الأجهزة
- **Antivirus Software:** Using software to detect and remove malicious programs. استخدام البرامج لاكتشاف وإزالة البرامج الضارة
- **Use Case:** A company installs antivirus software on all employee devices to protect against malware.

تقوم شركة بتثبيت برامج مكافحة الفيروسات على جميع أجهزة الموظفين للحماية من البرمجيات الخبيثة

2.2 Defense in Depth

Definition: A multi-layered approach to security that includes multiple defense mechanisms to protect information.

نهج متعدد الطبقات للأمان يشمل آليات دفاعية متعددة لحماية المعلومات

- **Components:**

Network Segmentation / Partitioning: Dividing a network into smaller segments to enhance security. تجزئة الشبكة تقسيم الشبكة إلى أجزاء أصغر لتعزيز الأمان

o Network Perimeter: The boundary between an organization's internal network and external networks. محيط الشبكة الحدود بين الشبكة الداخلية للمؤسسة والشبكات الخارجية

o DMZ (Demilitarized Zone): A physical or logical subnetwork that contains and exposes an organization's external-facing services. المنطقة منزوعة السلاح شبكة فرعية فيزيائية أو منطقية تحتوي على خدمات المؤسسة المواجهة للخارج وتعرضها

o Bastion Host: A heavily secured server located on a network perimeter, used to defend against attacks. المضيف المعزز خادم مؤمن بشكل كبير يقع على محيط الشبكة، يستخدم للدفاع ضد الهجمات

o Proxy: A server that acts as an intermediary for requests from clients seeking

resources from other servers. وكيل خادم يعمل كوسيط لطلبات العملاء الباحثين عن موارد من خوادم أخرى

o NAT/PAT (Network Address Translation / Port Address Translation): A method of remapping IP addresses by modifying network address information in the IP header. ترجمة عنوان الشبكة/ترجمة عنوان المنفذ طريقة لإعادة تعيين عناوين عن طريق تعديل معلومات عنوان الشبكة في رأس بروتوكول الإنترنت

2.3 Firewalls

Definition: A network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

جهاز أمان شبكي يراقب ويتحكم في حركة المرور الشبكية الواردة والصادرة بناءً على قواعد أمان محددة مسبقًا

- **Types:**

• Packet Filtering Firewall: Filters packets based on IP addresses, ports, and protocols. جدار الحماية القائم على تصفية الحزم يصفي الحزم بناءً على عناوين والمنافذ والبروتوكولات

• Stateful Packet Filtering Firewall: Monitors the state of active connections and makes decisions based on the context of the traffic. جدار الحماية القائم على تصفية الحزم ذات الحالة يراقب حالة الاتصالات النشطة ويتخذ القرارات بناءً على سياق حركة المرور

• Circuit Proxy Firewall: Operates at the session layer to manage network traffic. جدار الحماية القائم على وكيل الدائرة يعمل في طبقة الجلسة لإدارة حركة المرور الشبكية

• Application Firewall: Inspects and controls traffic at the application layer. جدار الحماية القائم على التطبيقات يفحص ويتحكم في حركة المرور في طبقة التطبيقات

- **Famous Brands:**

• Cisco

• Palo Alto Networks

• Fortinet

• Check Point

• Juniper Networks

- **Use Case:** A company uses a stateful packet filtering firewall to monitor and manage network traffic, ensuring that only legitimate traffic is allowed.

تستخدم شركة جدار ناري يقوم بتصفية الحزم لمراقبة وإدارة حركة المرور الشبكية، مما يضمن السماح فقط لحركة المرور الشرعية

2.4 Inspection

Definition: Techniques used to examine and analyze network traffic to detect and respond to threats.

تقنيات تُستخدم لفحص وتحليل حركة مرور الشبكة لاكتشاف التهديدات والرد عليها

- **IDS/IPS Location:**

• Host-Based IDS/IPS: Installed on individual hosts to monitor and protect them. نظام كشف/منع التسلل القائم على المضيف يتم تثبيته على مضيفين فرديين لمراقبتهم وحمايتهم

• Network-Based IDS/IPS: Monitors network traffic across entire segments. نظام كشف/منع التسلل القائم على الشبكة يراقب حركة مرور الشبكة عبر أجزاء كاملة

- **IDS/IPS Detection Methods:**

• Pattern Matching: Detects threats based on known patterns. المطابقة النمطية تكتشف التهديدات بناءً على أنماط معروفة

• Anomaly Detection: Identifies deviations from normal behavior. كشف الشذوذ يحدد الانحرافات عن السلوك الطبيعي

• Statistical Analysis: Uses statistical methods to detect unusual activities. التحليل الإحصائي يستخدم الأساليب الإحصائية لاكتشاف الأنشطة غير العادية

• Signature Analysis: Compares network traffic against a database of known threat signatures. تحليل التوقيعات يقارن حركة مرور الشبكة بقاعدة بيانات من توقيعات التهديدات

المعروفة

- **IDS/IPS Types:**

• In-line: Placed directly in the path of network traffic to block or allow it. النظام المدمج يوضع مباشرة في مسار حركة مرور الشبكة لحظره أو السماح به

• Mirror: Receives a copy of network traffic for analysis. النظام المعكوس يستقبل نسخة من حركة مرور الشبكة للتحليل

• Span: Monitors traffic from specific ports or VLANs. النظام الممتد يراقب حركة المرور من منافذ محددة أو شبكات محلية افتراضية

• Protocol: Focuses on specific network protocols. النظام القائم على البروتوكول يركز على بروتوكولات شبكية محددة

• Stateful Matching: Tracks the state of network connections to detect threats. المطابقة الحالة تتبع حالة اتصالات الشبكة لاكتشاف التهديدات

• Traffic Analysis: Analyzes the overall flow of network traffic. تحليل حركة المرور يحلل التدفق العام لحركة مرور الشبكة

Techniques:

• **White & Black Lists:** Allow or block traffic based on pre-approved lists. القوائم البيضاء والسوداء السماح أو حظر حركة المرور بناءً على قوائم معتمدة مسبقًا

• Sandbox: Isolates suspicious files to observe their behavior. البيئة المعزولة تعزل الملفات المشبوهة لمراقبة سلوكها

- **Additional Tools:**

• **Honeypots:** Deceptive systems set up to attract attackers. المصائد الإلكترونية أنظمة خادعة تُعد لجذب المهاجمين

• **Honeynets:** Networks of honeypots designed to study attacker behavior. الشبكات الخادعة شبكات من المصائد الإلكترونية مصممة لدراسة سلوك المهاجمين

• **Ingress vs. Egress:** Ingress monitors incoming traffic, egress monitors outgoing traffic. الدخول مقابل الخروج يراقب الدخول حركة المرور الواردة، يراقب الخروج حركة المرور الصادرة

2.5 Advanced Endpoint Security Solutions

- **Endpoint Detection and Response (EDR):** A cybersecurity technology that continuously monitors and responds to advanced threats on endpoints. تقنية الأمن السيبراني التي تراقب وتستجيب باستمرار للتهديدات المتقدمة على النقاط النهائية

- **Network Detection and Response (NDR):** A cybersecurity technology that uses network traffic analysis to detect and respond to threats within the network. تقنية الأمن السيبراني التي تستخدم تحليل حركة مرور الشبكة لاكتشاف والرد على التهديدات داخل الشبكة

- **Extended Detection and Response (XDR):** An advanced security solution that integrates multiple security products into a unified system for comprehensive threat detection and response. حل أمني متقدم يدمج بين العديد من المنتجات الأمنية في نظام واحد لاكتشاف والرد الشامل على التهديدات

- **Use Case:** A financial institution uses EDR to monitor endpoints for advanced threats, NDR to analyze network traffic for anomalies, and XDR to unify threat detection across multiple security layers.

2.6 Network Access Control (NAC) Solutions

Definition: Solutions that control access to network resources by enforcing security policies.

حلول تتحكم في الوصول إلى موارد الشبكة بفرض سياسات الأمان

- **Top Brands:**

• Cisco Identity Services Engine (ISE)

• Aruba ClearPass

• ForeScout CounterACT

• Extreme Networks ExtremeControl

• Pulse Secure

- **How It Works:**

• **Authentication:** Verifies the identity of users and devices. المصادقة التحقق من هوية المستخدمين والأجهزة

• **Authorization:** Determines the level of access granted to users and devices. التفويض يحدد مستوى الوصول الممنوح للمستخدمين والأجهزة

• **Policy Enforcement:** Applies security policies to control access to network resources. فرض السياسات تطبيق سياسات الأمان للتحكم في الوصول إلى موارد الشبكة

• **Monitoring:** Continuously monitors network activity to detect and respond to security incidents. المراقبة مراقبة النشاط الشبكي باستمرار لاكتشاف والرد على الحوادث الأمنية

- **Use Case:** An enterprise uses NAC solutions to ensure only authenticated and authorized devices can access the corporate network, enforcing security policies and monitoring for suspicious activities.

تستخدم مؤسسة تلك الحلول لضمان أن الأجهزة المصادقة والمفوضة فقط يمكنها الوصول إلى شبكة الشركة، وتطبيق سياسات الأمان ومراقبة الأنشطة المشبوهة

2.7 Intrusion Prevention Systems (IPS) and Next-Generation IPS (NGIPS)

Definition: Systems that monitor network traffic for malicious activity and take action to prevent it.

أنظمة تراقب حركة مرور الشبكة للنشاطات الخبيثة وتتخذ إجراءات لمنعها

- **IPS vs. NGIPS:**

• IPS: Traditional IPS focuses on detecting and blocking known threats using signatures and pattern matching. نظام منع التسلل التقليدي يركز على اكتشاف وحظر التهديدات المعروفة باستخدام التوقيعات والمطابقة النمطية

• NGIPS: Next-Generation IPS includes advanced features like application awareness, contextual analysis, and integrated threat intelligence for detecting and preventing sophisticated threats. نظام منع التسلل الجيل القادم يشمل ميزات متقدمة مثل الوعي بالتطبيقات، التحليل السياقي، والاستخبارات التهديدات المتكاملة لاكتشاف ومنع التهديدات المعقدة

- **Top Brands:**

• Cisco Firepower

• Palo Alto Networks Threat Prevention

• Fortinet FortiGate IPS

• McAfee Network Security Platform

• Trend Micro TippingPoint

- **Use Case:** A financial institution uses NGIPS to detect and block sophisticated cyber-attacks, integrating threat intelligence for real-time protection.

تستخدم مؤسسة مالية نظام منع التسلل الجيل القادم لاكتشاف وحظر الهجمات السيبرانية المعقدة، وتكامل الاستخبارات التهديدات للحماية في الوقت الحقيقي

Multiple Choice Questions

1. What is the primary advantage of using NGIPS over traditional IPS?

a. Increased network speed

b. Application awareness and contextual analysis

c. Reduced cost

d. Simplified configuration

2. Which security solution continuously monitors endpoints for advanced threats?

a. NDR

b. EDR

c. NAC

d. IPS

3. How does XDR improve threat detection and response?

a. By increasing bandwidth

b. By integrating multiple security products into a unified system

c. By simplifying user interfaces

d. By reducing latency

4. What is a key feature of a honeynet?

a. Encrypting data

b. Attracting attackers to study their behavior

c. Increasing network speed

d. Reducing bandwidth usage

5. Which NAC solution brand is known for enforcing security policies and monitoring network activity?

a. Palo Alto Networks

b. Cisco Identity Services Engine (ISE)

c. Fortinet

d. Trend Micro

Answers and Explanations

1. b. Application awareness and contextual analysis

Explanation: NGIPS includes advanced features like application awareness and contextual analysis to detect and prevent sophisticated threats. يشمل نظام منع التسلل الجيل القادم ميزات متقدمة مثل الوعي بالتطبيقات والتحليل السياقي لاكتشاف ومنع

التهديدات المعقدة

2. b. EDR

Explanation: Endpoint Detection and Response (EDR) solutions continuously monitor endpoints for advanced threats and provide visibility and analytics. تراقب حلول الكشف والاستجابة للنقاط النهائية التهديدات المتقدمة باستمرار وتوفر الرؤية والتحليلات

3. b. By integrating multiple security products into a unified system

Explanation: XDR improves threat detection and response by integrating multiple security products into a single, unified system for comprehensive protection. يحسن اكتشاف التهديدات والاستجابة لها عن طريق دمج العديد من المنتجات الأمنية في نظام واحد موحد للحماية الشاملة

4. b. Attracting attackers to study their behavior

Explanation: A honeynet is a network of honeypots designed to attract attackers and study their behavior to improve security defenses. الشبكة الخادعة هي شبكة من المصائد الإلكترونية مصممة لجذب المهاجمين ودراسة سلوكهم لتحسين الدفاعات الأمنية

5. b. Cisco Identity Services Engine (ISE)

Explanation: Cisco Identity Services Engine (ISE) is a NAC solution known for enforcing security policies and continuously monitoring network activity. تُعرف بأنها حل يفرض سياسات الأمان ويراقب نشاط الشبكة باستمرار

---

3. Implement Secure Communication Channels According to Design

3.1 Voice, Video, and Collaboration

Definition: Securely managing communication channels used for voice, video, and collaboration tools.

إدارة قنوات الاتصال بأمان المستخدمة في أدوات الصوت والفيديو والتعاون

Examples:

- **Conferencing:** Using secure protocols for online meetings. استخدام البروتوكولات الآمنة للاجتماعات عبر الإنترنت
- **Zoom Rooms:** Secure configurations for virtual meeting rooms. تكوينات آمنة لغرف الاجتماعات الافتراضية
- **Use Case:** A multinational corporation uses secure video conferencing tools to facilitate communication between teams in different countries. تستخدم شركة متعددة الجنسيات أدوات المؤتمرات عبر الفيديو الآمنة لتسهيل الاتصال بين الفرق في بلدان مختلفة

3.2 Remote Access

Definition: Securely accessing network resources from remote locations.

الوصول الآمن إلى موارد الشبكة من مواقع بعيدة

Examples:

- **Network Administrative Functions:** Securely managing network devices from a remote location. إدارة أجهزة الشبكة بأمان من موقع بعيد
- **Virtual Private Networks (VPNs):** Creating secure connections over the internet. إنشاء اتصالات آمنة عبر الإنترنت
- **Use Case:** IT administrators use VPNs to securely access and manage network resources while working remotely. يستخدم مسؤولو تكنولوجيا المعلومات الشبكات الافتراضية الخاصة للوصول إلى موارد الشبكة وإدارتها بأمان أثناء العمل عن بُعد

3.3 Data Communications

Definition: Securely transmitting data across networks.

نقل البيانات بأمان عبر الشبكات

Examples:

- **Backhaul Networks:** Secure connections for data transfer between distant locations. اتصالات الباكهول اتصالات آمنة لنقل البيانات بين المواقع البعيدة
- **Satellite Communications:** Secure transmission of data via satellites. نقل البيانات بأمان عبر الأقمار الصناعية

- **Use Case:** A telecommunications company uses secure backhaul networks to transmit data between regional offices. تستخدم شركة الاتصالات شبكات الباكهول الآمنة لنقل البيانات بين المكاتب الإقليمية

3.4 Third-Party Connectivity

Definition: Managing secure connections between the network and third-party systems or services.

إدارة الاتصالات الآمنة بين الشبكة والأنظمة أو الخدمات الخارجية

Examples:

- **Vendor Access:** Securely granting access to vendors for system maintenance. منح الوصول الآمن للبائعين لصيانة النظام
- **Cloud Services:** Ensuring secure connections to cloud service providers. ضمان الاتصالات الآمنة مع مزودي خدمات السحابة

- **Use Case:** An enterprise uses secure third-party connectivity to allow cloud service providers to maintain its applications without compromising security. تستخدم مؤسسة الاتصالات الآمنة مع الأطراف الثالثة للسماح لمزودي خدمات السحابة بصيانة تطبيقاتها دون المساس بالأمان

Multiple Choice Questions

1. What is the primary purpose of using secure protocols in conferencing?

a. To increase meeting length

b. To improve video quality

c. To ensure data security

d. To enhance user experience

2. How does a Virtual Private Network (VPN) contribute to secure remote access?

a. By increasing network speed

b. By encrypting data transmissions

c. By improving user interfaces

d. By enhancing bandwidth

3. What is a key function of backhaul networks in data communications?

a. To increase storage capacity

b. To secure data transfer between distant locations

c. To manage user accounts

d. To enhance video quality

4. Why is vendor access management important in third-party connectivity?

a. To increase network speed

b. To improve encryption

c. To securely grant access for system maintenance

d. To enhance user experience

5. What is the primary benefit of using secure satellite communications?

a. To reduce signal interference

b. To increase data storage

c. To secure data transmission

d. To improve user interfaces

Answers and Explanations

1. **c. To ensure data security**

Secure protocols in conferencing ensure that the data transmitted during meetings is protected from unauthorized access. البروتوكولات الآمنة في المؤتمرات تضمن أن البيانات المنقولة خلال الاجتماعات محمية من الوصول غير المصرح به

2. **b. By encrypting data transmissions**

A Virtual Private Network (VPN) secures remote access by encrypting data transmissions between the user and the network. الشبكة الافتراضية الخاصة تؤمن الوصول عن بعد عن طريق تشفير نقل البيانات بين المستخدم والشبكة

3. **b. To secure data transfer between distant locations**

Backhaul networks are used to secure data transfer between distant locations, ensuring the integrity and confidentiality of the data. تستخدم شبكات الباكهول لنقل البيانات بأمان بين المواقع البعيدة مما يضمن سلامة وسرية البيانات

4. **c. To securely grant access for system maintenance**

Vendor access management ensures that vendors can securely access the system for

maintenance without compromising security. إدارة وصول البائعين تضمن أن البائعين يمكنهم الوصول بأمان إلى النظام للصيانة دون المساس بالأمان

5. **c. To secure data transmission**

Secure satellite communications protect data transmission from interception and unauthorized access. تحمي اتصالات الأقمار الصناعية الآمنة نقل البيانات من الاعتراض والوصول غير المصرح به

---

4. Remote Access

4.1 Tunneling

Definition: Technologies that encapsulate and transmit data securely through tunnels.

تقنيات تغلف وتنقل البيانات بأمان من خلال الأنفاق

Technologies:

- **GRE:** Generic Routing Encapsulation. تغليف التوجيه العام
- **PPTP:** Point-to-Point Tunneling Protocol. بروتوكول الأنفاق من نقطة إلى نقطة
- **L2TP:** Layer 2 Tunneling Protocol. بروتوكول الأنفاق الطبقة الثانية
- **Split Tunneling:** Directs some traffic through a secure VPN tunnel while allowing other traffic to access the internet directly. توجيه بعض حركة المرور عبر نفق آمن بينما يسمح لحركة المرور الأخرى بالوصول إلى الإنترنت مباشرة

- **Use Case:** A company uses L2TP for secure remote access, ensuring data is encapsulated and transmitted securely between remote users and the corporate network. تستخدم شركة للوصول الآمن عن بُعد، مما يضمن تغليف البيانات ونقلها بأمان بين المستخدمين عن بُعد وشبكة الشركة

4.2 Encryption

Definition: The process of encoding data to prevent unauthorized access.

عملية تشفير البيانات لمنع الوصول غير المصرح به

- **Use Case:** Remote employees use encrypted communication channels to ensure the confidentiality of sensitive business data. يستخدم الموظفون عن بُعد قنوات اتصال مشفرة لضمان سرية البيانات التجارية الحساسة

4.3 VPN (Tunneling + Encryption)

Definition: Virtual Private Networks combine tunneling and encryption to secure data transmission over public networks.

تجمع الشبكات الخاصة الافتراضية بين الأنفاق والتشفير لتأمين نقل البيانات عبر الشبكات العامة

- **Use Case:** A company deploys a VPN to allow remote workers to securely connect to the corporate network, protecting data from interception. تقوم شركة بنشر شبكة افتراضية خاصة للسماح للعاملين عن بُعد بالاتصال بأمان بشبكة الشركة، مما يحمي البيانات من الاعتراض

4.4 IPSec

Definition: A suite of protocols designed to secure Internet Protocol (IP) communications.

مجموعة من البروتوكولات المصممة لتأمين اتصالات بروتوكول الإنترنت

- **Components:**

-Authentication Header (AH): Provides data integrity, authentication, and anti-replay. يوفر تكامل البيانات والمصادقة ومكافحة إعادة التشغيل

-Encapsulating Security Payload (ESP): Provides confidentiality, data origin authentication, and anti-replay. يوفر السرية ومصادقة أصل البيانات ومكافحة إعادة التشغيل

- **Modes:**

-Transport Mode: Encrypts only the payload of the IP packet. يشفر حمولة حزمة فقط

-Tunnel Mode: Encrypts the entire IP packet. يشفر حزمة بالكامل

- **Processes:**

-IKE (Internet Key Exchange): Establishes a shared security policy and authenticated keys. يحدد سياسة الأمان المشتركة والمفاتيح المصدق عليها

-Security Association (SA): A set of policies and keys used to secure a network connection. مجموعة من السياسات والمفاتيح المستخدمة لتأمين اتصال الشبكة

-Mutual Authentication: Both parties verify each other's identity. يتحقق الطرفان من هوية بعضهما البعض

- **Use Case:** An enterprise uses IPSec to secure communications between remote offices, ensuring data is protected during transmission. تستخدم مؤسسة لتأمين الاتصالات بين المكاتب البعيدة، مما يضمن حماية البيانات أثناء النقل

4.5 Remote Authentication

Definition: Protocols used to authenticate remote users accessing a network.

البروتوكولات المستخدمة لمصادقة المستخدمين البعيدين الذين يصلون إلى الشبكة

- **Protocols:**

-RADIUS: Remote Authentication Dial-In User Service. خدمة مصادقة المستخدمين عن بُعد

-TACACS+: Terminal Access Controller Access-Control System Plus. نظام تحكم الوصول إلى وحدة التحكم الطرفية بلس

-Diameter: A protocol for authentication, authorization, and accounting. بروتوكول للمصادقة والتفويض والمحاسبة

- **Use Case:** A university uses RADIUS to authenticate students and staff accessing the campus network remotely. تستخدم جامعة لمصادقة الطلاب والموظفين الذين يصلون إلى شبكة الحرم الجامعي عن بُعد

4.6 Remote Access / Management

Definition: Tools and methods used to manage network devices and resources from remote locations.

الأدوات والأساليب المستخدمة لإدارة أجهزة الشبكة والموارد من المواقع البعيدة

Examples:

- **SNMP (Simple Network Management Protocol):** Monitors and manages network devices. يراقب ويدير أجهزة الشبكة

- **Telnet:** Provides remote access to network devices. يوفر الوصول عن بعد إلى أجهزة الشبكة

- **Use Case:** Network administrators use SNMP to monitor the health and performance of devices across the organization from a central location. يستخدم مسؤولو الشبكة لمراقبة صحة وأداء الأجهزة في جميع أنحاء المنظمة من موقع مركزي

Multiple Choice Questions

1- What is the primary purpose of a VPN?

a. To increase internet speed

b. To secure data transmission over public networks

c. To improve user interfaces

d. To enhance bandwidth

2- Which tunneling protocol encapsulates data at the network layer?

a. GRE

b. PPTP

c. L2TP

d. Split Tunneling

3- How does IPSec Tunnel Mode differ from Transport Mode?

a. Tunnel Mode encrypts only the payload

b. Transport Mode encrypts the entire IP packet

c. Tunnel Mode encrypts the entire IP packet

d. Transport Mode does not use encryption

4- What is a key feature of RADIUS in remote authentication?

a. Provides encryption for data transmission

b. Monitors network devices

c. Authenticates remote users accessing a network

d. Secures communications between offices

5- Which tool provides remote access to network devices?

a. SNMP

b. Telnet

c. RADIUS

d. IKE

Answers and Explanations

1- b. To secure data transmission over public networks

A Virtual Private Network (VPN) secures data transmission over public networks by encrypting data between the user's device and the network. الشبكة الافتراضية الخاصة تؤمن نقل البيانات عبر الشبكات العامة عن طريق تشفير البيانات بين جهاز المستخدم والشبكة

2- c. L2TP

Layer 2 Tunneling Protocol (L2TP) encapsulates data at the network layer, providing secure data transmission. بروتوكول الأنفاق الطبقة الثانية يغلف البيانات عند طبقة الشبكة، مما يوفر نقل بيانات آمن

3- c. Tunnel Mode encrypts the entire IP packet

IPSec Tunnel Mode encrypts the entire IP packet, while Transport Mode encrypts only the payload. يشفر وضع النفق لـ حزمة بأكملها، بينما ال اى بى يشفر وضع النقل الحمولة فقط

4- c. Authenticates remote users accessing a network

RADIUS is used to authenticate remote users accessing a network, ensuring secure access. يستخدم لمصادقة المستخدمين البعيدين الذين يصلون إلى الشبكة، مما يضمن الوصول الآمن

5- b. Telnet

Telnet provides remote access to network devices, allowing administrators to manage them from remote locations. يوفر الوصول عن بعد إلى أجهزة الشبكة، مما يسمح للمسؤولين بإدارتها من المواقع البعيدة

---

5. Network Attacks

5.1 Phases of Network Attacks

Definition: The various stages an attacker goes through to compromise a network.

المراحل المختلفة التي يمر بها المهاجم لاختراق الشبكة

- Phases:

1. Reconnaissance: Gathering information about the target network.

الاستطلاع جمع المعلومات عن الشبكة المستهدفة

2. Enumeration: Identifying valid accounts and resources.

العد تحديد الحسابات والموارد الصالحة

3. Vulnerability Analysis: Identifying weaknesses that can be exploited.

تحليل الثغرات تحديد نقاط الضعف التي يمكن استغلالها

4. Exploitation: Taking advantage of identified vulnerabilities to gain unauthorized access.

الاستغلال الاستفادة من الثغرات المحددة للوصول غير المصرح به

- **Use Case:** An attacker uses reconnaissance techniques to gather information about a company's network before attempting to exploit identified vulnerabilities.

يستخدم المهاجم تقنيات الاستطلاع لجمع المعلومات عن شبكة الشركة قبل محاولة استغلال الثغرات المحددة

5.2 Types of Network Attacks

Definition: Various methods used by attackers to compromise network security.

الطرق المختلفة التي يستخدمها المهاجمون لاختراق أمان الشبكة

Types:

1. Eavesdropping: Intercepting and listening to network traffic.

التنصت اعتراض والاستماع إلى حركة مرور الشبكة

Example: Using packet sniffers to capture unencrypted data.

استخدام ملتقط الحزم لالتقاط البيانات غير المشفرة

- **Use Case:** An attacker uses a packet sniffer to capture login credentials transmitted over an unencrypted connection.

يستخدم المهاجم ملتقط الحزم لالتقاط بيانات تسجيل الدخول المرسلة عبر اتصال غير مشفر

- **Mitigation Controls:**

o Use encryption protocols: Implement SSL/TLS for secure communication.

استخدام بروتوكولات التشفير لتنفيذ الاتصال الآمن

-Example: Implementing **SSL/TLS** on a web server to ensure data is encrypted during transmission. **Brands: DigiCert, GlobalSign.**

تنفيذها على خادم ويب لضمان تشفير البيانات أثناء النقل

o Monitor network traffic: Use IDS/IPS to detect unusual activities.

مراقبة حركة مرور الشبكة واستخدامه لاكتشاف الأنشطة غير العادية

-Example: Deploying ***Snort*** (an open-source IDS/IPS) to monitor network traffic for suspicious activity. (نظام كشف ومنع التسلل مفتوح المصدر) لمراقبة حركة مرور الشبكة للنشاط المشبوه

---

2. SYN Flooding: Overwhelming a server with a flood of SYN requests to exhaust resources.

هجوم الفيضانات إغراق الخادم بوابل من الطلبات لاستنزاف الموارد

Example: Sending a large number of SYN packets to a web server.

إرسال عدد كبير من الحزم إلى خادم ويب

- **Use Case:** A DDoS attack involves sending a flood of SYN requests to a web server, causing it to crash or become unresponsive.

هجوم يتضمن إرسال وابل من الطلبات إلى خادم ويب، مما يؤدي إلى تعطله أو عدم استجابته

- **Mitigation Controls:**

o Rate limiting: Limit the number of incoming SYN requests.

تحديد المعدل تحديد عدد الطلبات الواردة

-Example: Configuring rate limiting on a firewall to restrict the number of SYN requests from a single source. **Brands: Cisco, Palo Alto Networks.**تكوين تحديد المعدل على جدار الحماية لتقييد عدد طلبات من مصدر واحد

o SYN cookies: Use SYN cookies to handle excess SYN requests.

ملفات تعريف الارتباط استخدام ملفات تعريف الارتباط للتعامل مع طلبات الزائدة

-Example: Enabling SYN cookies on a Linux server to prevent SYN flood attacks.

مثال تمكين ملفات تعريف الارتباط على خادم لمنع هجمات الفيضانات

---

3. IP Spoofing: Sending packets with a forged IP address to impersonate another device.

انتحال إرسال حزم أى بى بعنوان مزيف لانتحال هوية جهاز آخر

Example: Crafting packets with a fake source IP address.

صياغة حزم بعنوان مزيف

- **Use Case:** An attacker uses IP spoofing to impersonate a trusted device and gain access to

restricted areas of a network.

يستخدم المهاجم انتحال أى بى لانتحال هوية جهاز موثوق به والوصول إلى المناطق المقيدة من الشبكة

- **Mitigation Controls:**

o Ingress filtering: Block packets with suspicious source addresses.

تصفية الدخول حظر الحزم بعناوين مصدر مشبوهة

-Example: Configuring ingress filtering on a router to block packets with invalid source IP addresses. Brands: Juniper Networks, Check Point.مثال تكوين تصفية الدخول على جهاز توجيه لحظر الحزم ذات عناوين المصدر غير الصالحة

o Strong authentication: Implement strong authentication mechanisms.

المصادقة القوية تنفيذ آليات المصادقة القوية

-Example: Using two-factor authentication (2FA) to verify user identity. Brands: RSA, Google Authenticator.مثال استخدام المصادقة الثنائية للتحقق من هوية المستخدم

---

4. DoS/DDoS: Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks disrupt services by overwhelming them with traffic.

هجمات حجب الخدمة وهجمات حجب الخدمة الموزعة تعطل الخدمات بإغراقها بحركة المرور

Example: Botnets used to launch a DDoS attack.

استخدام الشبكات الروبوتية لشن هجوم

- **Use Case:** A botnet is used to flood an online retailer's website with traffic, rendering it inaccessible to legitimate users.

يتم استخدام شبكة روبوتية لإغراق موقع تاجر تجزئة عبر الإنترنت بحركة المرور، مما يجعله غير متاح للمستخدمين الشرعيين

- **Mitigation Controls:**

o Traffic analysis: Use NDR to monitor and analyze network traffic.

تحليل حركة المرور استخدام الاداة لمراقبة وتحليل حركة مرور الشبكة

-Example: Implementing Darktrace for network traffic analysis to detect and mitigate DDoS attacks.

o Blackholing: Redirect malicious traffic to a non-existent server.

الإرسال إلى عنوان غير موجود إعادة توجيه حركة المرور الضارة إلى خادم غير موجود

-Example: Configuring blackholing on a router to drop malicious traffic. Brands: Cisco, Fortinet.

---

5. Man-in-the-Middle (MitM): Intercepting and altering communication between two parties without their knowledge.

هجوم الرجل في الوسط اعتراض وتعديل الاتصال بين طرفين دون علمهما

Example: Intercepting communications between a user and a website.

اعتراض الاتصالات بين المستخدم وموقع الويب

- **Use Case:** An attacker intercepts and modifies financial transactions between a user and their bank.

يعترض المهاجم ويعدل المعاملات المالية بين المستخدم وبنكه

- **Mitigation Controls:**

o Public key infrastructure (PKI): Use PKI to secure communications.

البنية التحتية للمفتاح العام استخدام لتأمين الاتصالات

-Example: Deploying a PKI system to ensure secure communication channels. Brands: Symantec, Entrust.نشر نظام -لضمان قنوات الاتصال الآمن

o VPNs: Implement VPNs to encrypt communication channels.

الشبكات الافتراضية الخاصة تنفيذ الشبكات الافتراضية الخاصة لتشفير قنوات الاتصال

-Example: Using Cisco AnyConnect VPN to secure remote communications. لتأمين الاتصالات عن بُعد.

---

6. ARP Poisoning: Sending fake ARP (Address Resolution Protocol) messages to associate the attacker's MAC address with a legitimate IP address.

تسميم إرسال رسائل مزيفة لربط عنوان الخاص بالمهاجم بعنوان شرعي

Example: Associating the attacker's MAC address with the IP address of a gateway.

ربط العنوان الخاص بالمهاجم بعنوان للبوابة

- **Use Case:** An attacker uses ARP poisoning to redirect network traffic through their device for eavesdropping or manipulation.

يستخدم المهاجم التسميم لإعادة توجيه حركة مرور الشبكة عبر جهازه للتنصت أو التلاعب

- **Mitigation Controls:**

o Static ARP entries: Use static ARP entries to prevent spoofing.

Example: Configuring static ARP entries on critical network devices. Brands: HP, Dell. تكوين إدخالات الثابتة على أجهزة الشبكة الحيوية

o Dynamic ARP inspection: Implement dynamic ARP inspection to detect and prevent ARP attacks.

Example: Enabling Dynamic ARP Inspection (DAI) on Cisco switches to prevent ARP

spoofing attacks.

Multiple Choice Questions

1. What is the first phase of a network attack?

a. Enumeration

b. Exploitation

c. Reconnaissance

d. Vulnerability Analysis

2. What type of attack involves intercepting and altering communication between two parties?

a. DoS

b. Man-in-the-Middle

c. IP Spoofing

d. ARP Poisoning

3. How does ARP poisoning affect network communication?

a. By encrypting data packets

b. By sending fake ARP messages to associate the attacker's MAC address with a legitimate IP address

c. By overwhelming the server with traffic

d. By altering DNS records

4. What is the primary goal of a DDoS attack?

a. To intercept communication

b. To impersonate another device

c. To disrupt services by overwhelming them with traffic

d. To eavesdrop on network traffic

5. What is the main purpose of using IP spoofing in an attack?

a. To capture unencrypted data

b. To send packets with a forged IP address to impersonate another device

c. To overwhelm a server with traffic

d. To alter communication between two parties

Answers and Explanations

1. c. Reconnaissance

The first phase of a network attack is reconnaissance, where the attacker gathers information about the target network.

المرحلة الأولى من الهجوم على الشبكة هي الاستطلاع، حيث يجمع المهاجم المعلومات عن الشبكة المستهدفة

2. b. Man-in-the-Middle

A Man-in-the-Middle attack involves intercepting and altering communication between two parties without their knowledge.

يتضمن هجوم الرجل في الوسط اعتراض وتعديل الاتصال بين طرفين دون علمهما

3. b. By sending fake ARP messages to associate the attacker's MAC address with a legitimate IP address

ARP poisoning involves sending fake ARP messages to associate the attacker's MAC address with a legitimate IP address, redirecting network traffic through the attacker's device.

يتضمن تسميم إرسال رسائل مزيفة لربط عنوان الخاص بالمهاجم بعنوان شرعي، وإعادة توجيه حركة مرور الشبكة عبر جهاز المهاجم

4. c. To disrupt services by overwhelming them with traffic

The primary goal of a DDoS attack is to disrupt services by overwhelming them with a flood of traffic, rendering them inaccessible.

الهدف الأساسي من هجوم هو تعطيل الخدمات بإغراقها بوابل من حركة المرور، مما يجعلها غير متاحة

5. b. To send packets with a forged IP address to impersonate another device

IP spoofing involves sending packets with a forged IP address to impersonate another device, often to bypass security measures or gain unauthorized access.

يتضمن انتحال إرسال حزم بعنوان مزيف لانتحال هوية جهاز آخر، غالبًا لتجاوز إجراءات الأمان أو الوصول غير المصرح به

Conclusion

This module provided a comprehensive overview of communication and network security principles. It covered secure network design, the operation of secure network components, the implementation of secure communication channels, and secure remote access. Additionally, it explored various types of network attacks and their mitigation controls. By understanding these principles, one can effectively design, implement, and manage secure network infrastructures to protect against emerging threats and vulnerabilities.

قدم هذا الفصل نظرة شاملة على مبادئ الاتصال والأمان الشبكي وتناول تصميم الشبكة الآمنة وتشغيل مكونات الشبكة الآمنة وتنفيذ قنوات الاتصال الآمنة والوصول الآمن عن بُعد. بالإضافة إلى ذلك، استكشاف أنواع مختلفة من الهجمات الشبكية ووسائل التخفيف منها. من

خلال فهم هذه المبادئ، يمكن للمرء تصميم وتنفيذ وإدارة البنية التحتية للشبكة الآمنة بفعالية لحمايتها من التهديدات والثغرات الناشئة

Resources

1- Official (ISC)² CISSP Study Guide

2- CISSP (ISC)² Official Practice Tests

3- CISSP All-in-One Exam Guide by Shon Harris

4- Cybrary – CISSP Training by Kelly Handerhan

https://www.cybrary.it/course/cissp

5- Oreilly – CISSP Training by Sari Greene

https://www.oreilly.com/library/view/cissp-4th-edition/9780135328613/?_gl=1*jwhz1z*_ga*MTgyMDY2NDI5LjE3MTczNzAwMDI.*_ga_092EL089CH*MTcxNzM3MDAwMi4xLjEuMTcxNzM3MDEwNi41OC4wLjA.

6- CISSP bundles by Thor Pedersen

https://thorteaches.com/cissp/

7- CISSP MindMaps YouTube Playlist from Destination Certification

https://www.youtube.com/playlist?list=PLZKdGEfEyJhLd-pJhAD7dNbJyUgpqI4pu

Ahmad Mohamed Zidan 1mo
CCNA || Network Security || Cyber ops

معلش هو حضرتك بتشرح اخر اصدار للمنهج صح !؟

Like · Reply

See more comments

To view or add a comment, sign in

More articles by this author

Module 7: Security Operations / إدارة عمليات...
Aug 5, 2024

Module 6: Security Assessment and Testing...
Jul 28, 2024

CISSP Module 5: Identi and Access Manageme
Jul 8, 2024

See all

Insights from the community

Computer Network Operations

How do you optimize the performance and accuracy of your network protocol analysis tools in CNO?

Computer Networking

How can you evaluate the security of your OSPF implementation?

Network Security

What is the purpose of TCP port scanning and how can it be used for Network Security?

Information Security

How do you assess the risks and vulnerabilities of your microsegmented SDN network?

Network Security

How can you configure TCP timeouts to improve security?

Network Security

How do you test the security of legacy systems in your network?

Show more

Others also viewed

❗The problem with monolithic network stacks

Ronald Bartels · 3y

Part 3: Harnessing the Power of STIGs for Network Devices: A Guide for Routers and Switches

Jeff Glenn, CCNA, CAPM · 1y

Securing Networks Requires a Global Perspective

Steve Goeringer · 7y

At ADI Expo London: Hikvision Appointed CVE Numbering Authority

Astrid Van Norden · 6y

❗SD-WAN use cases: Centralized firewalls

Ronald Bartels · 3y

Cimetrics will be demonstrating their new BACnet routers that solve tough BACnet segmentation problems found on both BACnet/IP and BACnet/SC networks

Cimetrics · 1y

Show more

Explore topics

Sales

Marketing

Business Administration

HR Management

Content Management

Engineering

Soft Skills

See All

إدارة الهوية والوصول
Identity and Access Management

Emad M. Abdelhamid • 2nd
Technical Leader | SME IT Security Design @ Cisco - CX EMEA . ...
View my portfolio
+ Follow
3w • Edited •

لسلام عليكم ورحمة الله وبركاته
اليوم بإذن الله سنقدم مختصر عن الفصل الخامس (إدارة الهوية والوصول) من الشرح المختصر لشهادة ال
CISSP
يغطي هذا الفصل المبادئ الأساسية لإدارة الهوية والوصول بما في ذلك التعريف والمصادقة والتفويض والمساءلة.
ويركز على تصميم وتنفيذ أطر وفهم التقنيات والبروتوكولات المختلفة المستخدمة في إدارة الهوية والوصول واستكشاف أفضل الممارسات لإدارة هويات المستخدمين وضوابط الوصول.
الهدف هو توفير فهم شامل لكيفية حماية الأنظمة والبيانات من خلال إدارة من يمكنه الوصول إلى الموارد وفي ظل أي ظروف بشكل فعال.

ويحتوى على 8 أجزاء
It contains 8 parts

1. - التحكم في الوصول المادي والمنطقي إلى الأصولControl Physical and Logical Access to Assets
2. - تحديد التصميم واستراتيجية المصادقةDesign Identification and Authentication Strategy
3. - الهوية الموحدة مع خدمة الطرف الثالثFederated Identity with a Third-Party Service

4. - تنفيذ وإدارة آليات التفويضImplement and Manage Authorization Mechanisms

5. - إدارة دورة حياة توفير الهوية والوصولManage the Identity and Access Provisioning Lifecycle

6. - تنفيذ أنظمة المصادقةImplement Authentication Systems

7. - تقنيات إدارة الهوية والوصولIdentity and Access Management Technologies

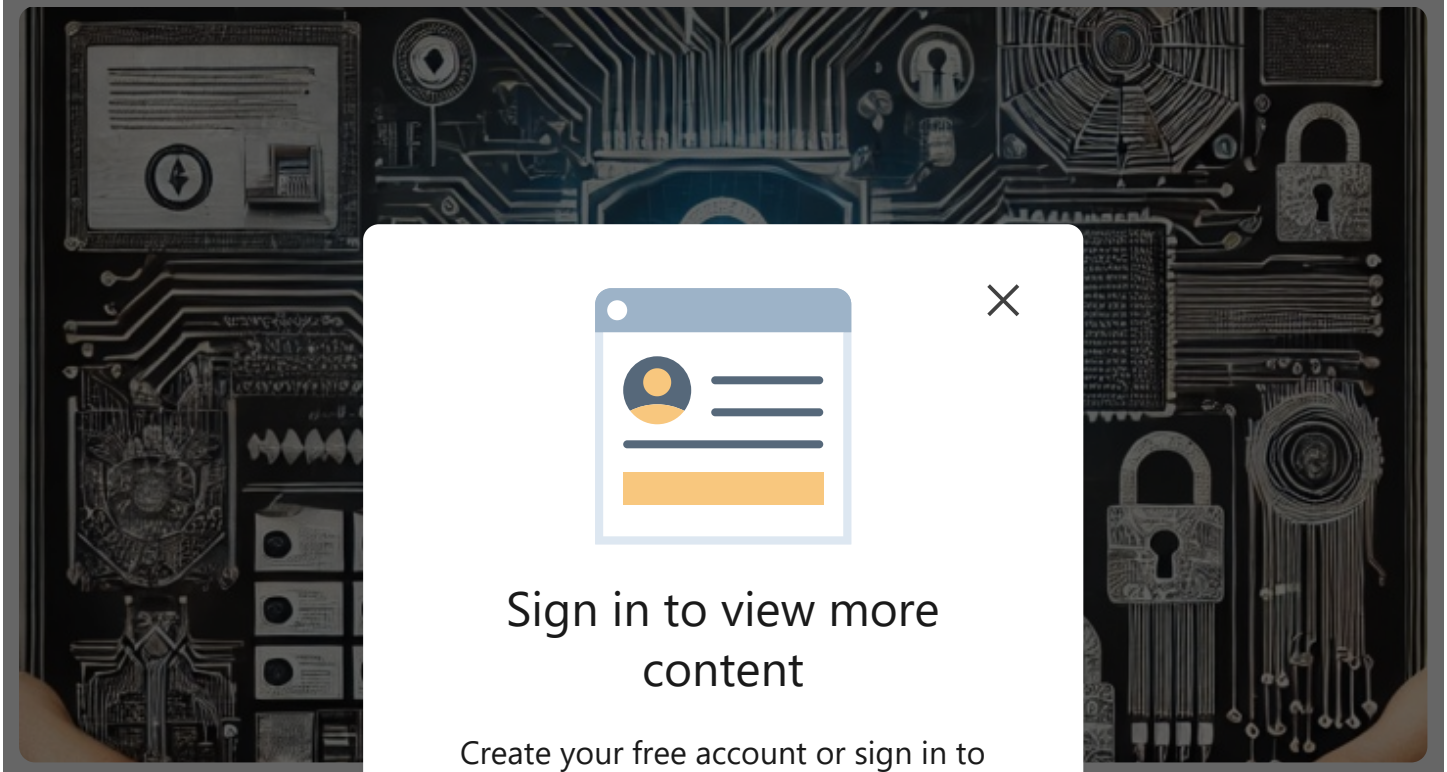
8. - أفضل الممارسات والتحدياتIAM Best Practices and Challenges

المقالات

For Module 1 : https://lnkd.in/dkkyFGdW
For Module 2 : https://lnkd.in/dNUWhiJs
For Module 3: https://lnkd.in/dsqBXhEc
For Module 4: https://lnkd.in/d_DBAm4h
For Module 5: https://lnkd.in/dGPDeKWF
For Module 6: https://lnkd.in/dZHHJKJx
For Module 7: https://lnkd.in/d_JswW5W
For Module 8: https://lnkd.in/dQsQHqgR

Resources - المصادر

1- Official (ISC)² CISSP Study Guide
2- CISSP (ISC)² Official Practice Tests
3- CISSP All-in-One Exam Guide by Shon Harris
4- Cybrary – CISSP Training by Kelly Handerhan https://lnkd.in/d4zrAkJz
5- Oreilly – CISSP Training by Sari Greene https://lnkd.in/dANS-hVc.
6- CISSP bundles by Thor Pedersen https://lnkd.in/d2tpqaJk
7- CISSP MindMaps YouTube Playlist from Destination Certification https://lnkd.in/deJM44xX



CISSP Mod ... s Manageme ...إدارة

Emad M. Ab
Technical Lead
CCIE#58413 | ™ |
ISO27001 LA |
Published Jul 8

Introduction

This module covers the essential principles of Identity and Access Management (IAM), including identification, authentication, authorization, and accountability.

يغطي هذا المقرر المبادئ الأساسية لإدارة الهوية والوصول بما في ذلك التعريف والمصادقة والتفويض والمساءلة

various technologies and protocols used in IAM, and exploring best practices for managing user identities and access controls.

ويركز على تصميم وتنفيذ أطر وفهم التقنيات والبروتوكولات المختلفة المستخدمة فيه, واستكشاف أفضل الممارسات لإدارة هويات المستخدمين وضوابط الوصول

The goal is to provide a comprehensive understanding of how to protect systems and data by effectively managing who can access what resources and under what conditions.

الهدف هو توفير فهم شامل لكيفية حماية الأنظمة والبيانات من خلال إدارة من يمكنه الوصول إلى الموارد وفي ظل أي ظروف بشكل فعال

Module Brief

1. Control Physical and Logical Access to Assets

This section covers controlling access to information, systems, devices, facilities, applications, and services.

يتناول هذا القسم التحكم في الوصول إلى المعلومات والأنظمة والأجهزة والمرافق والتطبيقات والخدمات

2. Design Identification and Authentication Strategy

This section focuses on designing strategies for groups and roles, multi-factor authentication (MFA), session management, federated identity management, and more.

يركز هذا القسم على تصميم استراتيجيات للمجموعات والأدوار، والمصادقة متعددة العوامل، وإدارة الجلسات، وإدارة الهوية الفيدرالية، والمزيد

3. Federated Identity with a Third-Party Service

This section explores federated identity management with on-premise, cloud, and hybrid environments.

يستكشف هذا القسم إدارة الهوية الفيدرالية مع البيئات المحلية والسحابية والهجينة

4. Implement and Manage Authorization Mechanisms

This section covers various access control models and techniques such as RBAC, MAC, DAC, ABAC, and risk-based access control.

يغطي هذا القسم نماذج وتقنيات التحكم في الوصول المختلفة ، والتحكم في الوصول المستند إلى المخاطر

5. Manage the Identity and Access Provisioning Lifecycle

This section outlines the lifecycle management of identities and access, including account access review, provisioning, deprovisioning, and privilege escalation.

يوضح هذا القسم إدارة دورة حياة الهويات والوصول، بما في ذلك مراجعة الوصول إلى الحساب، والتوفير، وإلغاء التوفير، وتصعيد الامتيازات

6. Implement Authentication Systems

This section details the implementation of various authentication systems.

يوضح هذا القسم تنفيذ أنظمة المصادقة المختلفة

7. Identity and Access Management Technologies

This section explores various IAM technologies and their applications.

يستكشف هذا القسم تقنيات إدارة الهوية والوصول المختلفة وتطبيقاتها

8. IAM Best Practices and Challenges

This section provides best practices for implementing IAM and addresses common challenges with mitigation controls.

يقدم هذا القسم أفضل الممارسات لتنفيذ إدارة الهوية والوصول ويتناول التحديات الشائعة مع ضوابط التخفيف

---

1. Control Physical and Logical Access to Assets

1.1 Access Control Methods

Definition: Methods used to control access to information, systems, devices, facilities, applications, and services to protect against unauthorized use or abuse.

طرق تستخدم للتحكم في الوصول إلى المعلومات والأنظمة والأجهزة والمرافق والتطبيقات والخدمات لحمايتها من الاستخدام أو الإساءة غير المصرح به

List of Access Control Methods:

- Information
- Systems
- Devices
- Facilities
- Applications
- Services

1.1.1 Information

Definition: Controlling access to information resources to protect confidentiality, integrity, and availability.

التحكم في الوصول إلى موارد المعلومات لحماية السرية والسلامة والتوافر

Examples:

- **Data Classification:** Classifying data to determine appropriate security measures. تصنيف البيانات لتحديد التدابير الأمنية المناسبة

- **Access Controls:** Implementing access controls based on data classification. تنفيذ ضوابط الوصول بناءً على تصنيف البيانات

Use Case: An organization classifies its data and implements access controls to ensure that sensitive information is only accessible to authorized personnel. تقوم منظمة بتصنيف بياناتها وتنفيذ ضوابط الوصول لضمان أن المعلومات الحساسة متاحة فقط للأفراد المصرح لهم

1.1.2 Systems

Definition: Controlling access to system resources to prevent unauthorized use or abuse.

التحكم في الوصول إلى موارد النظام لمنع الاستخدام أو الإساءة غير المصرح به

Examples:

- **System Access Controls:** Using authentication and authorization mechanisms to control access to systems. استخدام آليات المصادقة والتفويض للتحكم في الوصول إلى الأنظمة

- **Monitoring:** Monitoring system access to detect and respond to unauthorized access attempts. مراقبة الوصول إلى النظام لاكتشاف والاستجابة لمحاولات الوصول غير المصرح به

Use Case: A company uses system access controls and monitoring to prevent and detect unauthorized access to its servers. تستخدم شركة ضوابط الوصول إلى النظام والمراقبة لمنع واكتشاف الوصول غير المصرح به إلى خوادمها

1.1.3 Devices

Definition: Securing devices to ensure that only authorized individuals can access and use them.

تأمين الأجهزة لضمان أن الأفراد المصرح لهم فقط يمكنهم الوصول إليها واستخدامها

Examples:

- **Device Authentication:** Using authentication mechanisms to verify the identity of device

users. استخدام آليات المصادقة للتحقق من هوية مستخدمي الأجهزة

- **Device Encryption:** Encrypting data on devices to protect against unauthorized access. تشفير البيانات على الأجهزة لحمايتها من الوصول غير المصرح به

Use Case: A healthcare organization uses device authentication and encryption to protect patient data on mobile devices. تستخدم منظمة الرعاية الصحية المصادقة على الأجهزة والتشفير لحماية بيانات المرضى على الأجهزة المحمولة

1.1.4 Facilities

Definition: Implementing physical security controls to protect facilities and the assets within them.

تنفيذ ضوابط الأمن الفيزيائي لحماية المرافق والأصول الموجودة بها

Examples:

- **Access Controls:** Using card readers and biometric systems to control access to facilities. استخدام قارئات البطاقات وأنظمة القياسات الحيوية للتحكم في الوصول إلى المرافق

- **Surveillance:** Using video surveillance to monitor facility access points. استخدام المراقبة بالفيديو لمراقبة نقاط الوصول إلى المرافق

Use Case: A financial institution uses access controls and surveillance to secure its data centers. تستخدم مؤسسة مالية ضوابط الوصول والمراقبة لتأمين مراكز البيانات الخاصة بها

1.1.5 Applications

Definition: Controlling access to applications to ensure that only authorized users can access and use them.

التحكم في الوصول إلى التطبيقات لضمان أن المستخدمين المصرح لهم فقط يمكنهم الوصول إليها واستخدامها

Examples:

- **Application Security Controls:** Implementing authentication and authorization mechanisms within applications. تنفيذ آليات المصادقة والتفويض داخل التطبيقات

- **Logging and Monitoring:** Logging application access and monitoring for suspicious activity. تسجيل الوصول إلى التطبيقات ومراقبة النشاط المشبوه

Use Case: A software company implements application security controls and monitoring to protect its proprietary software from unauthorized access and use. تقوم شركة برمجيات بتنفيذ ضوابط الأمان للتطبيقات والمراقبة لحماية برامجها الملكية من الوصول والاستخدام غير المصرح به

1.1.6 Services

Definition: Securing access to services to protect against unauthorized use and abuse.

تأمين الوصول إلى الخدمات لحمايتها من الاستخدام والإساءة غير المصرح به

Examples:

- **Service Authentication:** Implementing authentication mechanisms to verify the identity of service users. تنفيذ آليات المصادقة للتحقق من هوية مستخدمي الخدمة
- **Service Authorization:** Implementing authorization mechanisms to control access to services. تنفيذ آليات التفويض للتحكم في الوصول إلى الخدمات

Use Case: A cloud service provider uses service authentication and authorization to ensure that only authorized users can access its services. يستخدم مزود خدمة السحابة المصادقة على الخدمة والتفويض لضمان أن المستخدمين المصرح لهم فقط يمكنهم الوصول إلى خدماته

1.2 Access Control Principles

Definition: Principles that guide the implementation of access controls to ensure they are effective and secure.

المبادئ التي توجه تنفيذ ضوابط الوصول لضمان فعاليتها وأمانها

List of Access Control Principles:

- Separation of Duties

- Need to Know
- Least Privilege

1.2.1 Separation of Duties

Definition: Ensuring that no single individual has complete control over all aspects of a critical process, reducing the risk of fraud or error.

يضمن مبدأ فصل الواجبات أن لا يتمتع فرد واحد بالسيطرة الكاملة على جميع جوانب عملية حاسمة، مما يقلل من مخاطر الاحتيال أو الخطأ

Examples:

- **Financial Transactions:** Separating the duties of initiating, approving, and recording financial transactions. فصل واجبات بدء المعاملات المالية والموافقة عليها وتسجيلها
- **IT Operations:** Separating the roles of system administrators and security administrators. فصل أدوار مسؤولي النظام ومسؤولي الأمان

Use Case: A company separates the roles of requesting and approving purchases to reduce the risk of fraudulent transactions. تفصل شركة بين أدوار طلب والموافقة على المشتريات لتقليل مخاطر المعاملات الاحتيالية

1.2.2 Need to Know

Definition: Restricting access to information only to those who require it to perform their job duties.

يقيد مبدأ الحاجة إلى المعرفة الوصول إلى المعلومات فقط لأولئك الذين يحتاجون إليها لأداء مهام عملهم

Examples:

- **Data Access:** Limiting access to sensitive data to employees who need it for their work. تقييد الوصول إلى البيانات الحساسة للموظفين الذين يحتاجون إليها لعملهم
- **Project Information:** Granting access to project details only to team members working on the project. منح الوصول إلى تفاصيل المشروع فقط لأعضاء الفريق العاملين في المشروع

Use Case: An organization restricts access to customer data to customer service representatives who need it to assist customers. تقييد منظمة الوصول إلى بيانات العملاء لممثلي خدمة العملاء الذين يحتاجون إليها لمساعدة العملاء

1.2.3 Least Privilege

Definition: Providing users with the minimum level of access necessary to perform their job functions.

يمنح مبدأ أقل الامتيازات المستخدمين الحد الأدنى من الوصول اللازم لأداء وظائفهم

Examples:

- **Access Rights:** Granting employees only the access rights they need to perform their duties. منح الموظفين فقط حقوق الوصول التي يحتاجونها لأداء واجباتهم
- **System Permissions:** Limiting administrative privileges to IT staff who require them for system maintenance. تقييد الامتيازات الإدارية لموظفي تكنولوجيا المعلومات الذين يحتاجون إليها لصيانة النظام

Use Case: A company implements least privilege by restricting administrative access to systems to only a few IT administrators. تقوم شركة بتنفيذ مبدأ أقل الامتيازات من خلال تقييد الوصول الإداري إلى الأنظمة لعدد قليل من مسؤولي تكنولوجيا المعلومات

1.3 Administration Approaches

Definition: Methods of organizing and managing access controls within an organization.

طرق تنظيم وإدارة ضوابط الوصول داخل المنظمة

List of Administration Approaches:

- Centralized
- Decentralized
- Hybrid

1.3.1 Centralized

Definition: Consolidating access control management in a single location or system.

تجمع الإدارة المركزية إدارة التحكم في الوصول في موقع أو نظام واحد

Examples:

- **Centralized Directory:** Using a centralized directory service like Active Directory to manage user accounts and permissions. استخدام خدمة دليل مركزي لإدارة حسابات المستخدمين والأذونات
- **Unified Access Management:** Implementing a unified access management system to control access to all resources. تنفيذ نظام إدارة وصول موحد للتحكم في الوصول إلى جميع الموارد

Use Case: An organization uses a centralized directory service to manage user accounts and access permissions across its entire network. تستخدم منظمة خدمة دليل مركزي لإدارة حسابات المستخدمين وأذونات الوصول عبر شبكتها بالكامل

1.3.2 Decentralized

Definition: Distributing access control management across multiple locations or systems.

توزع الإدارة اللامركزية إدارة التحكم في الوصول عبر مواقع أو أنظمة متعددة

Examples:

- **Local Administration:** Allowing local administrators to manage access controls for their specific departments. السماح للمسؤولين المحليين بإدارة ضوابط الوصول لأقسامهم المحددة
- **Departmental Control:** Granting departments the autonomy to manage their own access permissions. منح الأقسام الاستقلالية لإدارة أذونات الوصول الخاصة بهم

Use Case: A multinational corporation allows each regional office to manage its own user accounts and access permissions. تسمح شركة متعددة الجنسيات لكل مكتب إقليمي بإدارة حسابات المستخدمين وأذونات الوصول الخاصة به

1.3.3 Hybrid

Definition: Combining elements of both centralized and decentralized approaches.

تجمع الإدارة الهجينة بين عناصر النهجين المركزي واللامركزي

Examples:

- **Centralized Policies, Local Control:** Implementing centralized access control policies with local control over specific permissions. تنفيذ سياسات التحكم في الوصول المركزية مع السيطرة المحلية على الأذونات المحددة
- **Federated Access Management:** Using a federated model to manage access controls across different regions or departments. استخدام نموذج اتحادي لإدارة ضوابط الوصول عبر المناطق أو الأقسام المختلفة

Use Case: An enterprise adopts a hybrid approach by setting global access policies while allowing local IT teams to manage day-to-day access permissions. تتبنى مؤسسة نهجًا هجينًا من خلال وضع سياسات وصول عالمية بينما تسمح لفرق تكنولوجيا المعلومات المحلية بإدارة أذونات الوصول اليومية

Multiple Choice Questions

1. What is the primary purpose of the separation of duties principle?

a. To increase data availability

b. To reduce the risk of fraud or error

c. To improve data encryption

d. To monitor data access

2. Which access control principle restricts access to information only to those who require it for their job duties?

a. Least Privilege

b. Need to Know

c. Separation of Duties

d. Centralized Administration

3. What is the key feature of least privilege?

a. Providing maximum access at all times

b. Providing minimum access necessary to perform job functions

c. Using multi-factor authentication

d. Implementing single sign-on

4. What is the benefit of centralized administration?

a. Distributing access control management

b. Consolidating access control management in a single location or system

c. Granting departments the autonomy to manage their own access permissions

d. Combining elements of both centralized and decentralized approaches

5. How does a hybrid administration approach manage access control?

a. By centralizing all access control management

b. By decentralizing all access control management

c. By combining centralized policies with local control over specific permissions

d. By using a single access management system for all resources

---

Answers and Explanations

1. b. To reduce the risk of fraud or error

Separation of duties ensures that no single individual has complete control over all aspects of a critical process, reducing the risk of fraud or error.

يضمن مبدأ فصل الواجبات أن لا يتمتع فرد واحد بالسيطرة الكاملة على جميع جوانب عملية حاسمة، مما يقلل من مخاطر الاحتيال أو الخطأ

2. b. Need to Know

Need to Know restricts access to information only to those who require it to perform their job duties.

يقيد مبدأ الحاجة إلى المعرفة الوصول إلى المعلومات فقط لأولئك الذين يحتاجون إليها لأداء مهام عملهم

3. b. Providing minimum access necessary to perform job functions

Least privilege provides users with the minimum level of access necessary to perform their job functions.

يمنح مبدأ أقل الامتيازات المستخدمين الحد الأدنى من الوصول اللازم لأداء وظائفهم

4. b. Consolidating access control management in a single location or system

Centralized administration consolidates access control management in a single location or system.

تجمع الإدارة المركزية إدارة التحكم في الوصول في موقع أو نظام واحد

5. c. By combining centralized policies with local control over specific permissions

A hybrid administration approach combines centralized policies with local control over specific permissions.

تجمع الإدارة الهجينة بين سياسات الوصول المركزية والسيطرة المحلية على الأذونات المحددة

---

2. Design Identification and Authentication Strategy

2.1 Groups and Roles

Definition: Using groups and roles to simplify the management of access controls.

استخدام المجموعات والأدوار لتبسيط إدارة ضوابط الوصول

Examples:

- **Group Policies:** Applying policies to groups of users to manage access rights. تطبيق السياسات على مجموعات المستخدمين لإدارة حقوق الوصول
- **Role-Based Access Control (RBAC):** Assigning access rights based on user roles. تعيين حقوق الوصول بناءً على أدوار المستخدمين

Use Case: An organization uses RBAC to assign access rights to employees based on their job functions. تستخدم منظمة لتعيين حقوق الوصول للموظفين بناءً على وظائفهم.

2.2 Identification, Authentication, Authorization and Accounting (AAA)

Definition: A framework for intelligently controlling access to computer resources, enforcing policies, and auditing usage.

إطار عمل للتحكم الذكي في الوصول إلى موارد الكمبيوتر، وفرض السياسات، وتدقيق الاستخدام

2.2.1 Identification

Definition: The process of recognizing an individual as a valid user.

عملية التعرف على الفرد كمستخدم صالح

Examples:

- **User IDs:** Assigning unique user IDs to individuals. تعيين معرفات مستخدم فريدة للأفراد

- **Biometric Identifiers:** Using biometric data such as fingerprints or facial recognition. استخدام البيانات البيومترية مثل بصمات الأصابع أو التعرف على الوجه

- **Email Addresses:** Using email addresses as unique identifiers. استخدام عناوين البريد الإلكتروني كمعرفات فريدة

- **Phone Numbers:** Using phone numbers for identity verification. استخدام أرقام الهاتف للتحقق من الهوية

- **Use Case:** A company uses biometric identifiers, email addresses, and phone numbers to recognize employees and grant them access to secure areas. تستخدم شركة معرفات بيومترية، وعناوين البريد الإلكتروني، وأرقام الهاتف للتعرف على الموظفين ومنحهم الوصول إلى المناطق الآمنة

2.2.2 Authentication

Definition: Verifying the identity of a user through various methods.

التحقق من هوية المستخدم من خلال طرق مختلفة

List of Authentication Approaches:

- Knowledge (Something the user knows)
- Ownership (Something the user has)
- Characteristic (Something the user is)
- Single/Multifactor (Using one or more methods of authentication)
- Authenticator Assurance Levels
- Levels of confidence in the authentication process
- Just-in-time Access

2.2.2.1 Knowledge

Definition: Something the user knows.

شيء يعرفه المستخدم

Examples:

- **Password:** A secret word or phrase used to authenticate a user. كلمة سر: كلمة أو عبارة سرية تستخدم لمصادقة المستخدم
- **Passphrase:** A longer phrase used to authenticate a user. عبارة مرور: عبارة أطول تستخدم لمصادقة المستخدم
- **Questions:** Security questions used to verify identity. أسئلة: أسئلة أمان تستخدم للتحقق من الهوية
- **Use Case:** An organization requires users to enter a password and answer a security question to access sensitive data. تطلب منظمة من المستخدمين إدخال كلمة مرور والإجابة على سؤال أمان للوصول إلى البيانات الحساسة

2.2.2.2 Ownership

Definition: Something the user has.

شيء يمتلكه المستخدم

Examples:

- **One-time Passwords:** Passwords that are valid for only one login session. كلمات مرور لمرة واحدة: كلمات مرور صالحة لجلسة تسجيل دخول واحدة فقط **Hard Tokens:** Physical devices that generate one-time passwords. رموز صلبة: أجهزة مادية تولد كلمات مرور لمرة واحدة **Soft Tokens:** Software applications that generate one-time passwords. رموز ناعمة: تطبيقات برمجية تولد كلمات مرور لمرة واحدة **Synchronous:** Tokens synchronized with a server to generate one-time passwords. متزامنة: رموز متزامنة مع خادم لتوليد كلمات مرور لمرة واحدة **Asynchronous:** Tokens that generate one-time passwords independently. غير متزامنة: رموز تولد كلمات مرور لمرة واحدة بشكل مستقل
- **Smart/Memory Cards:** Cards that store authentication data. بطاقات ذكية / ذاكرة: بطاقات تخزن بيانات المصادقة

- **Use Case:** A financial institution uses smart cards to authenticate employees accessing secure systems. تستخدم مؤسسة مالية بطاقات ذكية لمصادقة الموظفين الذين يصلون إلى الأنظمة الآمنة

2.2.2.3 Characteristic

Definition: Something the user is.

شيء يكونه المستخدم

Examples:

- **Physiological:** Using physical characteristics to verify identity. فسيولوجية: استخدام الخصائص الفيزيائية للتحقق من الهوية **Fingerprint:** Using fingerprint recognition for authentication. بصمة: استخدام التعرف على بصمات الأصابع للمصادقة **Hand Geometry:** Using the shape of the hand for authentication. هندسة اليد: استخدام شكل اليد للمصادقة **Vascular Pattern:** Using the pattern of veins for authentication. نمط الأوعية الدموية: استخدام نمط الأوردة للمصادقة **Facial:** Using facial recognition for authentication. الوجه: استخدام التعرف على الوجه للمصادقة **Retina:** Using retinal scans for authentication. شبكية العين: استخدام مسح الشبكية للمصادقة **Iris:** Using iris scans for authentication. قزحية: استخدام مسح القزحية للمصادقة

- **Behavioral:** Using behavior patterns to verify identity. سلوكية: استخدام أنماط السلوك للتحقق من الهوية **Voice:** Using voice recognition for authentication. الصوت: استخدام التعرف على الصوت للمصادقة **Signature:** Using signature analysis for authentication. التوقيع: استخدام تحليل التوقيع للمصادقة **Keystroke:** Using typing patterns for authentication. ضربات المفاتيح: استخدام أنماط الكتابة للمصادقة **Gait:** Using walking patterns for authentication. مشية: استخدام أنماط المشي للمصادقة

- **Templates:** Stored data used to compare against captured biometric data. القوالب: بيانات مخزنة تستخدم للمقارنة مع البيانات البيومترية الملتقطة

- **Type 1: False Reject:** Incorrectly rejecting an authorized user. النوع 1: رفض كاذب: رفض غير صحيح لمستخدم مخول

- **Type 2: False Accept:** Incorrectly accepting an unauthorized user. النوع 2: قبول كاذب: قبول غير صحيح لمستخدم غير مخول

- **Crossover Error Rate:** The rate at which false accept and false reject rates are equal. معدل الخطأ المتقاطع: المعدل الذي تتساوى فيه معدلات القبول الكاذب والرفض الكاذب

- **Use Case:** An airport uses iris scans to authenticate passengers at security checkpoints. يستخدم مطار مسح القزحية لمصادقة الركاب عند نقاط التفتيش الأمنية

2.2.2.4 Single/Multifactor

Definition: Using one or more methods of authentication.

استخدام طريقة واحدة أو أكثر للمصادقة

Examples:

- **Single-Factor Authentication:** Using one method, such as a password. مصادقة العامل الواحد: استخدام طريقة واحدة، مثل كلمة المرور

- **Multi-Factor Authentication (MFA):** Using multiple methods, such as a password and a fingerprint. المصادقة متعددة العوامل: استخدام طرق متعددة، مثل كلمة المرور وبصمة الإصبع

- **Use Case:** A company uses MFA to secure remote access by requiring both a password and a fingerprint. تستخدم شركة المصادقة متعددة العوامل لتأمين الوصول عن بعد من خلال طلب كلمة مرور وبصمة إصبع

2.2.2.5 Authenticator Assurance Levels (AAL)

Definition: Levels of confidence in the authentication process.

مستويات الثقة في عملية المصادقة

Examples:

- **AAL1:** Low confidence, single-factor authentication. مستوى الثقة 1: ثقة منخفضة، مصادقة العامل الواحد

- **AAL2:** Moderate confidence, two-factor authentication. مستوى الثقة 2: ثقة متوسطة،

مصادقة العاملين

- **AAL3:** High confidence, multi-factor authentication with strong cryptographic mechanisms. مستوى الثقة 3: ثقة عالية، مصادقة متعددة العوامل مع آليات تشفير قوية

- **Use Case:** A government agency uses AAL3 to secure access to classified information. تستخدم وكالة حكومية مستوى الثقة 3 لتأمين الوصول إلى المعلومات المصنفة

2.2.2.6 Just-in-time Access

Definition: Providing users with the minimum level of access they need, only when they need it.

تزويد المستخدمين بالحد الأدنى من الوصول الذي يحتاجونه فقط عندما يحتاجونه

- **Use Case:** A company implements just-in-time access to ensure employees only have access to sensitive data when it is required for their tasks. تقوم شركة بتنفيذ الوصول في الوقت المناسب لضمان أن الموظفين لديهم وصول إلى البيانات الحساسة فقط عندما يكون ذلك مطلوبًا لمهامهم

2.2.3 Authorization

Definition: Determining what an authenticated user is allowed to do.

تحديد ما يُسمح للمستخدم المصادق عليه بالقيام به

2.2.3.1 Discretionary

Definition: Access control based on the discretion of the resource owner.

التحكم في الوصول بناءً على تقدير مالك المورد

Examples:

- **Rule-Based:** Access control based on predefined rules. المستند إلى القواعد: التحكم في الوصول بناءً على قواعد محددة مسبقًا

- **Role-Based:** Access control based on user roles. المستند إلى الدور: التحكم في الوصول بناءً على أدوار المستخدمين

- **Attribute/Content-Based:** Access control based on user attributes or content of the resource. المستند إلى السمة / المحتوى: التحكم في الوصول بناءً على سمات المستخدم أو محتوى المورد

- **Use Case:** A department manager grants access to project files based on the roles and responsibilities of team members. يمنح مدير القسم الوصول إلى ملفات المشروع بناءً على أدوار ومسؤوليات أعضاء الفريق

2.2.3.2 Non-discretionary

Definition: Access control based on predefined policies that cannot be altered by resource owners.

التحكم في الوصول بناءً على سياسات محددة مسبقًا لا يمكن تغييرها بواسطة مالكي الموارد

Examples:

- **Mandatory Access Control (MAC):** Access control enforced by a central authority based on security labels. التحكم الإجباري في الوصول: التحكم في الوصول المفروض من قبل سلطة مركزية بناءً على تصنيفات الأمان

Use Case: A government agency uses MAC to enforce strict access controls based on security classifications. تستخدم وكالة حكومية MAC لفرض ضوابط وصول صارمة بناءً على التصنيفات الأمنية

2.2.4 Accountability

Definition: Ensuring that user actions can be traced back to the individual.

ضمان أن تكون أفعال المستخدم قابلة للتتبع إلى الفرد

Examples:

- **Audit Logs:** Recording user activities to trace actions back to individuals. سجلات التدقيق: تسجيل أنشطة المستخدم لتتبع الأفعال إلى الأفراد

- **Monitoring:** Continuously monitoring user actions for compliance and security. المراقبة: مراقبة أفعال المستخدم باستمرار للامتثال والأمان

Use Case: An organization maintains audit logs to trace any unauthorized access attempts back to specific users. تحافظ منظمة على سجلات التدقيق لتتبع أي محاولات وصول غير مصرح بها إلى مستخدمين محددين

2.3 Session Management

Definition: Managing user sessions to ensure secure access and usage of resources.

إدارة جلسات المستخدمين لضمان الوصول الآمن واستخدام الموارد

Examples:

- **Session Timeouts:** Automatically ending user sessions after a period of inactivity. إنهاء جلسات المستخدمين تلقائيًا بعد فترة من عدم النشاط
- **Session Monitoring:** Monitoring active sessions for suspicious activity. مراقبة الجلسات النشطة للنشاط المشبوه
- **Single Sign-On (SSO):** Providing users with one login session to access multiple resources. تسجيل الدخول الأحادي: توفير جلسة تسجيل دخول واحدة للمستخدمين للوصول إلى موارد متعددة
- **Session Encryption:** Encrypting session data to protect it from eavesdropping. تشفير الجلسة: تشفير بيانات الجلسة لحمايتها من التنصت

Use Case: An organization implements session timeouts, monitoring, and encryption to reduce the risk of unauthorized access to inactive sessions. تقوم منظمة بتنفيذ انتهاء الجلسات، والمراقبة، والتشفير لتقليل مخاطر الوصول غير المصرح به إلى الجلسات غير النشطة

2.4 Registration, Proofing, and Establishment of Identity

Definition: Processes for verifying and establishing user identities.

عمليات التحقق من هويات المستخدمين وإثباتها

Examples:

- **Identity Proofing:** Verifying the identity of a user before granting access. التحقق من هوية المستخدم قبل منح الوصول
- **Credential Issuance:** Issuing credentials to verified users. إصدار بيانات الاعتماد للمستخدمين الذين تم التحقق منهم
- **Background Checks:** Conducting background checks to verify identity information. إجراء فحوصات الخلفية للتحقق من معلومات الهوية
- **Document Verification:** Verifying identity documents provided by the user. التحقق من الوثائق: التحقق من وثائق الهوية التي يقدمها المستخدم

Use Case: A university uses identity proofing, background checks, and document verification to verify the identities of students before issuing them campus access cards. تستخدم جامعة التحقق من الهوية، وفحوصات الخلفية، والتحقق من الوثائق للتحقق من هويات الطلاب قبل إصدار بطاقات الوصول إلى الحرم الجامعي لهم

2.5 Federated Identity Management (FIM)

Definition: An arrangement that allows users to use the same identification data to obtain access to the networks of all enterprises in the group.

ترتيب يسمح للمستخدمين باستخدام نفس بيانات التعريف للحصول على الوصول إلى شبكات جميع المؤسسات في المجموعة

2.5.1 Trust Relationship

Definition: The relationship between different entities involved in federated identity management.

العلاقة بين الكيانات المختلفة المشاركة في إدارة الهوية الفيدرالية

Examples:

- **Principal/User:** The entity that needs to be authenticated. المستخدم: الكيان الذي يحتاج إلى المصادقة
- **Identity Provider:** The entity that provides the identity information. مزود الهوية: الكيان الذي يقدم معلومات الهوية

- **Relying Party/Service Provider:** The entity that relies on the identity information to provide services. مزود الخدمة: الكيان الذي يعتمد على معلومات الهوية لتقديم الخدمات.

Use Case: A company uses federated identity management to allow employees to access external services using their corporate credentials. تستخدم شركة إدارة الهوية الفيدرالية للسماح للموظفين بالوصول إلى الخدمات الخارجية باستخدام بيانات اعتماد الشركة الخاصة بهم

2.5.2 SAML

Definition: An open standard for exchanging authentication and authorization data between parties.

معيار مفتوح لتبادل بيانات المصادقة والتفويض بين الأطراف

Examples:

- **Tokens:** Digital representations of user credentials. رموز: تمثيلات رقمية لبيانات اعتماد المستخدم

- **Assertions written in XML:** Statements that provide information about the user. تأكيدات مكتوبة بلغة XML: بيانات تقدم معلومات عن المستخدم

- **Single Sign-On (SSO):** Using SAML for single sign-on across multiple applications. تسجيل الدخول الأحادي: استخدام SAML لتسجيل الدخول الأحادي عبر تطبيقات متعددة

Use Case: An enterprise uses SAML to enable single sign-on for its employees across various web applications. تستخدم مؤسسة SAML لتمكين تسجيل الدخول الأحادي لموظفيها عبر تطبيقات الويب المختلفة

2.5.3 Components

Definition: The elements that make up the SAML framework.

العناصر التي تشكل إطار عمل SAML

Examples:

- **Profiles:** Define the use cases for SAML. ملفات تعريف: تحدد حالات الاستخدام لـ SAML

- **Bindings:** Define how SAML messages are transported. روابط SAML: تحدد كيفية نقل رسائل
- **Protocol:** Defines the communication between entities. بروتوكول: يحدد التواصل بين الكيانات
- **Assertion:** The statement that provides information about the user. تأكيد: البيان الذي يقدم معلومات عن المستخدم

Use Case: An organization uses SAML profiles and bindings to ensure secure communication between its identity provider and service providers. تستخدم منظمة ملفات تعريف SAML والروابط لضمان التواصل الآمن بين مزود الهوية ومقدمي الخدمات

2.5.4 WS-Federation

Definition: A standard for federated identity management that extends the capabilities of SAML.

معيار لإدارة الهوية الفيدرالية الذي يوسع قدرات SAML

Examples:

- **Web Services Security:** Providing secure communication between web services. أمان خدمات الويب: توفير التواصل الآمن بين خدمات الويب
- **Token Translation:** Converting tokens between different formats for interoperability. ترجمة الرموز: تحويل الرموز بين تنسيقات مختلفة للتشغيل البيني

Use Case: A company uses WS-Federation to enable secure communication between its internal web services and external partners. تستخدم شركة WS-Federation لتمكين التواصل الآمن بين خدمات الويب الداخلية والشركاء الخارجيين

2.5.5 OpenID

Definition: An open standard for decentralized authentication.

معيار مفتوح للمصادقة اللامركزية

Examples:

- **OpenID Connect:** An authentication layer built on top of OAuth 2.0. OpenID Connect: طبقة مصادقة مبنية على OAuth 2.0

- **OAuth 2.0 Integration:** Using OpenID for authentication and OAuth 2.0 for authorization. تكامل OAuth 2.0: استخدام OpenID للمصادقة و OAuth 2.0 للتفويض

Use Case: A user logs into multiple websites using their OpenID account, simplifying the authentication process. يقوم المستخدم بتسجيل الدخول إلى مواقع ويب متعددة باستخدام حساب OpenID الخاص به، مما يبسط عملية المصادقة

2.5.6 OAuth

Definition: An open standard for access delegation.

معيار مفتوح لتفويض الوصول

Examples:

- **Authorization Tokens:** Tokens used to grant access to resources without sharing user credentials. رموز التفويض: رموز تُستخدم لمنح الوصول إلى الموارد دون مشاركة بيانات اعتماد المستخدم

- **Scopes:** Defining the level of access granted by an authorization token. النطاقات: تحديد مستوى الوصول الممنوح بواسطة رمز التفويض

- **Authorization Grants:** Different methods for obtaining authorization tokens (e.g., authorization code, client credentials). منح التفويض: طرق مختلفة للحصول على رموز التفويض (مثل رمز التفويض، بيانات اعتماد العميل)

Use Case: A mobile app uses OAuth to access user data from social media platforms without requiring the user's password. يستخدم تطبيق الجوال OAuth للوصول إلى بيانات المستخدم من منصات التواصل الاجتماعي دون الحاجة إلى كلمة مرور المستخدم

2.6 Credential Management Systems

Definition: Systems that manage the issuance, storage, and use of credentials.

أنظمة تدير إصدار وتخزين واستخدام بيانات الاعتماد

Examples:

- **Password Vaults:** Securely storing and managing passwords. تخزين وإدارة كلمات المرور

بأمان

- **Public Key Infrastructure (PKI):** Managing digital certificates and public keys. إدارة الشهادات الرقمية والمفاتيح العامة
- **Smart Card Management:** Managing the issuance and use of smart cards. إدارة البطاقات الذكية: إدارة إصدار واستخدام البطاقات الذكية
- **Credential Rotation:** Regularly updating credentials to enhance security. تدوير بيانات الاعتماد: تحديث بيانات الاعتماد بانتظام لتعزيز الأمان

Use Case: An organization uses a password vault, PKI, and smart card management to securely store and manage employee credentials. تستخدم منظمة مخزن كلمات المرور، وبنية المفاتيح العامة، وإدارة البطاقات الذكية لتخزين وإدارة بيانات اعتماد الموظفين بأمان

2.7 Single Sign-On (SSO)

Definition: A user authentication process that allows a user to access multiple applications with one set of login credentials.

عملية مصادقة المستخدم التي تسمح للمستخدم بالوصول إلى تطبيقات متعددة باستخدام مجموعة واحدة من بيانات تسجيل الدخول

2.7.1 Kerberos

Definition: A network authentication protocol designed to provide strong authentication for client-server applications.

بروتوكول مصادقة شبكة مصمم لتوفير مصادقة قوية لتطبيقات العميل-الخادم

Components:

- **User/Client:** The entity requesting access. المستخدم: الكيان الذي يطلب الوصول
- **Key Distribution Center (KDC):** The central authority that manages keys. مركز توزيع المفاتيح: السلطة المركزية التي تدير المفاتيح
- **Authentication Service (AS):** Verifies the identity of the user. خدمة المصادقة: تتحقق من هوية المستخدم

- **Ticket Granting Ticket (TGT):** A ticket issued by the AS that allows the user to request service tickets. تذكرة منح التذاكر: تذكرة صادرة عن خدمة المصادقة تسمح للمستخدم بطلب تذاكر الخدمة

- **Ticket Granting Service (TGS):** Issues service tickets based on the TGT. خدمة منح التذاكر: تصدر تذاكر الخدمة بناءً على تذكرة منح التذاكر

- **Service Tickets:** Tickets that grant access to specific services. تذاكر الخدمة: تذاكر تمنح الوصول إلى خدمات محددة

- **Service:** The entity providing the requested service. الخدمة: الكيان الذي يقدم الخدمة المطلوبة

Encryption: Uses symmetric encryption for secure communication. التشفير: يستخدم التشفير المتماثل للتواصل الآمن

Use Case: An enterprise uses Kerberos to provide secure authentication for its internal network services. تستخدم مؤسسة Kerberos لتوفير المصادقة الآمنة لخدمات الشبكة الداخلية

2.7.2 Sesame

Definition: A network authentication protocol similar to Kerberos, but with additional support for asymmetric encryption.

بروتوكول مصادقة شبكة مشابه لـ Kerberos، لكنه يدعم التشفير غير المتماثل

Components:

- **Symmetric and Asymmetric Encryption:** Uses both types of encryption for secure communication. التشفير المتماثل وغير المتماثل: يستخدم كلا النوعين من التشفير للتواصل الآمن

Use Case: A company uses Sesame to provide secure authentication for its external partner network. تستخدم شركة Sesame لتوفير المصادقة الآمنة لشبكة الشركاء الخارجية

2.8 Just-In-Time

Definition: Providing users with the minimum level of access they need, only when they need it.

تزويد المستخدمين بالحد الأدنى من الوصول الذي يحتاجونه فقط عندما يحتاجونه

Examples:

- **Temporary Access:** Granting temporary access to users for specific tasks. منح الوصول المؤقت للمستخدمين للمهام المحددة
- **Automated Provisioning:** Automatically provisioning access based on predefined criteria. التوفير الآلي: توفير الوصول تلقائيًا بناءً على معايير محددة مسبقًا
- **Access Review:** Regularly reviewing access permissions to ensure they are still necessary. مراجعة الوصول: مراجعة أذونات الوصول بانتظام لضمان أنها لا تزال ضرورية
- **Dynamic Access Control:** Adjusting access permissions in real-time based on user activity and behavior. التحكم في الوصول الديناميكي: تعديل أذونات الوصول في الوقت الفعلي بناءً على نشاط وسلوك المستخدم

Use Case: A company implements just-in-time access to ensure employees only have access to sensitive data when it is required for their tasks. تقوم شركة بتنفيذ الوصول في الوقت المناسب لضمان أن الموظفين لديهم وصول إلى البيانات الحساسة فقط عندما يكون ذلك مطلوبًا لمهامهم

Multiple Choice Questions

1. What is the primary purpose of federated identity management?

a. Managing identities within a single organization

b. Allowing users to use the same identification data to access multiple networks

c. Using multiple authentication methods

d. Managing access rights based on roles

2. Which standard is used for exchanging authentication and authorization data between parties?

a. OAuth

b. SAML

c. Kerberos

d. LDAP

3. What is an example of biometric identification?

a. Password

b. Smart Card

c. Fingerprint

d. One-time Password

4. What does just-in-time access provide?

a. Maximum access at all times

b. Access only when needed

c. Multi-factor authentication

d. Permanent access to all resources

5. What is the key benefit of single sign-on (SSO)?

a. Improved data encryption

b. Simplified user authentication

c. Enhanced network security

d. Increased data availability

Answers and Explanations

1. b. Allowing users to use the same identification data to access multiple networks

Federated identity management allows users to use the same identification data to access multiple networks.

تسمح إدارة الهوية الفيدرالية للمستخدمين باستخدام نفس بيانات التعريف للوصول إلى شبكات متعددة

2. b. SAML

SAML is a standard for exchanging authentication and authorization data between parties.

هو معيار لتبادل بيانات المصادقة والتفويض بين الأطراف

3. c. Fingerprint

Biometric identification can include methods such as fingerprint recognition.

يمكن أن تتضمن المصادقة البيومترية طرقًا مثل التعرف على بصمات الأصابع

4. b. Access only when needed

Just-in-time access provides users with the minimum level of access they need, only when they need it.

يوفر الوصول في الوقت المناسب للمستخدمين الحد الأدنى من الوصول الذي يحتاجونه فقط عندما يحتاجونه

5. b. Simplified user authentication

Single sign-on (SSO) simplifies user authentication by allowing users to access multiple applications with one set of login credentials.

يبسط تسجيل الدخول الأحادي مصادقة المستخدم من خلال السماح للمستخدمين بالوصول إلى تطبيقات متعددة باستخدام مجموعة واحدة من بيانات تسجيل الدخول

3. Federated Identity with a Third-Party Service

3.1 On-Premise

Definition: Federated identity management within an organization's own infrastructure.

إدارة الهوية الفيدرالية داخل البنية التحتية الخاصة بالمؤسسة

Examples:

- **Internal SSO:** Implementing SSO within the organization’s internal systems. تنفيذ SSO داخل أنظمة المنظمة الداخلية
- **Active Directory Federation Services (ADFS):** Using ADFS to manage federated identities. استخدام خدمات اتحاد الدليل النشط (ADFS) لإدارة الهويات الفيدرالية
- **Kerberos:** Utilizing Kerberos for secure authentication in on-premise systems. استخدام Kerberos للمصادقة الآمنة في الأنظمة المحلية
- **LDAP:** Leveraging LDAP for directory services and authentication. استخدام LDAP لخدمات الدليل والمصادقة
- **RADIUS:** Implementing RADIUS for centralized authentication, authorization, and accounting. استخدام RADIUS للمصادقة والتفويض والمحاسبة المركزية

Use Case: An organization uses on-premise federated identity management to allow employees to access internal applications with a single login. تستخدم منظمة إدارة الهوية الفيدرالية المحلية للسماح للموظفين بالوصول إلى التطبيقات الداخلية باستخدام تسجيل دخول واحد

3.2 Cloud

Definition: Federated identity management using cloud-based identity providers.

إدارة الهوية الفيدرالية باستخدام مزودي الهوية المستندة إلى السحابة

Examples:

- **Azure AD:** Using Azure Active Directory for federated identity management. استخدام Azure Active Directory لإدارة الهوية الفيدرالية
- **Okta:** Leveraging Okta for cloud-based identity management and SSO. استخدام Okta لإدارة الهوية المستندة إلى السحابة وتسجيل الدخول الأحادي
- **AWS Cognito:** Utilizing AWS Cognito for secure user authentication and data synchronization. استخدام AWS Cognito للمصادقة الآمنة للمستخدمين ومزامنة البيانات
- **Google Cloud Identity:** Implementing Google Cloud Identity for unified identity, access, and device management. استخدام Google Cloud Identity لإدارة الهوية والوصول والأجهزة الموحدة
- **Ping Identity:** Using Ping Identity for identity security and intelligent access. استخدام Ping Identity لأمان الهوية والوصول الذكي

Use Case: A company uses a cloud-based federated identity provider to enable single sign-on for various cloud applications. تستخدم شركة مزود هوية فيدرالية مستندة إلى السحابة لتمكين تسجيل الدخول الأحادي لتطبيقات السحابة المختلفة

3.3 Hybrid

Definition: Federated identity management that integrates both on-premise and cloud-based systems.

إدارة الهوية الفيدرالية التي تدمج بين الأنظمة المحلية والمستندة إلى السحابة

Examples:

- **Hybrid Federated Identity:** Combining on-premise SSO with cloud-based identity providers. دمج SSO المحلي مع مزودي الهوية المستندة إلى السحابة
- **Azure AD Connect:** Using Azure AD Connect to synchronize on-premise and cloud directories. استخدام Azure AD Connect لمزامنة الأدلة المحلية والسحابية
- **PingFederate:** Leveraging PingFederate for seamless integration of on-premise and cloud identity systems. استخدام PingFederate للتكامل السلس بين الأنظمة الهوية المحلية والسحابية

- **ADFS with Azure AD:** Implementing ADFS in conjunction with Azure AD for hybrid identity management. استخدام ADFS مع Azure AD لإدارة الهوية الهجينة

- **VMware Workspace ONE:** Utilizing VMware Workspace ONE for unified endpoint management and identity management across hybrid environments. استخدام VMware Workspace ONE لإدارة نقاط النهاية الموحدة وإدارة الهوية عبر البيئات الهجينة

Use Case: An enterprise uses a hybrid federated identity solution to provide seamless access to both internal and cloud-based applications. تستخدم مؤسسة حل الهوية الفيدرالية الهجينة لتوفير الوصول السلس إلى التطبيقات الداخلية والمستندة إلى السحابة

Multiple Choice Questions

1. What is federated identity management?

a. Managing identities within a single organization

b. Allowing users to use the same identification data to access multiple networks

c. Using multiple authentication methods

d. Managing access rights based on roles

2. Which federated identity solution combines on-premise and cloud-based systems?

a. On-Premise

b. Cloud

c. Hybrid

d. Single Sign-On (SSO)

3. What is an example of a cloud-based federated identity provider?

a. Internal SSO

b. Azure AD

c. Role-Based Access Control (RBAC)

d. Multi-Factor Authentication (MFA)

4. What type of federated identity management is implemented within an organization's own infrastructure?

a. On-Premise

b. Cloud

c. Hybrid

d. Single Sign-On (SSO)

5. What is the benefit of using federated identity management in a hybrid environment?

a. Increased security

b. Simplified management

c. Seamless access to both internal and cloud-based applications

d. Improved encryption

Answers and Explanations

1. b. Allowing users to use the same identification data to access multiple networks

Federated identity management allows users to use the same identification data to access multiple networks.

تسمح إدارة الهوية الفيدرالية للمستخدمين باستخدام نفس بيانات التعريف للوصول إلى

شبكات متعددة

2. c. Hybrid

Hybrid federated identity management integrates both on-premise and cloud-based systems.

تدمج إدارة الهوية الفيدرالية الهجينة بين الأنظمة المحلية والمستندة إلى السحابة

3. b. Azure AD

Azure AD is an example of a cloud-based federated identity provider.

هو مثال على مزود هوية فيدرالية مستندة إلى السحابة

4. a. On-Premise

On-premise federated identity management is implemented within an organization's own infrastructure.

يتم تنفيذ إدارة الهوية الفيدرالية المحلية داخل البنية التحتية الخاصة بالمؤسسة

5. c. Seamless access to both internal and cloud-based applications

Hybrid federated identity management provides seamless access to both internal and cloud-based applications.

توفر إدارة الهوية الفيدرالية الهجينة الوصول السلس إلى التطبيقات الداخلية والمستندة إلى السحابة

---

4. Implement and Manage Authorization Mechanisms

4.1 Access Control Models

- Role-based access control (RBAC)
- Rule based access control
- Mandatory access control (MAC)
- Discretionary access control (DAC)
- Attribute-based access control (ABAC)
- Risk based access control

4.1.1 Role-Based Access Control (RBAC)

Definition: Access control based on user roles within an organization.

التحكم في الوصول بناءً على أدوار المستخدمين داخل المنظمة

Examples:

- **Job Functions:** Assigning access rights based on job functions. تعيين حقوق الوصول بناءً على وظائف العمل
- **Role Hierarchies:** Defining hierarchies of roles to manage access. تعريف التسلسل الهرمي للأدوار لإدارة الوصول

Use Case: An organization uses RBAC to ensure that employees have access only to the resources necessary for their job functions. تستخدم منظمة RBAC لضمان أن الموظفين لديهم الوصول فقط إلى الموارد اللازمة لوظائفهم

4.1.2 Rule-Based Access Control

Definition: Access control based on a set of rules defined by the organization.

التحكم في الوصول بناءً على مجموعة من القواعد التي تحددها المنظمة

Examples:

- **Access Rules:** Defining rules for access based on conditions such as time of day or location. تحديد قواعد الوصول بناءً على شروط مثل وقت اليوم أو الموقع

- **Policy Enforcement:** Enforcing access control policies through rules. فرض سياسات التحكم في الوصول من خلال القواعد

Use Case: A company uses rule-based access control to restrict access to its systems outside of business hours. تستخدم شركة التحكم في الوصول المستند إلى القواعد لتقييد الوصول إلى أنظمتها خارج ساعات العمل

4.1.3 Mandatory Access Control (MAC)

Definition: Access control based on a set of predefined policies and rules.

التحكم في الوصول بناءً على مجموعة من السياسات والقواعد المحددة مسبقًا

Examples:

- **Security Labels:** Using labels to classify information and enforce access controls. استخدام الملصقات لتصنيف المعلومات وفرض ضوابط الوصول
- **Clearance Levels:** Granting access based on security clearance levels. منح الوصول بناءً على مستويات التصريح الأمني

Use Case: A government agency uses MAC to enforce strict access controls based on security classifications. تستخدم وكالة حكومية MAC بناءً لفرض ضوابط وصول صارمة على التصنيفات الأمنية

4.1.4 Discretionary Access Control (DAC)

Definition: Access control based on the discretion of the resource owner.

التحكم في الوصول بناءً على تقدير مالك المورد

Examples:

- **File Permissions:** Allowing file owners to set permissions for their files. السماح لأصحاب الملفات بتحديد أذونات لملفاتهم
- **Resource Sharing:** Allowing resource owners to share access with others. السماح لأصحاب الموارد بمشاركة الوصول مع الآخرين

Use Case: A project manager sets file permissions to allow team members to access project documents. يقوم مدير المشروع بتحديد أذونات الملفات للسماح لأعضاء الفريق بالوصول إلى مستندات المشروع

4.1.5 Attribute-Based Access Control (ABAC)

Definition: Access control based on user attributes and environmental conditions.

التحكم في الوصول بناءً على سمات المستخدم والشروط البيئية

Examples:

- **User Attributes:** Granting access based on attributes such as department, job role, or security clearance. منح الوصول بناءً على سمات مثل القسم أو الدور الوظيفي أو التصريح الأمني
- **Environmental Conditions:** Granting access based on conditions such as time of day, location, or device type. منح الوصول بناءً على شروط مثل وقت اليوم أو الموقع أو نوع الجهاز

Use Case: An organization uses ABAC to grant access to sensitive data only during business hours and only from secure devices. تستخدم منظمة ABAC لمنح الوصول إلى البيانات الحساسة فقط خلال ساعات العمل ومن الأجهزة الآمنة فقط

4.1.6 Risk-Based Access Control

Definition: Access control based on the assessment of risk levels.

التحكم في الوصول بناءً على تقييم مستويات المخاطر

Examples:

- **Risk Assessment:** Evaluating the risk associated with granting access to a resource. تقييم المخاطر المرتبطة بمنح الوصول إلى مورد
- **Dynamic Access Control:** Adjusting access control decisions based on real-time risk assessments. تعديل قرارات التحكم في الوصول بناءً على تقييمات المخاطر في الوقت الفعلي

Use Case: A financial institution uses risk-based access control to restrict access to high-risk transactions unless additional authentication is provided. تستخدم مؤسسة مالية التحكم في الوصول المستند إلى المخاطر لتقييد الوصول إلى المعاملات عالية المخاطر إلا إذا تم تقديم مصادقة إضافية

4.2 Access Control Techniques

- Access Control Lists (ACLs)
- Risk based access control

- Access policy enforcement

4.2.1 Access Control Lists (ACLs)

Definition: Lists that specify which users or system processes are granted access to objects.

قوائم تحدد المستخدمين أو عمليات النظام الممنوحة الوصول إلى الكائنات

Examples:

- **File ACLs:** Lists that specify which users can read, write, or execute a file. قوائم ACL للملفات: قوائم تحدد المستخدمين الذين يمكنهم قراءة أو كتابة أو تنفيذ ملف
- **Network ACLs:** Lists that control which network traffic is allowed or denied. قوائم ACL للشبكة: قوائم تتحكم في حركة المرور التي يُسمح بها أو يُرفضها
- **Database ACLs:** Lists that specify access permissions for database users. قوائم ACL لقواعد البيانات: قوائم تحدد أذونات الوصول لمستخدمي قاعدة البيانات
- **API ACLs:** Lists that control access to APIs. قوائم ACL لواجهات البرمجة: قوائم تتحكم في الوصول إلى واجهات برمجة التطبيقات
- **Directory ACLs:** Lists that specify access permissions for directory services. قوائم ACL لدليل الخدمات: قوائم تحدد أذونات الوصول لخدمات الدليل

Use Case: A network administrator configures network ACLs to allow only authorized devices to connect to the company network. يقوم مسؤول الشبكة بتكوين قوائم ACL للشبكة للسماح فقط للأجهزة المصرح لها بالاتصال بشبكة الشركة

4.2.2 Access Policy Enforcement

Definition: Enforcing access control policies through designated points in the network or system.

فرض سياسات التحكم في الوصول من خلال نقاط محددة في الشبكة أو النظام

Examples:

- **Policy Decision Point (PDP):** The component that makes access control decisions. نقطة

قرار السياسة: المكون الذي يتخذ قرارات التحكم في الوصول

- **Policy Enforcement Point (PEP):** The component that enforces access control decisions. نقطة تنفيذ السياسة: المكون الذي ينفذ قرارات التحكم في الوصول
- **Access Gateways:** Devices or systems that enforce access control policies at network entry points. بوابات الوصول: أجهزة أو أنظمة تفرض سياسات التحكم في الوصول عند نقاط دخول الشبكة
- **Firewall Rules:** Configuring firewall rules to enforce access control policies. قواعد الجدار الناري: تكوين قواعد الجدار الناري لفرض سياسات التحكم في الوصول
- **Endpoint Security Solutions:** Using endpoint security software to enforce access control policies. حلول أمان النقاط النهائية: استخدام برامج أمان النقاط النهائية لفرض سياسات التحكم في الوصول

Use Case: An organization uses PDPs, PEPs, and access gateways to enforce access control policies for its cloud services. تستخدم منظمة نقاط قرار السياسة ونقاط تنفيذ السياسة وبوابات الوصول لفرض سياسات التحكم في الوصول لخدماتها السحابية

Multiple Choice Questions

1. What is the primary purpose of Role-Based Access Control (RBAC)?

a. Increased security

b. Simplified management of access rights

c. Improved encryption

d. Enhanced user interfaces

2. What is the key feature of Mandatory Access Control (MAC)?

a. Access control based on user discretion

b. Access control enforced by a central authority based on security labels

c. Access control based on user roles

d. Access control based on user attributes

3. Which access control model adjusts access control decisions based on real-time risk assessments?

a. Role-Based Access Control (RBAC)

b. Discretionary Access Control (DAC)

c. Attribute-Based Access Control (ABAC)

d. Risk-Based Access Control (RBAC)

4. What is an Access Control List (ACL)?

a. A list that specifies which users or system processes are granted access to objects

b. A component that makes access control decisions

c. A component that enforces access control decisions

d. A list that defines security labels

5. How does rule-based access control manage access?

a. By assigning access rights based on job functions

b. By defining rules for access based on conditions such as time of day or location

c. By granting access based on user attributes and environmental conditions

d. By evaluating the risk associated with granting access to a resource

---

Answers and Explanations

1. b. Simplified management of access rights

Role-Based Access Control (RBAC) simplifies the management of access rights by assigning permissions based on user roles.

يبسط التحكم في الوصول المستند إلى الدور إدارة حقوق الوصول من خلال تعيين الأذونات بناءً على أدوار المستخدمين

2. b. Access control enforced by a central authority based on security labels

Mandatory Access Control (MAC) is enforced by a central authority based on security labels.

يتم فرض التحكم الإجباري في الوصول بواسطة سلطة مركزية بناءً على تصنيفات الأمان

3. d. Risk-Based Access Control (RBAC)

Risk-Based Access Control adjusts access control decisions based on real-time risk assessments.

يتحكم الوصول المستند إلى المخاطر في قرارات التحكم في الوصول بناءً على تقييمات المخاطر في الوقت الفعلي

4. a. A list that specifies which users or system processes are granted access to objects

An Access Control List (ACL) specifies which users or system processes are granted access to objects.

تحدد قائمة التحكم في الوصول المستخدمين أو عمليات النظام الممنوحة الوصول إلى الكائنات

5. b. By defining rules for access based on conditions such as time of day or location

Rule-based access control manages access by defining rules based on conditions such as time of day or location.

يتحكم الوصول المستند إلى القواعد في الوصول من خلال تحديد القواعد بناءً على شروط مثل وقت اليوم أو الموقع

5. Manage the Identity and Access Provisioning Lifecycle

5.1 Account Access Review

Definition: Periodically reviewing user accounts to ensure that access rights are appropriate.

مراجعة حسابات المستخدمين بشكل دوري لضمان أن حقوق الوصول مناسبة

Examples:

- **User Accounts:** Reviewing access rights of user accounts to ensure they match job functions. حسابات المستخدمين: مراجعة حقوق الوصول لحسابات المستخدمين لضمان تطابقها مع وظائف العمل
- **System Accounts:** Reviewing access rights of system accounts to ensure they are not excessive. حسابات النظام: مراجعة حقوق الوصول لحسابات النظام لضمان عدم وجودها بشكل مفرط
- **Privileged Accounts:** Reviewing access rights of privileged accounts to ensure they are still necessary. حسابات متميزة: مراجعة حقوق الوصول لحسابات متميزة لضمان أنها لا تزال ضرورية
- **Service Accounts:** Reviewing access rights of service accounts to ensure they are not over-privileged. حسابات الخدمة: مراجعة حقوق الوصول لحسابات الخدمة لضمان عدم وجود امتيازات زائدة

Use Case: An organization conducts quarterly reviews of user accounts to ensure that access rights are updated based on role changes. تقوم منظمة بإجراء مراجعات ربع سنوية لحسابات المستخدمين لضمان تحديث حقوق الوصول بناءً على تغييرات الدور

5.2 Provisioning and Deprovisioning

Definition: The process of creating and deleting user accounts and access rights.

عملية إنشاء وحذف حسابات المستخدمين وحقوق الوصول

Examples:

- **Onboarding:** Creating user accounts and granting access rights for new employees. التوظيف: إنشاء حسابات المستخدمين ومنح حقوق الوصول للموظفين الجدد
- **Offboarding:** Deleting user accounts and revoking access rights for departing employees. إنهاء الخدمة: حذف حسابات المستخدمين وإلغاء حقوق الوصول للموظفين المغادرين
- **Automated Provisioning:** Using automated tools to create and manage user accounts. التوفير الآلي: استخدام أدوات آلية لإنشاء وإدارة حسابات المستخدمين
- **Manual Provisioning:** Manually creating and managing user accounts. التوفير اليدوي: إنشاء وإدارة حسابات المستخدمين يدويًا
- **Just-In-Time Provisioning:** Providing user accounts and access rights only when needed. التوفير في الوقت المناسب: توفير حسابات المستخدمين وحقوق الوصول فقط عندما تكون مطلوبة

Use Case: A company automates the provisioning and deprovisioning process to ensure that access rights are promptly updated when employees join or leave the organization. تقوم شركة بأتمتة عملية التوفير والإلغاء لضمان تحديث حقوق الوصول بسرعة عندما ينضم الموظفون أو يغادرون المنظمة

5.3 Role Definition and Transition

Definition: Defining roles and managing transitions between roles.

تعريف الأدوار وإدارة التحولات بين الأدوار

Examples:

- **Role Assignment:** Assigning roles to employees based on job functions. تعيين الأدوار: تعيين الأدوار للموظفين بناءً على وظائف العمل
- **Role Transition:** Managing transitions between roles when employees change positions. تحول الأدوار: إدارة التحولات بين الأدوار عندما يغير الموظفون المناصب
- **Role Hierarchies:** Defining hierarchies of roles to manage access. تعريف التسلسل الهرمي للأدوار لإدارة الوصول

- **Role Mapping:** Mapping roles to access rights to ensure consistency. تعيين الأدوار: تعيين الأدوار لحقوق الوصول لضمان التناسق

- **Role-Based Access Control (RBAC):** Using RBAC to manage role definitions and transitions. استخدام RBAC التحكم في الوصول المستند إلى الدور: لإدارة تعريف الأدوار والتحولات

Use Case: An organization defines clear roles and manages transitions to ensure that employees have the appropriate access rights when they change positions. تقوم منظمة بتحديد الأدوار بوضوح وإدارة التحولات لضمان أن يكون لدى الموظفين حقوق الوصول المناسبة عندما يغيرون المناصب

5.4 Privilege Escalation

Definition: The process of granting higher levels of access privileges, often temporarily.

عملية منح مستويات أعلى من حقوق الوصول، غالبًا بشكل مؤقت

Examples:

- **Sudo:** A command that allows users to execute commands with elevated privileges. Sudo: أمر يسمح للمستخدمين بتنفيذ الأوامر بامتيازات مرتفعة

- **Auditing:** Monitoring and auditing the use of elevated privileges. التدقيق: مراقبة واستخدام الامتيازات المرتفعة

- **Temporary Access:** Granting temporary administrative access for specific tasks. منح الوصول المؤقت الإداري للمهام المحددة

- **Privilege Management:** Managing and monitoring elevated privileges to ensure they are used appropriately. إدارة الامتيازات: إدارة ومراقبة الامتيازات المرتفعة لضمان استخدامها بشكل مناسب

- **Emergency Access:** Granting emergency access to resolve critical issues. منح الوصول الطارئ لحل القضايا الحرجة

Use Case: A system administrator uses sudo to perform administrative tasks and audits the use of elevated privileges to ensure compliance. يستخدم مسؤول النظام

لتنفيذ المهام الإدارية ويقوم بتدقيق استخدام الامتيازات المرتفعة لضمان الامتثال Sudo

---

5.5 Service Accounts Management

Definition: Managing accounts used by applications or services rather than individual users.

إدارة الحسابات المستخدمة من قبل التطبيقات أو الخدمات بدلاً من المستخدمين الأفراد

Examples:

- **Service Accounts:** Creating and managing accounts used by services or applications. حسابات الخدمة: إنشاء وإدارة الحسابات المستخدمة من قبل الخدمات أو التطبيقات
- **Account Security:** Implementing security measures to protect service accounts. أمان الحساب: تنفيذ تدابير أمنية لحماية حسابات الخدمة
- **Service Account Rotation:** Regularly rotating service account credentials to enhance security. تدوير حساب الخدمة: تدوير بيانات اعتماد حساب الخدمة بانتظام لتعزيز الأمان
- **Service Account Auditing:** Monitoring and auditing the use of service accounts. تدقيق حساب الخدمة: مراقبة واستخدام حسابات الخدمة
- **Service Account Access Controls:** Implementing access controls to restrict the use of service accounts. ضوابط الوصول لحساب الخدمة: تنفيذ ضوابط الوصول لتقييد استخدام حسابات الخدمة

Use Case: An organization manages service accounts to ensure that they are used securely and do not pose a security risk. تدير منظمة حسابات الخدمة لضمان استخدامها بشكل آمن وعدم تشكيلها خطرًا أمنيًا

Multiple Choice Questions

1. What is the primary purpose of account access review?

a. To increase data availability

b. To ensure that access rights are appropriate

c. To improve data encryption

d. To monitor data access

2. What does provisioning refer to in the context of IAM?

a. Reviewing user accounts

b. Creating and deleting user accounts and access rights

c. Defining roles and managing transitions

d. Granting higher levels of access privileges

3. Which process involves granting higher levels of access privileges, often temporarily?

a. Account Access Review

b. Provisioning

c. Role Transition

d. Privilege Escalation

4. What is the role of auditing in privilege escalation?

a. To create user accounts

b. To monitor and audit the use of elevated privileges

c. To delete user accounts

d. To manage transitions between roles

5. How are service accounts different from individual user accounts?

a. They are used by applications or services rather than individual users

b. They are reviewed periodically

c. They are created during onboarding

d. They are deleted during offboarding

Answers and Explanations

1. b. To ensure that access rights are appropriate

The primary purpose of account access review is to ensure that access rights are appropriate.

الهدف الأساسي من مراجعة حسابات المستخدمين هو ضمان أن تكون حقوق الوصول مناسبة

2. b. Creating and deleting user accounts and access rights

Provisioning refers to the process of creating and deleting user accounts and access rights.

يشير التوفير إلى عملية إنشاء وحذف حسابات المستخدمين وحقوق الوصول

3. d. Privilege Escalation

Privilege escalation involves granting higher levels of access privileges, often temporarily.

يتضمن تصعيد الامتيازات منح مستويات أعلى من حقوق الوصول، غالبًا بشكل مؤقت

4. b. To monitor and audit the use of elevated privileges

Auditing in privilege escalation is used to monitor and audit the use of elevated privileges.

يُستخدم التدقيق في تصعيد الامتيازات لمراقبة وتدقيق استخدام الامتيازات المرتفعة

5. a. They are used by applications or services rather than individual users

Service accounts are used by applications or services rather than individual users.

تُستخدم حسابات الخدمة من قبل التطبيقات أو الخدمات بدلاً من المستخدمين الأفراد

---

6. Implement Authentication Systems

6.1 Password Authentication

Definition: The process of verifying a user's identity based on a secret password.

عملية التحقق من هوية المستخدم بناءً على كلمة مرور سرية

Examples:

- **Password Policies:** Enforcing policies such as password complexity and expiration. سياسات كلمة المرور: فرض سياسات مثل تعقيد كلمة المرور وانتهائها
- **Password Management Tools:** Tools to help users manage and store passwords securely. أدوات إدارة كلمة المرور: أدوات لمساعدة المستخدمين في إدارة كلمات المرور وتخزينها بأمان

Use Case: An organization enforces password policies and uses password management tools to ensure secure password practices. تفرض منظمة سياسات كلمة المرور وتستخدم أدوات إدارة كلمة المرور لضمان ممارسات كلمة مرور آمنة

6.2 Multi-Factor Authentication (MFA)

Definition: The process of verifying a user's identity using multiple methods.

عملية التحقق من هوية المستخدم باستخدام طرق متعددة

Examples:

- **MFA Methods:** Using a combination of passwords, biometrics, and tokens. طرق MFA: استخدام مزيج من كلمات المرور والبيومترية والرموز

- **MFA Devices:** Devices such as smartphones or hardware tokens used for authentication. أجهزة MFA: أجهزة مثل الهواتف الذكية أو الرموز الصلبة المستخدمة للمصادقة

- **Companies:** Okta, Duo Security, Microsoft Authenticator, Google Authenticator, RSA SecurID.

Use Case: A company uses MFA to secure remote access by requiring both a password and a fingerprint. تستخدم شركة المصادقة متعددة العوامل لتأمين الوصول عن بعد من خلال طلب كلمة مرور وبصمة إصبع

6.3 Biometric Authentication

Definition: The process of verifying a user's identity based on physical or behavioral characteristics.

عملية التحقق من هوية المستخدم بناءً على الخصائص الفيزيائية أو السلوكية

Examples:

- **Fingerprint Scanners:** Devices that read and verify fingerprints. ماسحات بصمات الأصابع: أجهزة تقرأ وتتحقق من بصمات الأصابع

- **Facial Recognition:** Technology that verifies identity based on facial features. التعرف على الوجه: تقنية تتحقق من الهوية بناءً على ملامح الوجه

Use Case: An airport uses biometric authentication to verify the identity of passengers at security checkpoints. يستخدم مطار المصادقة البيومترية للتحقق من هوية الركاب عند نقاط التفتيش الأمنية

6.4 Token-Based Authentication

Definition: The process of verifying a user's identity using a physical or virtual token.

عملية التحقق من هوية المستخدم باستخدام رمز مادي أو افتراضي

Examples:

- **Hardware Tokens:** Physical devices that generate one-time passwords. رموز الأجهزة: أجهزة مادية تولد كلمات مرور لمرة واحدة
- **Software Tokens:** Applications that generate one-time passwords. رموز البرمجيات: تطبيقات تولد كلمات مرور لمرة واحدة

Use Case: A financial institution uses hardware tokens to authenticate employees accessing secure systems. تستخدم مؤسسة مالية رموز الأجهزة لمصادقة الموظفين الذين يصلون إلى الأنظمة الآمنة

6.5 Certificate-Based Authentication

Definition: The process of verifying a user's identity using digital certificates.

عملية التحقق من هوية المستخدم باستخدام الشهادات الرقمية

Examples:

- **Digital Certificates:** Electronic documents that use public key infrastructure (PKI) to verify identity. الشهادات الرقمية: مستندات إلكترونية تستخدم بنية المفاتيح العامة للتحقق من الهوية
- **Certificate Authorities:** Entities that issue and manage digital certificates. سلطات الشهادات: كيانات تصدر وتدير الشهادات الرقمية

Use Case: A company uses digital certificates to authenticate users accessing its secure website. تستخدم شركة الشهادات الرقمية لمصادقة المستخدمين الذين يصلون إلى موقعها الآمن

Multiple Choice Questions

1. What is the primary purpose of password policies?

a. To increase data availability

b. To enforce secure password practices

c. To improve data encryption

d. To monitor data access

2. What does multi-factor authentication (MFA) involve?

a. Using a single password for authentication

b. Using multiple methods to verify a user's identity

c. Using physical characteristics for authentication

d. Using digital certificates for authentication

3. Which authentication method verifies identity based on physical or behavioral characteristics?

a. Password Authentication

b. Token-Based Authentication

c. Biometric Authentication

d. Certificate-Based Authentication

4. What is a hardware token used for?

a. Storing digital certificates

b. Generating one-time passwords

c. Scanning fingerprints

d. Recognizing facial features

5. How does certificate-based authentication verify identity?

a. Using passwords

b. Using physical tokens

c. Using digital certificates

d. Using behavioral characteristics

Answers and Explanations

1. b. To enforce secure password practices

Password policies enforce secure password practices by requiring complex passwords and regular changes.

تفرض سياسات كلمة المرور ممارسات كلمة مرور آمنة من خلال طلب كلمات مرور معقدة وتغييرات منتظمة

2. b. Using multiple methods to verify a user's identity

Multi-factor authentication (MFA) involves using multiple methods, such as passwords, biometrics, and tokens, to verify a user's identity.

تتضمن المصادقة متعددة العوامل استخدام طرق متعددة، مثل كلمات المرور والبيومترية والرموز، للتحقق من هوية المستخدم

3. c. Biometric Authentication

Biometric authentication verifies identity based on physical or behavioral characteristics, such as fingerprints or facial recognition.

تتحقق المصادقة البيومترية من الهوية بناءً على الخصائص الفيزيائية أو السلوكية، مثل بصمات الأصابع أو التعرف على الوجه

4. b. Generating one-time passwords

Hardware tokens are physical devices used to generate one-time passwords for authentication.

رموز الأجهزة هي أجهزة مادية تُستخدم لتوليد كلمات مرور لمرة واحدة للمصادقة

5. c. Using digital certificates

Certificate-based authentication verifies identity using digital certificates issued and managed by certificate authorities.

تتحقق المصادقة المستندة إلى الشهادات من الهوية باستخدام الشهادات الرقمية التي تصدرها وتديرها سلطات الشهادات

---

7. Identity and Access Management Technologies

7.1 Directory Services

Definition: Systems that store and manage information about users and resources in a network.

أنظمة تخزن وتدير المعلومات عن المستخدمين والموارد في الشبكة

Examples:

- **Active Directory:** A directory service developed by Microsoft for Windows domain networks. Active Directory: خدمة دليل طورتها Microsoft لشبكات المجال Windows
- **LDAP (Lightweight Directory Access Protocol):** An open protocol used to access and maintain directory information. بروتوكول الوصول إلى الدليل الخفيف: بروتوكول مفتوح يستخدم للوصول إلى معلومات الدليل والحفاظ عليها

Use Case: An organization uses Active Directory to manage user accounts and access permissions across its network. تستخدم منظمة Active Directory لإدارة حسابات المستخدمين وأذونات الوصول عبر شبكتها

7.2 Identity Management (IdM)

Definition: The process of managing the identity lifecycle, including creation, maintenance, and deletion of identities.

عملية إدارة دورة حياة الهوية، بما في ذلك إنشاء الهويات وصيانتها وحذفها

Examples:

- **User Provisioning:** Automating the process of creating and managing user accounts. توفير المستخدمين: أتمتة عملية إنشاء حسابات المستخدمين وإدارتها
- **Identity Governance:** Ensuring that identity policies and practices comply with regulations and standards. حوكمة الهوية: ضمان أن السياسات والممارسات الهوية تتوافق مع اللوائح والمعايير

Use Case: A company uses an identity management system to automate the provisioning and deprovisioning of user accounts. تستخدم شركة نظام إدارة الهوية لأتمتة توفير وإلغاء توفير حسابات المستخدمين

7.3 Access Management

Definition: The process of managing access to resources based on policies and rules.

عملية إدارة الوصول إلى الموارد بناءً على السياسات والقواعد

Examples:

- **Single Sign-On (SSO):** Allowing users to access multiple applications with one set of login credentials. تسجيل الدخول الأحادي: السماح للمستخدمين بالوصول إلى تطبيقات متعددة باستخدام مجموعة واحدة من بيانات تسجيل الدخول
- **Federated Identity Management:** Allowing users to use the same identification data to access multiple networks. إدارة الهوية الفيدرالية: السماح للمستخدمين باستخدام نفس بيانات التعريف للوصول إلى شبكات متعددة

Use Case: An enterprise uses access management to ensure that employees can

seamlessly access both internal and external applications. تستخدم مؤسسة إدارة الوصول لضمان أن يتمكن الموظفون من الوصول السلس إلى التطبيقات الداخلية والخارجية

7.4 Privileged Access Management (PAM)

Definition: The process of managing and monitoring privileged accounts and access rights.

عملية إدارة ومراقبة الحسابات المتميزة وحقوق الوصول

Examples:

- **Privileged Account Management:** Managing accounts with elevated privileges to ensure they are used securely. إدارة الحسابات المتميزة: إدارة الحسابات بامتيازات مرتفعة لضمان استخدامها بشكل آمن
- **Session Monitoring:** Monitoring and recording sessions initiated by privileged accounts. مراقبة الجلسات: مراقبة وتسجيل الجلسات التي تبدأها الحسابات المتميزة

Use Case: A company uses PAM to manage and monitor the use of administrative accounts to prevent unauthorized access. تستخدم شركة إدارة ومراقبة الوصول المتميز لإدارة ومراقبة استخدام الحسابات الإدارية لمنع الوصول غير المصرح به

Multiple Choice Questions

1. What is the primary function of directory services in IAM?

a. To manage passwords

b. To store and manage information about users and resources in a network

c. To authenticate users

d. To encrypt data

2. What does identity management (IdM) involve?

a. Managing the identity lifecycle, including creation, maintenance, and deletion of identities

b. Storing and managing information about users and resources in a network

c. Allowing users to access multiple applications with one set of login credentials

d. Monitoring privileged accounts and access rights

3. Which technology allows users to access multiple applications with one set of login credentials?

a. Multi-Factor Authentication (MFA)

b. Single Sign-On (SSO)

c. Directory Services

d. Privileged Access Management (PAM)

4. What is the purpose of privileged access management (PAM)?

a. To manage and monitor privileged accounts and access rights

b. To automate the provisioning and deprovisioning of user accounts

c. To ensure that identity policies comply with regulations

d. To authenticate users

5. How does federated identity management benefit users?

a. By encrypting their data

b. By allowing them to use the same identification data to access multiple networks

c. By managing their passwords

d. By storing their information in a directory service

Answers and Explanations

1. b. To store and manage information about users and resources in a network

Directory services store and manage information about users and resources in a network.

تقوم خدمات الدليل بتخزين وإدارة المعلومات حول المستخدمين والموارد في الشبكة

2. a. Managing the identity lifecycle, including creation, maintenance, and deletion of identities

Identity management (IdM) involves managing the identity lifecycle, including creation, maintenance, and deletion of identities.

تشمل إدارة الهوية إدارة دورة حياة الهوية، بما في ذلك إنشاء الهويات وصيانتها وحذفها

3. b. Single Sign-On (SSO)

Single Sign-On (SSO) allows users to access multiple applications with one set of login credentials.

يسمح تسجيل الدخول الأحادي للمستخدمين بالوصول إلى تطبيقات متعددة باستخدام مجموعة واحدة من بيانات تسجيل الدخول

4. a. To manage and monitor privileged accounts and access rights

Privileged access management (PAM) manages and monitors privileged accounts and access rights.

تقوم إدارة الوصول المتميز بإدارة ومراقبة الحسابات المتميزة وحقوق الوصول

5. b. By allowing them to use the same identification data to access multiple networks

Federated identity management allows users to use the same identification data to access multiple networks.

تسمح إدارة الهوية الفيدرالية للمستخدمين باستخدام نفس بيانات التعريف للوصول إلى شبكات متعددة

---

8. IAM Best Practices and Challenges

8.1 Best Practices

8.1.1 Implement Strong Authentication Methods

Definition: Using robust authentication methods to verify user identities.

استخدام طرق مصادقة قوية للتحقق من هويات المستخدمين

Examples:

- **Multi-Factor Authentication (MFA):** Combining multiple authentication methods to enhance security. المصادقة متعددة العوامل: دمج طرق مصادقة متعددة لتعزيز الأمان
- **Biometric Authentication:** Using physical or behavioral characteristics to verify identity. المصادقة البيومترية: استخدام الخصائص الفيزيائية أو السلوكية للتحقق من الهوية

Use Case: An organization implements MFA and biometric authentication to secure access to sensitive systems. تقوم منظمة بتنفيذ المصادقة متعددة العوامل والمصادقة البيومترية لتأمين الوصول إلى الأنظمة الحساسة

8.1.2 Regularly Review and Update Access Controls

Definition: Periodically reviewing and updating access controls to ensure they remain effective.

مراجعة وتحديث ضوابط الوصول بشكل دوري لضمان بقائها فعالة

Examples:

- **Access Reviews:** Conducting regular reviews of access permissions to ensure they are appropriate. مراجعات الوصول: إجراء مراجعات دورية لأذونات الوصول لضمان أنها مناسبة

- **Policy Updates:** Updating access control policies to reflect changes in the organization or threat landscape. تحديث السياسات: تحديث سياسات التحكم في الوصول لتعكس التغييرات في المنظمة أو مشهد التهديدات

Use Case: A company conducts quarterly access reviews and updates its access control policies to address new security threats. تقوم شركة بإجراء مراجعات ربع سنوية للوصول وتحديث سياسات التحكم في الوصول لمعالجة التهديدات الأمنية الجديدة

8.1.3 Implement Least Privilege

Definition: Providing users with the minimum level of access necessary to perform their job functions.

تزويد المستخدمين بالحد الأدنى من الوصول اللازم لأداء وظائفهم

Examples:

- **Access Rights:** Granting employees only the access rights they need to perform their duties. منح الموظفين فقط حقوق الوصول التي يحتاجونها لأداء واجباتهم

- **Role-Based Access Control (RBAC):** Assigning access rights based on user roles. التحكم في الوصول المستند إلى الدور: تعيين حقوق الوصول بناءً على أدوار المستخدمين

Use Case: An organization implements least privilege by restricting administrative access to systems to only a few IT administrators. تقوم منظمة بتنفيذ مبدأ أقل الامتيازات من خلال تقييد الوصول الإداري إلى الأنظمة لعدد قليل من مسؤولي تكنولوجيا المعلومات

8.1.4 Use Automated Identity Management Tools

Definition: Using tools to automate the management of identities and access rights.

استخدام أدوات لأتمتة إدارة الهويات وحقوق الوصول

Examples:

- **Identity Provisioning:** Automating the process of creating and managing user accounts. توفير الهوية: أتمتة عملية إنشاء حسابات المستخدمين وإدارتها
- **Access Reviews:** Using tools to automate the review and update of access permissions. مراجعات الوصول: استخدام أدوات لأتمتة مراجعة وتحديث أذونات الوصول

Use Case: A company uses identity management tools to automate the provisioning and deprovisioning process, reducing the risk of human error. تستخدم شركة أدوات إدارة الهوية لأتمتة عملية التوفير والإلغاء، مما يقلل من مخاطر الخطأ البشري

8.2 Detailed Comparison Between PAM and IAM

8.2.1 Privileged Access Management (PAM)

Definition: The process of managing and monitoring privileged accounts and access rights.

عملية إدارة ومراقبة الحسابات المتميزة وحقوق الوصول

Examples:

- **Session Management:** Monitoring and controlling sessions initiated by privileged accounts. إدارة الجلسات: مراقبة والسيطرة على الجلسات التي تبدأها الحسابات المتميزة.
- **Credential Vaulting:** Storing privileged account credentials in a secure vault. تخزين بيانات الاعتماد: تخزين بيانات اعتماد الحسابات المتميزة في مخزن آمن

Top 5 PAM Products:

- **CyberArk:** Offers comprehensive privileged access security solutions.
- **BeyondTrust:** Provides privilege management and vulnerability management solutions.
- **Thycotic:** Delivers password and privilege access management solutions.
- **ManageEngine PAM360:** Integrates IT operations management with PAM.

- **Centrify:** Focuses on securing privileged access and identity management.

Use Case: A financial institution uses CyberArk to manage and monitor administrative access to critical systems. تستخدم مؤسسة مالية CyberArk لإدارة ومراقبة الوصول الإداري إلى الأنظمة الحرجة

8.2.2 Identity and Access Management (IAM)

Definition: The process of managing user identities, access rights, and authentication methods.

عملية إدارة هويات المستخدمين وحقوق الوصول وطرق المصادقة

Examples:

- **User Provisioning:** Automating the creation and management of user accounts. توفير المستخدمين: أتمتة إنشاء حسابات المستخدمين وإدارتها
- **Single Sign-On (SSO):** Allowing users to access multiple applications with one set of login credentials. تسجيل الدخول الأحادي: السماح للمستخدمين بالوصول إلى تطبيقات متعددة باستخدام مجموعة واحدة من بيانات تسجيل الدخول

Top 5 IAM Products:

- **Okta:** Provides identity management and SSO solutions.
- **Microsoft Azure AD:** Offers directory and identity management as part of the Azure platform.
- **Ping Identity:** Delivers identity and access management solutions.
- **IBM Security Identity Governance and Intelligence:** Focuses on identity governance and intelligence.
- **SailPoint:** Provides identity governance solutions.

Use Case: A technology company uses Okta for single sign-on and identity management across its cloud applications. تستخدم شركة تكنولوجيا Okta لتسجيل الدخول الأحادي وإدارة الهوية عبر تطبيقاتها السحابية

8.2.3 Differences Between PAM and IAM

- **Scope:** PAM focuses on managing and monitoring privileged accounts, while IAM encompasses all user identities and access rights. النطاق: يركز PAM على إدارة ومراقبة الحسابات المتميزة، بينما يشمل IAM جميع هويات المستخدمين وحقوق الوصول
- **Use Cases:** PAM is used for administrative and high-risk accounts, whereas IAM is used for all user accounts and access rights. حالات الاستخدام: يستخدم PAM للحسابات الإدارية وعالية المخاطر، بينما يستخدم IAM لجميع حسابات المستخدمين وحقوق الوصول
- **Tools:** PAM tools typically include session monitoring and credential vaulting, while IAM tools focus on user provisioning, SSO, and identity governance. الأدوات: تتضمن أدوات PAM عادةً مراقبة الجلسات وتخزين بيانات الاعتماد، بينما تركز أدوات IAM على توفير المستخدمين، وتسجيل الدخول الأحادي، وحوكمة الهوية

8.3 Challenges

8.3.1 Managing Privileged Accounts

Definition: Ensuring that privileged accounts are managed securely to prevent unauthorized access.

ضمان إدارة الحسابات المتميزة بأمان لمنع الوصول غير المصرح به

Examples:

- **Privileged Account Abuse:** Preventing misuse of privileged accounts. إساءة استخدام الحسابات المتميزة: منع إساءة استخدام الحسابات المتميزة
- **Credential Theft:** Protecting against the theft of privileged account credentials. سرقة بيانات الاعتماد: الحماية من سرقة بيانات اعتماد الحسابات المتميزة

Use Case: An organization implements PAM solutions to prevent the abuse and

theft of privileged account credentials. تقوم منظمة بتنفيذ حلول PAM لمنع إساءة استخدام وسرقة بيانات اعتماد الحسابات المتميزة

8.3.2 Ensuring Compliance

Definition: Meeting regulatory and compliance requirements for identity and access management.

الوفاء بالمتطلبات التنظيمية والامتثال لإدارة الهوية والوصول

Examples:

- **Audits:** Conducting regular audits to ensure compliance with regulations. عمليات التدقيق: إجراء عمليات تدقيق منتظمة لضمان الامتثال للوائح
- **Policy Enforcement:** Ensuring that identity and access management policies are enforced. فرض السياسات: ضمان تنفيذ سياسات إدارة الهوية والوصول

Use Case: A financial institution conducts regular audits and enforces IAM policies to comply with regulatory requirements. تقوم مؤسسة مالية بإجراء عمليات تدقيق منتظمة وتطبيق سياسات IAM للامتثال للمتطلبات التنظيمية

8.3.3 Scalability

Definition: Ensuring that identity and access management solutions can scale with the organization.

ضمان أن حلول إدارة الهوية والوصول يمكن أن تتوسع مع المنظمة

Examples:

- **User Growth:** Managing the growth of user identities and access rights. نمو المستخدمين: إدارة نمو هويات المستخدمين وحقوق الوصول
- **Integration:** Integrating IAM solutions with existing systems and applications. التكامل: دمج حلول IAM مع الأنظمة والتطبيقات الحالية

Use Case: A company selects scalable IAM solutions that can grow with the organization and integrate with its existing infrastructure. تختار شركة حلول IAM القابلة للتوسع التي يمكن أن تنمو مع المنظمة وتتكامل مع البنية التحتية الحالية

Multiple Choice Questions

1. What is the primary focus of Privileged Access Management (PAM)?

a. Managing all user identities

b. Managing and monitoring privileged accounts and access rights

c. Providing single sign-on

d. Automating user provisioning

2. Which IAM product is known for providing single sign-on and identity management solutions?

a. CyberArk

b. Okta

c. BeyondTrust

d. Thycotic

3. What is a key difference between PAM and IAM?

a. PAM focuses on all user accounts, while IAM focuses on privileged accounts

b. PAM includes session monitoring, while IAM includes user provisioning and SSO

c. PAM is used for low-risk accounts, while IAM is used for high-risk accounts

d. PAM and IAM are used interchangeably without distinction

4. Which of the following is a top PAM product?

a. Okta

b. SailPoint

c. BeyondTrust

d. IBM Security Identity Governance and Intelligence

5. How does PAM contribute to security in an organization?

a. By providing single sign-on for all applications

b. By managing and monitoring the use of elevated privileges

c. By automating the creation and deletion of user accounts

d. By enabling federated identity management

Answers and Explanations

1. b. Managing and monitoring privileged accounts and access rights

The primary focus of Privileged Access Management (PAM) is managing and monitoring privileged accounts and access rights.

يركز إدارة الوصول المتميز على إدارة ومراقبة الحسابات المتميزة وحقوق الوصول

2. b. Okta

Okta is known for providing single sign-on and identity management solutions.

تشتهر بتوفير حلول تسجيل الدخول الأحادي وإدارة الهوية

3. b. PAM includes session monitoring, while IAM includes user provisioning and SSO

A key difference between PAM and IAM is that PAM includes session monitoring, while IAM includes user provisioning and SSO.

أحد الفروق الرئيسية بين

PAM و IAM

هو أن

PAM

يشمل مراقبة الجلسات، بينما يشمل

IAM

توفير المستخدمين وتسجيل الدخول الأحادي

4. c. BeyondTrust

BeyondTrust is a top PAM product known for privilege management and vulnerability management solutions.

هو منتج

PAM

معروف بحلول إدارة الامتيازات وإدارة الثغرات الأمني

5. b. By managing and monitoring the use of elevated privileges

PAM contributes to security in an organization by managing and monitoring the use of elevated privileges.

يساهم في الأمان في المؤسسة من خلال إدارة ومراقبة استخدام الامتيازات المرتفعة

Conclusion

Identity and Access Management (IAM) is a critical component of an organization's security strategy.

إدارة الهوية والوصول هي عنصر أساسي في استراتيجية الأمان الخاصة بالمنظمة

By effectively managing identities, implementing robust authentication and authorization mechanisms, and following best practices, organizations can ensure that only authorized users have access to their resources.

من خلال إدارة الهويات بفعالية ,وتنفيذ آليات مصادقة وتفويض قوية, واتباع أفضل الممارسات, ويمكن للمنظمات ضمان أن المستخدمين المصرح لهم فقط هم من يمكنهم الوصول إلى مواردها

This module has covered the fundamental principles of IAM, explored various IAM technologies, and provided best practices to address common challenges.

لقد غطى هذا المقرر المبادئ الأساسية له واستكشف التقنيات المختلفة وقدم أفضل , الممارسات لمعالجة التحديات الشائعة

Understanding and implementing IAM effectively helps protect systems and data from unauthorized access and potential security threats.

فهم وتنفيذ إدارة الهويات بفعالية يساعد في حماية الأنظمة والبيانات من الوصول غير المصرح به والتهديدات الأمنية المحتملة

CISSP Resources

1- Official $(ISC)^2$ CISSP Study Guide

2- CISSP $(ISC)^2$ Official Practice Tests

3- CISSP All-in-One Exam Guide by Shon Harris

4- Cybrary – CISSP Training by Kelly Handerhan

https://www.cybrary.it/course/cissp

5- Oreilly – CISSP Training by Sari Greene

https://www.oreilly.com/library/view/cissp-4th-edition/9780135328613/?

_gl=1*jwhz1z*_ga*MTgyMDY2NDI5LjE3MTczNzAwMDI.*_ga_092EL089CH*MTcxNzM3MDAwMi4xLjEuMTcxNzM3MDEwNi41OC4wLjA.

6- CISSP bundles by Thor Pedersen

https://thorteaches.com/cissp/

7- CISSP MindMaps YouTube Playlist from Destination Certification

https://www.youtube.com/playlist?list=PLZKdGEfEyJhLd-pJhAD7dNbJyUgpqI4pu

Ahmed El-Nagdy 1mo
Group System Admin Section Head for Misr Cement Group

ربنا يوفقك يا عماد

Like · Reply | 1 Reaction

Mohamed Atta 1mo
IT section Chief @ Galaxy Chemicals EGYPT S.A.E

Mohamed Kamal

Like · Reply | 1 Reaction

See more comments

To view or add a comment, sign in

More articles by this author

Module 7: Security Operations / إدارة عمليات...
Aug 5, 2024

Module 6: Security Assessment and Testing...
Jul 28, 2024

CISSP Module 4: Communication and...
Jul 1, 2024

See all

Insights from the community

Information Security

What are the most effective ways to manage IAM risks in the architecture industry?

Information Security

How do you audit IAM events?

Cybersecurity

What are the most cost-effective ways to improve your IAM program?

Information Security

How do you create IAM awareness and accountability?

Information Security

What is the best IAM framework for your organization?

Cybersecurity

What are the most effective identity governance and administration practices for an IAM system?

Show more

Others also viewed

Using ITIL Best Practices to Improve Access Management

Bob Cadenhead, ITIL · 8y

Identity and Access Management Domains

Rassoul Ghaznavi Zadeh · 3y

Securing Kubernetes [Authentication & Authorization]

Deepak Pandey · 5y

Step-Up Authentication vs. Forced Authentication: Understanding the Difference and Their Use Cases

Identity Access Management Jobs · 1mo

User Authentication And Authorization In Kubernetes

AJIT VEDPATHAK · 4y

Securing hybrid IT: 5 principles for identity management

René J. Aerdts, Ph.D. · 5y

Show more

Explore topics

Sales

Marketing

Business Administration

HR Management

Content Management

Engineering

Soft Skills

See All

تقييم الأمان والاختبار
Security Assessment and Testing

Emad M. Abdelhamid • 2nd
Technical Leader | SME IT Security Design @ Cisco - CX EMEA . ...
View my portfolio

+ Follow

3w • Edited •

لسلام عليكم ورحمة الله وبركاته
اليوم بإذن الله سنستكمل دراسة الشرح المختصر لشهادة ال
CISSP
وسنقدم مختصر عن فصل مهم جدا وهو الفصل السادس والذى يتحدث عن تقييم الأمان والاختبار حيث ان تقييم الأمان والاختبار هما مكونان حيويان في عملية إدارة الأمان في المؤسسة. تساعد هذه الأنشطة في تحديد الثغرات وضمان الامتثال للوائح وتحسين الوضع الأمني العام.
يغطي هذ الفصل استراتيجيات وتقنيات وعمليات متنوعة تتعلق بتقييم الأمان والاختبار.

ويحتوى على 6 أجزاء
1. Design and Validate Assessment, Test, and Audit Strategies تصميم والتحقق من استراتيجيات التقييم والاختبار والتدقيق
2. Conduct Security Controls Testing إجراء اختبارات ضوابط الأمان
3. Collect Security Process Data جمع بيانات العمليات الأمنية
4. Analyze Test Output and Generate Report تحليل نتائج الاختبار وإنشاء التقرير
5. Conduct or Facilitate Security Audits إجراء أو تسهيل التدقيقات الأمنية
6. Security Assessment and Testing Techniques تقنيات التقييم والاختبار الأمني

المقالات

For Module 1 : https://lnkd.in/dkkyFGdW
For Module 2 : https://lnkd.in/dNUWhiJs
For Module 3: https://lnkd.in/dsqBXhEc
For Module 4: https://lnkd.in/d_DBAm4h
For Module 5: https://lnkd.in/dGPDeKWF
For Module 6: https://lnkd.in/dZHHJKJx
For Module 7: https://lnkd.in/d_JswW5W
For Module 8: https://lnkd.in/dQsQHqgR

Resources - المصادر

1- Official (ISC)² CISSP Study Guide
2- CISSP (ISC)² Official Practice Tests
3- CISSP All-in-One Exam Guide by Shon Harris
4- Cybrary – CISSP Training by Kelly Handerhan https://lnkd.in/d4zrAkJz
5- Oreilly – CISSP Training by Sari Greene https://lnkd.in/dANS-hVc.
6- CISSP bundles by Thor Pedersen https://lnkd.in/d2tpqaJk
7- CISSP MindMaps YouTube Playlist from Destination Certification https://lnkd.in/deJM44xX

Module 6: Testing

Emad M. Ab
Technical Lead
CCIE#58413 |
ISO27001 LA |

Published Jul

Introduction المقدمة

Security assessment and testing are critical components of an organization's security management process. These activities help identify vulnerabilities, ensure compliance with regulations, and improve overall security posture. This module covers various strategies, techniques, and processes involved in security assessment

تغطي هذه الوحدة استراتيجيات وتقنيات وعمليات متنوعة تتعلق بتقييم الأمان والاختبار.

Module Brief

1. Design and Validate Assessment, Test, and Audit Strategies / تصميم والتحقق من استراتيجيات التقييم والاختبار والتدقيق

This part involves planning and verifying methods to evaluate the effectiveness of security measures, ensuring they meet organizational goals and regulatory requirements. تتضمن هذه الجزء تخطيط والتحقق من طرق تقييم فعالية التدابير الأمنية لضمان توافقها مع أهداف المؤسسة والمتطلبات التنظيمية

2. Conduct Security Controls Testing / إجراء اختبارات ضوابط الأمان

This section covers various testing techniques to evaluate the effectiveness of security controls and identify vulnerabilities. يغطي هذا القسم تقنيات الاختبار المختلفة لتقييم فعالية ضوابط الأمان وتحديد الثغرات

3. Collect Security Process Data / جمع بيانات العمليات الأمنية

This part involves gathering technical and administrative data related to security processes to ensure they are functioning correctly and efficiently. يشمل هذا الجزء جمع البيانات الفنية والإدارية المتعلقة بالعمليات الأمنية لضمان عملها بشكل صحيح وفعال

4. Analyze Test Output and Generate Report / تحليل نتائج الاختبار وإنشاء التقرير

This section focuses on analyzing the results of security tests and generating reports that provide insights and recommendations for improvement. يركز هذا القسم على تحليل نتائج الاختبارات الأمنية وإنشاء تقارير توفر رؤى وتوصيات للتحسين

5. Conduct or Facilitate Security Audits / إجراء أو تسهيل التدقيقات الأمنية

This part involves conducting internal, external, and third-party audits to evaluate the organization’s security posture and ensure compliance with standards. يشمل هذا الجزء إجراء التدقيقات الداخلية والخارجية وللأطراف الثالثة لتقييم الوضع الأمني للمؤسسة وضمان الامتثال للمعايير

6. Security Assessment and Testing Techniques / تقنيات التقييم والاختبار الأمني

This section covers various techniques and methodologies used in security assessments and testing, including validation, verification, and rigorous testing methods. يغطي هذا القسم التقنيات والمنهجيات المختلفة المستخدمة في التقييمات والاختبارات الأمنية بما في ذلك التحقق والتحقق والأساليب الصارمة للاختبار

---

1. Design and Validate Assessment, Test, and Audit Strategies تصميم والتحقق من استراتيجيات التقييم والاختبار والتدقيق

Designing and validating assessment, test, and audit strategies involves planning and verifying methods to evaluate security measures. يشمل تصميم والتحقق من استراتيجيات التقييم والاختبار والتدقيق تخطيط وتحقق من طرق تقييم التدابير الأمنية

Purpose: To ensure that security measures are effective and align with organizational goals and regulatory requirements. لضمان أن التدابير الأمنية فعالة ومتوافقة مع أهداف المؤسسة والمتطلبات التنظيمية

1.1. Internal (e.g., within organization control) / داخلي

Internal assessments, tests, and audits conducted within the organization's control to evaluate its security posture. التقييمات والاختبارات والتدقيقات الداخلية تُجرى داخل سيطرة المنظمة لتقييم وضعها الأمني.

Examples: Internal security audits, self-assessments, internal penetration testing. تدقيقات الأمان الداخلية التقييمات الذاتية اختبار الاختراق الداخلي.

Use Case: An organization conducts an internal audit to assess compliance with its security policies and identify areas for improvement. تقوم المؤسسة بإجراء تدقيق داخلي لتقييم الامتثال لسياساتها الأمنية وتحديد مجالات التحسين.

1.2. External (e.g., outside organization control) / خارجي

Assessments, tests, and audits conducted by external entities to evaluate the organization's security posture. التقييمات والاختبارات والتدقيقات التي تُجرى بواسطة جهات خارجية لتقييم الوضع الأمني للمنظمة.

Examples: External security audits, third-party penetration testing, regulatory compliance assessments. تدقيقات الأمان الخارجية اختبار الاختراق من قبل طرف ثالث تقييمات الامتثال التنظيمي.

Use Case: A company hires an external auditor to assess its compliance with industry regulations and identify vulnerabilities. تقوم شركة بتوظيف مدقق خارجي لتقييم امتثالها للوائح الصناعة وتحديد الثغرات.

1.3. Third-party (e.g., outside of enterprise control) / طرف ثالث

Assessments, tests, and audits conducted by third-party vendors or partners to ensure compliance with security requirements. التقييمات والاختبارات والتدقيقات التي تُجرى بواسطة بائعين أو شركاء من طرف ثالث لضمان الامتثال لمتطلبات الأمان.

Examples: Vendor security assessments, third-party risk assessments, supply chain security audits. تقييمات أمان البائعين تقييمات مخاطر الطرف الثالث تدقيقات أمان سلسلة التوريد.

Use Case: An organization requires its vendors to undergo regular security assessments to ensure they meet the company's security standards. تتطلب المؤسسة من بائعيها إجراء تقييمات أمان منتظمة لضمان التزامهم بمعايير الأمان الخاصة بالشركة.

1.4. Location / الموقع

Assessments, tests, and audits can be conducted based on the location of the assets, such as on-premise, cloud, or hybrid environments. يمكن إجراء التقييمات والاختبارات والتدقيقات بناءً على موقع الأصول مثل في المقر أو السحابة أو البيئات الهجينة

- on-premise
- cloud
- hybrid

1.4.1. On-premise / في الموقع

Assessments, tests, and audits conducted within the physical premises of the organization. التقييمات والاختبارات والتدقيقات التي تُجرى داخل الموقع الفعلي للمؤسسة.

Examples: On-site security audits, physical security assessments, facility inspections. تدقيقات الأمان في الموقع تقييمات الأمان المادي تفتيش المنشآت.

Use Case: A company conducts an on-premise security assessment to evaluate the physical security controls and identify vulnerabilities. تقوم شركة بإجراء تقييم أمان في الموقع لتقييم ضوابط الأمان المادي وتحديد الثغرات.

1.4.2. Cloud / سحابي

Assessments, tests, and audits conducted on cloud-based environments to ensure their security. التقييمات والاختبارات والتدقيقات التي تُجرى على البيئات السحابية لضمان أمانها.

Examples: Cloud security audits, cloud penetration testing, compliance assessments for cloud services. تدقيقات الأمان السحابية اختبار الاختراق السحابي تقييمات الامتثال لخدمات السحابة.

Use Case: An organization conducts a cloud security audit to ensure its cloud infrastructure complies with security standards. تقوم المؤسسة بإجراء تدقيق أمان سحابي لضمان امتثال بنيتها التحتية السحابية لمعايير الأمان.

1.4.3. Hybrid / هجين

Assessments, tests, and audits conducted on hybrid environments, combining on-premise and cloud-based systems. التقييمات والاختبارات والتدقيقات التي تُجرى على البيئات الهجينة التي تجمع بين الأنظمة في الموقع والسحابية.

Examples: Hybrid environment security audits, integrated security assessments, compliance checks for hybrid deployments. تدقيقات الأمان للبيئات الهجينة تقييمات الأمان المتكاملة فحوصات الامتثال للنشرات الهجينة.

Use Case: A company conducts a hybrid security assessment to evaluate the security of its combined on-premise and cloud-based systems. تقوم شركة بإجراء تقييم أمان هجين لتقييم أمان أنظمتها المدمجة في الموقع والسحابية.

Multiple Choice Questions:

1. What is the primary purpose of internal assessments and audits?

a. To evaluate security controls of external vendors

b. To ensure compliance with internal policies and identify areas for improvement

c. To assess the security of cloud services

d. To evaluate the security posture of third-party partners

2. What is the purpose of engaging external auditors?

a. To ensure data protection in hybrid environments

b. To evaluate the organization's security posture and ensure adherence to industry standards

c. To manage internal security controls

d. To oversee the on-premise security infrastructure

3. What is the focus of third-party assessments?

a. Evaluating internal security controls

b. Assessing security measures of vendors and partners

c. Managing on-premise security infrastructure

d. Monitoring cloud-based services

4. Why are on-premise assessments important?

a. To evaluate security measures of cloud services

b. To ensure the security of physical and network infrastructure within the organization's premises

c. To assess third-party security controls

d. To manage hybrid environments

5. What is a key consideration for conducting cloud assessments?

a. Managing internal audits

b. Evaluating security controls of cloud service providers hosting critical business applications

c. Overseeing physical security measures

d. Monitoring on-premise network infrastructure

Answers and Explanation:

1. b. To ensure compliance with internal policies and identify areas for improvement

Explanation: Internal assessments and audits are conducted to ensure compliance with internal policies and identify areas for improvement.يتم إجراء التقييمات والتدقيقات الداخلية لضمان الامتثال للسياسات الداخلية وتحديد مجالات التحسين

2. b. To evaluate the organization's security posture and ensure adherence to industry standards

Explanation: External auditors provide an unbiased evaluation of the organization's security posture and ensure adherence to industry standards.يوفر المراجعون الخارجيون تقييمًا غير متحيز لوضع الأمان الخاص بالمؤسسة ويضمنون الالتزام بمعايير الصناعة

3. b. Assessing security measures of vendors and partners

Explanation: Third-party assessments focus on evaluating the security measures of vendors and partners to ensure compliance with organizational standards.تركز تقييمات الأطراف الثالثة على تقييم التدابير الأمنية للبائعين والشركاء لضمان الامتثال لمعايير المؤسسة

4. b. To ensure the security of physical and network infrastructure within the organization's premises

Explanation: On-premise assessments ensure the security of physical and network infrastructure within the organization's premises.تضمن التقييمات في المقر أمان البنية التحتية المادية والشبكية داخل مقر المؤسسة

5. b. Evaluating security controls of cloud service providers hosting critical business applications

Explanation: Cloud assessments evaluate the security controls of cloud service providers hosting critical business applications to ensure data protection and compliance.تقوم التقييمات السحابية بتقييم ضوابط الأمان لمزودي خدمة السحابة الذين يستضيفون تطبيقات الأعمال الحيوية لضمان حماية البيانات والامتثال

---

2. Conduct Security Controls Testing إجراء اختبارات ضوابط الأمان

Security controls testing involves evaluating the effectiveness of security measures through various testing techniques. يشمل اختبار ضوابط الأمان تقييم فعالية التدابير الأمنية من خلال تقنيات اختبار مختلفة

Purpose: To identify vulnerabilities and weaknesses in security measures and ensure they provide adequate protection. لتحديد الثغرات والضعف في التدابير الأمنية وضمان توفيرها للحماية الكافية

2.1. Vulnerability Assessment / تقييم الثغرات الأمنية

Vulnerability assessment is the process of identifying, quantifying, and prioritizing vulnerabilities in a system. تقييم الثغرات الأمنية هو عملية تحديد وتكميم وترتيب الثغرات في النظام

To identify security weaknesses that could be exploited by attackers and prioritize them for remediation. لتحديد نقاط الضعف الأمنية التي يمكن أن يستغلها المهاجمون وترتيبها حسب الأولوية للإصلاح

Testing Techniques / تقنيات الاختبار

A- Perspective / منظور (Internal , External)

B- Approach / نهج (Blind, Double-blind)

C- Knowledge / معرفة (Zero (black), Partial (gray), Full (white))

D- Types of Scans / أنواع المسح (Credentialed / Authenticated, Undifferentiated / Unauthenticated)

E- Banner Grabbing & Fingerprinting / التقاط البانر والتعرف على البصمة

F- Interpreting & Understanding Results / تفسير وفهم النتائج

G- SCAP

H- False Positive vs. False Negative / الإيجابيات الكاذبة مقابل السلبيات الكاذبة

2.1.1. Perspective منظور

Evaluating the system from different perspectives to identify vulnerabilities. تقييم النظام من زوايا مختلفة لتحديد الثغرات.

• **Internal / داخلي** Testing from within the organization's network.

Examples: Internal scans to identify vulnerabilities that may not be visible from outside.

• **External / خارجي** Testing from outside the organization's network.

Examples: External scans to identify vulnerabilities exposed to the internet.

2.1.2. Approach نهج

The level of awareness of the assessment team and system administrators about the test being conducted. مستوى وعي فريق التقييم ومسؤولي النظام حول الاختبار الجاري تنفيذه

• **Blind / أعمى** The tester has no prior knowledge of the target.

Examples: Simulating an external attacker with no insider information.

• **Double-blind / أعمى مزدوج** Neither the tester nor the defenders have prior knowledge of the test.

Examples: Simulating unexpected attacks to test real-time responses.

2.1.3. Knowledge معرفة

The amount of information available to the assessment team before conducting the test. مقدار المعلومات المتاحة لفريق التقييم قبل إجراء الاختبار.

• **Zero (black) / (أسود) لا شيء** The tester has no knowledge of the target.

Examples: Black-box testing to simulate an external attack with no insider information.

• **Partial (gray) / (رمادي) جزئي** The tester has limited knowledge of the target.

Examples: Gray-box testing to simulate an attack with some insider information.

• **Full (white) / (أبيض) كامل** The tester has complete knowledge of the target.

Examples: White-box testing to identify all possible vulnerabilities.

2.1.4. Types of Scans أنواع الفحوصات

The type of access the assessment team has during the scan. نوع الوصول الذي يمتلكه فريق التقييم أثناء الفحص.

• **Credentialed / Authenticated / مصادق** Scans conducted with access credentials.

Examples: Scanning with admin privileges to identify deeper vulnerabilities.

• **Undifferentiated / Unauthenticated / غير مصادق** Scans conducted without access credentials.

Examples: External scans to identify surface vulnerabilities.

2.1.5. Banner Grabbing & Fingerprinting التقاط البانر وبصمة الإصبع

Techniques used to gather information about systems and services running on a network. تقنيات تُستخدم لجمع المعلومات حول الأنظمة والخدمات التي تعمل على الشبكة.

Examples: Banner grabbing using tools like Nmap, fingerprinting operating systems. التقاط البانر باستخدام أدوات مثل بصمة الأنظمة التشغيلية.

2.1.6. Interpreting & Understanding Results تفسير وفهم النتائج

Analyzing and understanding the results of vulnerability assessments to determine the severity and potential impact of identified vulnerabilities. تحليل وفهم نتائج تقييمات الثغرات لتحديد شدة وتأثير الثغرات المحددة.

• CVE / CVE Definition: Common Vulnerabilities and Exposures - a list of publicly known security vulnerabilities.

• CVSS / CVSS Definition: Common Vulnerability Scoring System - a framework for rating the severity of vulnerabilities.

Examples: Reviewing CVE entries, using CVSS scores to prioritize remediation efforts. مراجعة الإدخالات واستخدام الدرجات لتحديد أولويات جهود الإصلاح.

2.1.7. SCAP بروتوكول الأمان المؤتمت

The Security Content Automation Protocol (SCAP) is a suite of specifications for standardizing the format and nomenclature by which security software communicates information about software flaws and security configurations. بروتوكول الأمان المؤتمت

هو مجموعة من المواصفات لتوحيد الشكل والتسمية التي تتواصل بها برامج الأمان المعلومات حول العيوب الأمنية وتكوينات الأمان.

Examples: Using SCAP tools to automate vulnerability management, policy compliance, and security measurement. استخدام الأدوات لأتمته إدارة الثغرات والامتثال للسياسات وقياس الأمان

2.1.8. False Positive vs. False Negative إيجابية كاذبة مقابل سلبية كاذبة

False positives occur when a vulnerability scanner incorrectly identifies a vulnerability that does not exist.

False negatives occur when a vulnerability scanner fails to identify an existing vulnerability. تحدث الإيجابيات الكاذبة عندما يحدد ماسح الثغرات الأمنية ثغرة بشكل غير صحيح وهي غير موجودة تحدث السلبيات الكاذبة عندما يفشل ماسح الثغرات الأمنية في تحديد ثغرة موجودة بالفعل.

Examples: A vulnerability scanner flags a non-existent issue as a vulnerability (false positive). A scanner misses a real vulnerability (false negative). يحدد ماسح الثغرات الأمنية مشكلة غير موجودة على أنها ثغرة (إيجابية كاذبة). يفوت ماسح الثغرات ثغرة حقيقية (سلبية كاذبة).

2.2. Penetration Testing / اختبار الاختراق

Penetration testing involves simulating cyber attacks on a system, network, or application to identify vulnerabilities that could be exploited by attackers. يتضمن اختبار الاختراق محاكاة الهجمات السيبرانية على نظام أو شبكة أو تطبيق لتحديد الثغرات التي يمكن استغلالها من قبل المهاجمين.

Examples: Conducting red team exercises to simulate real-world attacks, blue team exercises to defend against attacks, and purple team exercises to enhance collaboration between offense and defense teams. إجراء تمارين الفريق الأحمر لمحاكاة الهجمات الحقيقية تمارين الفريق الأزرق للدفاع ضد الهجمات تمارين الفريق الأرجواني لتعزيز التعاون بين فرق الهجوم والدفاع.

2.2.1. Process / عملية

The steps involved in conducting a penetration test, including planning, reconnaissance, exploitation, and reporting. الخطوات المتبعة في إجراء اختبار الاختراق بما في ذلك التخطيط الاستطلاع الاستغلال والتقرير.

Examples: Planning the scope of the test, gathering information about the target, exploiting vulnerabilities, and documenting findings. تخطيط نطاق الاختبار جمع المعلومات حول الهدف استغلال الثغرات وتوثيق النتائج.

2.2.2. Reconnaissance / استطلاع

The phase of penetration testing where information about the target is gathered, including network details, software versions, and potential vulnerabilities. مرحلة من اختبار الاختراق يتم فيها جمع المعلومات حول الهدف بما في ذلك تفاصيل الشبكة إصدارات البرمجيات والثغرات المحتملة.

Examples: Using tools like Nmap for network scanning, Shodan for discovering internet-facing devices, and searching for public data leaks. استخدام أدوات مثل Nmap لاكتشاف الأجهزة المتصلة بالإنترنت والبحث عن تسريبات البيانات Shodan لفحص الشبكة العامة.

2.2.3. Enumeration / تعداد

The process of extracting detailed information about the target system, such as user accounts, network shares, and open ports. عملية استخراج معلومات مفصلة حول نظام الهدف مثل حسابات المستخدمين المشاركات الشبكية والمنافذ المفتوحة.

Examples: Using tools like Netcat for banner grabbing, Enum4linux for Windows enumeration, and SNMPwalk for SNMP enumeration.

2.2.4. Vulnerability Analysis / تحليل الثغرات

The process of identifying, classifying, and prioritizing vulnerabilities in the target system. عملية تحديد تصنيف وتحديد أولويات الثغرات في نظام الهدف.

Examples: Using vulnerability scanning tools like Nessus, OpenVAS, and Qualys to identify potential vulnerabilities. استخدام أدوات فحص الثغرات مثل OpenVASو Nessus وQualys لتحديد الثغرات المحتملة.

2.2.5. Execution / تنفيذ

The phase of penetration testing where identified vulnerabilities are exploited to gain unauthorized access or perform malicious activities. مرحلة من اختبار الاختراق يتم فيها استغلال الثغرات المحددة للوصول غير المصرح به أو تنفيذ أنشطة ضارة.

Examples: Using exploit frameworks like Metasploit to exploit identified vulnerabilities, executing payloads, and maintaining persistence. استخدام أطر العمل مثل Metasploit لاستغلال الثغرات المحددة تنفيذ الحمولات والحفاظ على الاستمرارية.

2.2.6. Document Findings / توثيق النتائج

The process of recording and reporting the findings of the penetration test, including exploited vulnerabilities, attack paths, and remediation recommendations. عملية تسجيل وتوثيق نتائج اختبار الاختراق بما في ذلك الثغرات المستغلة ومسارات الهجوم وتوصيات الإصلاح.

Examples: Creating a detailed report that outlines the findings, provides evidence of exploitation, and suggests mitigation strategies. إنشاء تقرير مفصل يحدد النتائج ويقدم دليلًا على الاستغلال ويقترح استراتيجيات التخفيف.

2.3. Log Reviews / مراجعات السجلات

The process of examining log files from various systems and applications to detect security incidents, policy violations, and operational issues. عملية فحص ملفات السجلات من الأنظمة والتطبيقات المختلفة لاكتشاف الحوادث الأمنية وانتهاكات السياسات والمشكلات التشغيلية.

Examples: Reviewing logs from firewalls, intrusion detection systems (IDS), and application servers to identify suspicious activities. مراجعة السجلات من الجدران النارية وأنظمة اكتشاف التسلل وخوادم التطبيقات لتحديد الأنشطة المشبوهة.

Use Case: An organization performs regular log reviews to monitor for signs of security breaches and ensure compliance with security policies. تقوم المؤسسة بإجراء مراجعات دورية للسجلات لمراقبة علامات الاختراقات الأمنية وضمان الامتثال لسياسات الأمان.

2.3.1. Monitor for Errors, Modification and Breaches / مراقبة لـ

A. Errors الأخطاء

Reviewing logs to identify and address errors that may indicate security vulnerabilities or system malfunctions. مراجعة السجلات لتحديد ومعالجة الأخطاء التي قد تشير إلى ثغرات أمنية أو أعطال في النظام.

Examples: Identifying frequent login failures, application errors, and configuration issues in log files. تحديد حالات الفشل المتكررة في تسجيل الدخول وأخطاء التطبيقات ومشكلات التكوين في ملفات السجلات.

B. Modification التعديلات

Detecting unauthorized changes to system configurations, files, or applications through log analysis. اكتشاف التغييرات غير المصرح بها في تكوينات النظام أو الملفات أو التطبيقات من خلال تحليل السجلات.

Examples: Monitoring logs for changes to critical system files, configuration settings, and user privileges. مراقبة السجلات بحثًا عن التغييرات في ملفات النظام الحيوية وإعدادات التكوين وامتيازات المستخدم.

C. Breaches الاختراقات

Identifying signs of security breaches, such as unauthorized access attempts, malware infections, and data exfiltration, through log analysis. تحديد علامات الاختراقات الأمنية مثل محاولات الوصول غير المصرح بها وإصابات البرمجيات الخبيثة وسحب البيانات من خلال تحليل السجلات.

Examples: Reviewing logs for suspicious login attempts, unusual network traffic, and indicators of compromise (IOCs). مراجعة السجلات بحثًا عن محاولات تسجيل الدخول المشبوهة وحركة المرور الشبكية غير العادية ومؤشرات الاختراق (IOCs).

2.3.2. Security Information and Event Management (SIEM) / إدارة معلومات وأحداث الأمان (SIEM)

SIEM systems collect, analyze, and correlate security event data from various sources to provide real-time monitoring, threat detection, and incident response. تجمع بيانات أحداث الأمان من مصادر مختلفة لتحليلها وربطها لتوفير مراقبة في الوقت الفعلي واكتشاف التهديدات والاستجابة للحوادث.

Examples: Using SIEM tools like Splunk, IBM QRadar, and ArcSight to aggregate and analyze log data from firewalls, IDS/IPS, and servers. استخدام أدوات إدارة معلومات وأحداث الأمان لتجميع وتحليل بيانات السجلات من الجدران النارية والخوادم.

It is include Multiple the Following Steps: **Generation, Transmission, Collection / Aggregation, Normalization, Analysis, Retention and Disposal**

A. Generation / الانشاء

The process of creating log files from various systems and devices for security monitoring and analysis. عملية إنشاء ملفات السجلات من الأنظمة والأجهزة المختلفة

لمراقبة الأمان والتحليل.

Examples: Generating logs from firewalls, IDS/IPS, application servers, and network devices. إنشاء سجلات من الجدران النارية وخوادم التطبيقات والأجهزة الشبكية.

In Generation Process we should consider the Following Points: Limiting Log File Size and Time Stamps

1. Limiting Log File Size / تحديد حجم ملف السجل Implementing measures to control the size of log files to prevent excessive storage use and ensure efficient log management. تنفيذ تدابير للتحكم في حجم ملفات السجلات لمنع الاستخدام المفرط للتخزين وضمان إدارة فعالة للسجلات.

2. Time Stamps / الطوابع الزمنية Recording the exact time of each log entry to ensure accurate time correlation and sequence of events. تسجيل الوقت الدقيق لكل إدخال سجل لضمان الترابط الزمني الدقيق وتسلسل الأحداث.

B. Transmission / الإرسال

The process of securely transmitting log data from various systems to a centralized logging infrastructure. عملية نقل بيانات السجلات بأمان من الأنظمة المختلفة إلى بنية تحتية لتسجيل السجلات مركزية.

Examples: Using encrypted channels to transmit log data to a central SIEM system. استخدام قنوات مشفرة لنقل بيانات السجلات إلى نظام مركزي.

C. Collection / Aggregation / التجميع / الجمع

The process of collecting and consolidating log data from multiple sources into a centralized repository for analysis. عملية جمع وتوحيد بيانات السجلات من مصادر متعددة في مستودع مركزي للتحليل.

Examples: Aggregating log data from firewalls, IDS/IPS, servers, and applications into a central SIEM system. تجميع بيانات السجلات من الجدران النارية والخوادم والتطبيقات في نظام مركزي.

D. Normalization / التطبيع

The process of standardizing log data from different sources into a common format

for easier analysis and correlation. عملية توحيد بيانات السجلات من مصادر مختلفة إلى تنسيق مشترك لتسهيل التحليل والترابط.

Examples: Converting log entries from different systems into a standardized format using a SIEM tool. تحويل إدخالات السجلات من الأنظمة المختلفة إلى تنسيق موحد.

E. Analysis / التحليل

The process of examining log data to identify patterns, anomalies, and indicators of security incidents. عملية فحص بيانات السجلات لتحديد الأنماط والشذوذ ومؤشرات الحوادث الأمنية.

Examples: Using SIEM tools to analyze log data for signs of unauthorized access, malware activity, and policy violations. استخدام أدوات لتحليل بيانات السجلات بحثًا عن علامات الوصول غير المصرح به ونشاط البرمجيات الخبيثة وانتهاكات السياسات.

F. Retention / الاحتفاظ

The practice of retaining log data for a specified period to meet regulatory requirements, facilitate investigations, and support forensic analysis. ممارسة الاحتفاظ ببيانات السجلات لفترة محددة لتلبية المتطلبات التنظيمية وتسهيل التحقيقات ودعم التحليل الجنائي.

Examples: Setting log retention policies to keep log data for one year or longer as required by regulations. تحديد سياسات الاحتفاظ بالسجلات للاحتفاظ ببيانات السجلات لمدة سنة أو أكثر حسب المتطلبات التنظيمية.

G. Disposal / التخلص

The process of securely deleting log data after it is no longer needed, ensuring that sensitive information is not recoverable. عملية حذف بيانات السجلات بأمان بعد عدم الحاجة إليها لضمان عدم استعادة المعلومات الحساسة.

Examples: Using secure deletion methods to erase log files from storage devices. استخدام طرق الحذف الآمن لمسح ملفات السجلات من أجهزة التخزين.

2.3.3. Continuous Monitoring / المراقبة المستمرة

Continuous monitoring is the ongoing process of observing and evaluating the security posture of an organization's information systems to detect and respond to security threats in real-time. المراقبة المستمرة هي عملية مستمرة لمراقبة وتقييم وضع

الأمان لأنظمة معلومات المؤسسة لاكتشاف التهديدات الأمنية والاستجابة لها في الوقت الفعلي.

Purpose: To ensure the integrity, confidentiality, and availability of systems by detecting and responding to security incidents promptly. لضمان النزاهة والسرية وتوافر الأنظمة من خلال اكتشاف الحوادث الأمنية والاستجابة لها على الفور.

2.3.3.1. Continuous Monitoring Components / المكونات: Data Collection, Data Analysis, Alerting and Reporting,

1. Data Collection / جمع البيانات Gathering information from various sources, such as network traffic, system logs, and application logs, for analysis. جمع المعلومات من مصادر مختلفة مثل حركة مرور الشبكة سجلات النظام وسجلات التطبيقات للتحليل.

2. Data Analysis / تحليل البيانات Examining collected data to identify patterns, anomalies, and potential security incidents. فحص البيانات المجمعة لتحديد الأنماط والشذوذ والحوادث الأمنية المحتملة.

3. Alerting and Reporting / التنبيه والإبلاغ Setting up alerts for suspicious activities and generating regular and on-demand reports. إعداد التنبيهات للأنشطة المشبوهة وإنشاء تقارير دورية وعند الطلب.

_____

2.3.3.2. Technologies and Tools / التقنيات والأدوات : SIEM, IDS/IPS and EDR

1. Security Information and Event Management (SIEM) / إدارة معلومات وأحداث الأمان SIEM systems collect, analyze, and correlate security event data from various sources to provide real-time monitoring, threat detection, and incident response. تجمع أنظمة بيانات أحداث الأمان من مصادر مختلفة لتحليلها وربطها لتوفير مراقبة في الوقت الفعلي واكتشاف التهديدات والاستجابة للحوادث.

2. Intrusion Detection and Prevention Systems (IDS/IPS) / أنظمة اكتشاف ومنع التسلل IDS/IPS systems monitor network traffic for suspicious activity and take action to prevent potential threats. تراقب أنظمة حركة المرور الشبكية بحثًا عن الأنشطة المشبوهة وتتخذ إجراءات لمنع التهديدات المحتملة

3. Endpoint Detection and Response (EDR) / اكتشاف نقاط النهاية والاستجابة EDR solutions provide continuous monitoring and response capabilities for endpoint devices to detect and mitigate security threats. تقدم حلول مراقبة مستمرة وقدرات استجابة لأجهزة نقاط النهاية لاكتشاف التهديدات الأمنية وتخفيفها.

2.3.3.3. Best Practices / أفضل الممارسات

1. Regular Updates and Patching / التحديثات والتصحيحات الدورية Keeping monitoring tools and systems up to date with the latest security patches and updates to protect against known vulnerabilities. الحفاظ على أدوات وأنظمة المراقبة محدثة بأحدث التصحيحات والتحديثات الأمنية للحماية من الثغرات المعروفة.

2. Training and Awareness / التدريب والتوعية Providing training and raising awareness among staff about the importance of continuous monitoring and how to use monitoring tools effectively. توفير التدريب ورفع الوعي بين الموظفين حول أهمية المراقبة المستمرة وكيفية استخدام أدوات المراقبة بشكل فعال.

3. Collaboration and Communication / التعاون والتواصل Ensuring effective communication and collaboration between IT, security teams, and other stakeholders to enhance the monitoring process. ضمان التواصل والتعاون الفعال بين فرق تكنولوجيا المعلومات والأمان وأصحاب المصلحة الآخرين لتعزيز عملية المراقبة.

2.3.3.4. Challenges and Solutions / التحديات والحلول

1. Data Overload / التحميل الزائد للبيانات Managing the large volumes of data generated by continuous monitoring tools to avoid being overwhelmed and ensure meaningful analysis. إدارة كميات كبيرة من البيانات التي تولدها أدوات المراقبة المستمرة لتجنب التحميل الزائد وضمان التحليل المفيد.

2. False Positives and Negatives / الإيجابيات الكاذبة والسلبيات الكاذبة Addressing the challenges of false positives (incorrectly identified threats) and false negatives (missed threats) in the monitoring process. معالجة تحديات الإيجابيات الكاذبة (التهديدات التي تم تحديدها بشكل غير صحيح) والسلبيات الكاذبة (التهديدات التي لم يتم اكتشافها) في عملية المراقبة.

3. Resource Constraints / قيود الموارد Allocating sufficient resources, including personnel and technology, to effectively implement and maintain continuous monitoring. تخصيص الموارد الكافية بما في ذلك الأفراد والتكنولوجيا لتنفيذ وصيانة المراقبة المستمرة بشكل فعال.

2.3.3.5. Metrics and Key Performance Indicators (KPIs) / مقاييس ومؤشرات الأداء

الرئيسية

1. Incident Detection Time / وقت اكتشاف الحوادث : Measuring the time taken to detect security incidents from the moment they occur. قياس الوقت المستغرق لاكتشاف الحوادث الأمنية من لحظة حدوثها

2. Response Time / وقت الاستجابة : Measuring the time taken to respond to detected security incidents. قياس الوقت المستغرق للاستجابة للحوادث الأمنية المكتشفة.

3. System Uptime and Availability / وقت التشغيل وتوافر النظام : Monitoring the availability and uptime of critical systems to ensure they are operational and accessible. مراقبة توافر ووقت تشغيل الأنظمة الحيوية لضمان تشغيلها وإمكانية الوصول إليها.

2.4. Synthetic Transactions - Benchmarks / معايير الأداء / المعاملات الاصطناعية

Synthetic transactions involve simulating user activities to test the performance and availability of applications and systems. تشمل المعاملات الاصطناعية محاكاة أنشطة المستخدم لاختبار أداء وتوافر التطبيقات والأنظمة.

Purpose: To proactively identify performance issues and ensure that systems meet predefined benchmarks and service level agreements (SLAs). للتعرف بشكل استباقي على مشاكل الأداء وضمان أن الأنظمة تفي بالمعايير المحددة مسبقًا واتفاقيات مستوى الخدمة

2.4.1. Types of Synthetic Transactions / أنواع المعاملات الاصطناعية

A. User Simulation / محاكاة المستخدم Simulating typical user interactions with applications to test end-to-end user experiences. محاكاة تفاعلات المستخدم النموذجية مع التطبيقات لاختبار تجارب المستخدم من البداية إلى النهاية.

Examples: Simulating login processes, browsing activities, and form submissions. محاكاة عمليات تسجيل الدخول وأنشطة التصفح وإرسال النماذج.

B. API Testing : Sending requests to APIs to check response times, correctness, and performance under various conditions. إرسال طلبات إلى واجهات برمجة التطبيقات للتحقق من أوقات الاستجابة والصحة والأداء تحت ظروف مختلفة.

Examples: Testing API endpoints for response time, data integrity, and error handling. اختبار نقاط النهاية لـ لأوقات الاستجابة وسلامة البيانات ومعالجة الأخطاء.

C. Database Transactions / معاملات قاعدة البيانات: Simulating database queries and updates to monitor database performance and response times. محاكاة استعلامات وتحديثات قاعدة البيانات لمراقبة أداء قاعدة البيانات وأوقات الاستجابة.

Examples: Simulating read and write operations on a database to measure performance. محاكاة عمليات القراءة والكتابة على قاعدة البيانات لقياس الأداء.

2.4.2. Implementation Strategies / استراتيجيات التنفيذ

A. Selecting Scenarios / اختيار السيناريوهات

Identifying critical user journeys and interactions to define key performance indicators (KPIs) for each scenario. تحديد الرحلات والتفاعلات الحرجة للمستخدم لتحديد مؤشرات الأداء الرئيسية لكل سيناريو.

Examples: Selecting scenarios that represent typical user activities, such as login, checkout, and data entry. اختيار السيناريوهات التي تمثل أنشطة المستخدم النموذجية مثل تسجيل الدخول وإتمام الدفع وإدخال البيانات.

B. Tool Selection / اختيار الأدوات

Evaluating and selecting tools for creating and executing synthetic transactions. تقييم واختيار الأدوات لإنشاء وتنفيذ المعاملات الاصطناعية.

Examples: Using tools like Apache JMeter, Selenium, and LoadRunner to create and execute synthetic transactions. استخدام الأدوات مثل لإنشاء وتنفيذ المعاملات الاصطناعية

C. Scheduling and Frequency / الجدولة والتكرار

Determining the frequency and schedule for executing synthetic transactions to ensure consistent monitoring. تحديد تكرار وجدول تنفيذ المعاملات الاصطناعية لضمان المراقبة المستمرة.

Examples: Scheduling synthetic transactions to run every hour, daily, or weekly based on the application's criticality. جدولة المعاملات الاصطناعية لتشغيلها كل ساعة أو يوميًا أو أسبوعيًا بناءً على أهمية التطبيق.

2.4.3. Metrics and Benchmarks / المقاييس والمعايير

A. Response Time / وقت الاستجابة

Measuring the time taken to complete a synthetic transaction from start to finish. قياس الوقت المستغرق لإكمال معاملة اصطناعية من البداية إلى النهاية.

Examples: Tracking the response time for login, checkout, and data retrieval operations. تتبع وقت الاستجابة لعمليات تسجيل الدخول وإتمام الدفع واسترجاع البيانات

B. Availability / التوافر

Monitoring the availability of applications and systems to ensure they are operational and accessible. مراقبة توافر التطبيقات والأنظمة لضمان تشغيلها وإمكانية الوصول إليها.

Examples: Tracking the availability of web services, APIs, and databases. تتبع توافر خدمات الويب وواجهات برمجة التطبيقات وقواعد البيانات.

C. Error Rates / معدلات الأخطاء

Tracking the number of errors encountered during synthetic transactions to identify and address issues. تتبع عدد الأخطاء التي تم مواجهتها أثناء المعاملات الاصطناعية لتحديد ومعالجة المشكلات.

Examples: Monitoring error rates for failed login attempts, data retrieval errors, and transaction failures. مراقبة معدلات الأخطاء لمحاولات تسجيل الدخول الفاشلة وأخطاء استرجاع البيانات وإخفاقات المعاملات.

2.4.4. Challenges and Solutions / التحديات والحلول

A. Script Maintenance / صيانة النصوص

Managing and updating synthetic transaction scripts as applications evolve and change. إدارة وتحديث نصوص المعاملات الاصطناعية مع تطور وتغيير التطبيقات.

Examples: Automating script generation and updates to keep pace with application changes. أتمتة إنشاء النصوص والتحديثات لمواكبة تغييرات التطبيقات.

B. False Positives/Negatives / الإيجابيات الكاذبة / السلبيات الكاذبة

Reducing the occurrence of false positives (incorrect alerts) and false negatives (missed issues) in synthetic transaction testing. تقليل حدوث الإيجابيات الكاذبة (تنبيهات

غير صحيحة) والسلبيات الكاذبة (مشكلات مفقودة) في اختبار المعاملات الاصطناعية.

Examples: Fine-tuning test scenarios to minimize false positives and enhance detection capabilities to reduce false negatives. ضبط سيناريوهات الاختبار لتقليل الإيجابيات الكاذبة وتعزيز قدرات الاكتشاف لتقليل السلبيات الكاذبة.

C. Resource Utilization / استخدام الموارد

Ensuring that synthetic transactions do not consume excessive resources or impact system performance. ضمان أن المعاملات الاصطناعية لا تستهلك موارد مفرطة أو تؤثر على أداء النظام.

Examples: Balancing the frequency and depth of synthetic transaction tests to minimize resource impact. موازنة تكرار وعمق اختبارات المعاملات الاصطناعية لتقليل تأثير الموارد.

Examples: Balancing the frequency and depth of synthetic transaction tests to minimize resource impact. موازنة تكرار وعمق اختبارات المعاملات الاصطناعية لتقليل تأثير الموارد.

2.5 Code Review and Testing / مراجعة واختبار الشيفرة البرمجية

Code review is the process of examining source code to identify defects, ensure code quality, and verify adherence to coding standards. مراجعة الشيفرة البرمجية هي عملية فحص الشيفرة البرمجية لتحديد العيوب وضمان جودة الشيفرة والتحقق من الالتزام بمعايير البرمجة.

Purpose: To improve code quality, detect security vulnerabilities, and ensure maintainability and readability of code. لتحسين جودة الشيفرة واكتشاف الثغرات الأمنية وضمان سهولة الصيانة وقراءة الشيفرة.

2.5.1 Types of Code Review / أنواع مراجعة الشيفرة البرمجية

A. Manual Review / المراجعة اليدوية

Peer reviews and over-the-shoulder reviews where developers manually inspect each other's code. مراجعات الأقران والمراجعات المباشرة حيث يقوم المطورون بفحص الشيفرة لبعضهم البعض يدويًا.

Examples: Developers reviewing code changes in pull requests before merging them into the main codebase. يقوم المطورون بمراجعة تغييرات الشيفرة في طلبات السحب قبل دمجها في الشيفرة الأساسية.

B. Automated Review / المراجعة الآلية

Using static code analysis tools and continuous integration (CI) pipelines to automatically review code for defects and adherence to standards. استخدام أدوات تحليل الشيفرة الثابتة وخطوط التكامل المستمر (CI) لمراجعة الشيفرة تلقائيًا للكشف عن العيوب والالتزام بالمعايير.

Examples: Using tools like SonarQube, Checkmarx, and ESLint to perform automated code reviews. استخدام أدوات مثل SonarQube وCheckmarx وESLint لإجراء مراجعات الشيفرة الآلية.

2.5.2 Implementation Strategies / استراتيجيات التنفيذ

A. Review Process / عملية المراجعة

Defining review criteria, establishing workflows, and setting up protocols for code review. تحديد معايير المراجعة وإنشاء تدفقات العمل وإعداد البروتوكولات لمراجعة الشيفرة.

Examples: Creating a checklist for code reviewers to follow and establishing a review process for every pull request. إنشاء قائمة مراجعة للذين يقومون بمراجعة الشيفرة وإعداد عملية مراجعة لكل طلب سحب.

B. Tool Integration / تكامل الأدوات

Integrating code review tools with version control systems and automating reviews within CI/CD pipelines. دمج أدوات مراجعة الشيفرة مع أنظمة التحكم في الإصدار وأتمتة المراجعات داخل خطوط التكامل المستمر / التسليم المستمر (CI/CD).

Examples: Integrating SonarQube with GitHub to automatically review code changes and provide feedback. دمج SonarQube مع GitHub لمراجعة تغييرات الشيفرة تلقائيًا وتقديم الملاحظات.

C. Reviewer Assignment / تعيين المراجعين

Assigning reviewers based on expertise, availability, and ensuring diverse perspectives through reviewer rotation. تعيين المراجعين بناءً على الخبرة والتوافر وضمان تنوع المنظورات من خلال دوران المراجعين.

Examples: Assigning senior developers to review critical code changes and rotating reviewers to provide diverse feedback. تعيين المطورين الكبار لمراجعة تغييرات الشيفرة الحيوية وتدوير المراجعين لتقديم ملاحظات متنوعة.

Use Case: An organization assigns reviewers to code reviews based on their expertise to ensure thorough and knowledgeable feedback. تقوم المؤسسة بتعيين المراجعين لمراجعات الشيفرة بناءً على خبرتهم لضمان الحصول على ملاحظات شاملة ومطلعة.

2.5.3 Metrics and KPIs / المقاييس ومؤشرات الأداء الرئيسية (KPIs)

A. Defect Density / كثافة العيوب

The number of defects identified per line of code during code reviews. عدد العيوب التي تم تحديدها لكل سطر من الشيفرة أثناء مراجعات الشيفرة.

Examples: Tracking the number of defects found in code reviews to measure code quality. تتبع عدد العيوب التي تم العثور عليها في مراجعات الشيفرة لقياس جودة الشيفرة.

B. Code Coverage / تغطية الشيفرة

The percentage of code covered by automated tests to ensure that all parts of the code are tested. نسبة الشيفرة التي تغطيها الاختبارات الآلية لضمان اختبار جميع أجزاء الشيفرة.

Examples: Using code coverage tools to measure the extent of code tested by unit and integration tests. استخدام أدوات تغطية الشيفرة لقياس مدى الشيفرة التي تم اختبارها بواسطة اختبارات الوحدة والتكامل.

C. Review Time / وقت المراجعة

The average time spent on reviewing code to ensure timely feedback and continuous development. متوسط الوقت المستغرق في مراجعة الشيفرة لضمان الحصول على الملاحظات في الوقت المناسب واستمرار التطوير.

Examples: Tracking the time reviewers spend on code reviews to optimize the review process. تتبع الوقت الذي يقضيه المراجعون في مراجعات الشيفرة لتحسين عملية المراجعة.

2.5.4 Challenges and Solutions / التحديات والحلول

A. Time Constraints / قيود الوقت

Balancing thorough reviews with development timelines to ensure timely feedback without delaying the project. موازنة المراجعات الشاملة مع جداول التطوير الزمنية لضمان الحصول على الملاحظات في الوقت المناسب دون تأخير المشروع.

Examples: Prioritizing critical code segments for detailed reviews and using automated tools for routine checks. تحديد أولويات أقسام الشيفرة الحيوية للمراجعات التفصيلية واستخدام الأدوات الآلية للفحوصات الروتينية.

B. Reviewer Bias / تحيز المراجع

Ensuring objective and unbiased reviews by implementing peer review rotations and clear review criteria. ضمان مراجعات موضوعية وغير متحيزة من خلال تنفيذ دوران مراجعة الأقران ومعايير مراجعة واضحة.

Examples: Rotating reviewers for different code segments and establishing guidelines to minimize bias. تدوير المراجعين لأقسام الشيفرة المختلفة ووضع إرشادات لتقليل التحيز.

C. Scalability / قابلية التوسع

Managing code reviews for large codebases by automating repetitive tasks and prioritizing critical areas. إدارة مراجعات الشيفرة لقاعدة الشيفرة الكبيرة من خلال أتمتة المهام المتكررة وتحديد أولويات المناطق الحيوية.

Examples: Using automated code review tools for initial checks and focusing manual reviews on critical and complex code. استخدام أدوات مراجعة الشيفرة الآلية للفحوصات الأولية والتركيز على المراجعات اليدوية للشيفرة الحيوية والمعقدة.

2.6. Misuse Case Testing / اختبار حالات سوء الاستخدام

Misuse case testing involves creating scenarios where the system is used incorrectly or maliciously to identify potential vulnerabilities and weaknesses. يشمل اختبار حالات سوء الاستخدام إنشاء سيناريوهات حيث يتم استخدام النظام بشكل غير صحيح أو ضار لتحديد الثغرات والضعف المحتملة.

Purpose: To ensure the system can handle incorrect or malicious use without compromising security or functionality. لضمان أن النظام يمكنه التعامل مع الاستخدام

غير الصحيح أو الضار دون التأثير على الأمان أو الوظائف.

2.6.1 Types of Misuse Cases / أنواع حالات سوء الاستخدام

A. Malicious Use / الاستخدام الضار

Simulating attacks such as SQL injection, cross-site scripting (XSS), and phishing to identify vulnerabilities. محاكاة الهجمات مثل حقن SQL وXSS والتصيد الاحتيالي لتحديد الثغرات.

Examples: Testing for SQL injection by entering malicious SQL commands into input fields. اختبار حقن SQL عن طريق إدخال أوامر SQL ضارة في حقول الإدخال.

B. Accidental Misuse / الاستخدام العرضي

Testing for unintended actions by users, such as input errors and incorrect data formats, to identify potential issues. اختبار الإجراءات غير المقصودة من قبل المستخدمين مثل أخطاء الإدخال وتنسيقات البيانات غير الصحيحة لتحديد المشكلات المحتملة.

Examples: Entering invalid data formats into input fields to see how the system handles them. إدخال تنسيقات بيانات غير صحيحة في حقول الإدخال لمعرفة كيفية تعامل النظام معها.

C. Abuse of Functionality / إساءة استخدام الوظائف

Exploiting legitimate functions in unintended ways to cause harm, such as using a file upload feature to upload malicious files. استغلال الوظائف الشرعية بطرق غير مقصودة لإلحاق الضرر مثل استخدام ميزة تحميل الملفات لتحميل ملفات ضارة.

Examples: Testing file upload features by attempting to upload scripts or executable files instead of images. اختبار ميزات تحميل الملفات عن طريق محاولة تحميل نصوص أو ملفات تنفيذية بدلاً من الصور.

2.6.2 Implementation Strategies / استراتيجيات التنفيذ

A. Scenario Development / تطوير السيناريوهات

Identifying potential misuse scenarios and creating detailed descriptions and steps for each scenario. تحديد سيناريوهات سوء الاستخدام المحتملة وإنشاء أوصاف مفصلة وخطوات لكل سيناريو.

Examples: Developing scenarios for SQL injection, cross-site scripting (XSS), and buffer overflow attacks. تطوير سيناريوهات لهجمات حقن SQLو XSS وتجاوز سعة المخزن المؤقت.

B. Tool Selection / اختيار الأدوات

Using security testing tools to simulate attacks and identify vulnerabilities. استخدام أدوات اختبار الأمان لمحاكاة الهجمات وتحديد الثغرات.

Examples: Using tools like OWASP ZAP, Burp Suite, and Nessus for misuse case testing. استخدام أدوات مثل OWASP ZAPو Burp Suiteو Nessus لاختبار حالات سوء الاستخدام.

C. Integration with Testing Frameworks / التكامل مع أطر الاختبار

Incorporating misuse case tests into existing testing frameworks and running them as part of regular testing cycles. دمج اختبارات حالات سوء الاستخدام في أطر الاختبار الحالية وتشغيلها كجزء من دورات الاختبار المنتظمة.

Examples: Integrating misuse case tests into CI/CD pipelines to ensure they are run automatically during development. دمج اختبارات حالات سوء الاستخدام في خطوط التكامل المستمر / التسليم المستمر (CI/CD) لضمان تشغيلها تلقائيًا أثناء التطوير.

2.6.3 Metrics and KPIs / المقاييس ومؤشرات الأداء الرئيسية (KPIs)

A. Detection Rate / معدل الاكتشاف

The percentage of misuse cases detected by the system during testing. نسبة حالات سوء الاستخدام التي يتم اكتشافها بواسطة النظام أثناء الاختبار.

Examples: Tracking the detection rate for various misuse scenarios to measure the effectiveness of the system. تتبع معدل الاكتشاف لسيناريوهات سوء الاستخدام المختلفة لقياس فعالية النظام.

B. False Positive/Negative Rates / معدلات الإيجابيات الكاذبة / السلبيات الكاذبة

Measuring the accuracy of misuse case detection by tracking false positives (incorrect alerts) and false negatives (missed issues). قياس دقة اكتشاف حالات سوء الاستخدام من خلال تتبع الإيجابيات الكاذبة (تنبيهات غير صحيحة) والسلبيات الكاذبة (مشكلات مفقودة).

Examples: Monitoring false positive and negative rates to balance detection capabilities and minimize false alarms. مراقبة معدلات الإيجابيات الكاذبة والسلبيات الكاذبة لتحقيق توازن في قدرات الاكتشاف وتقليل الإنذارات الكاذبة.

C. Time to Remediate / وقت الإصلاح

The average time taken to address identified misuse cases and fix vulnerabilities. متوسط الوقت المستغرق لمعالجة حالات سوء الاستخدام المحددة وإصلاح الثغرات.

Examples: Tracking the time taken to remediate vulnerabilities identified during misuse case testing. تتبع الوقت المستغرق لإصلاح الثغرات التي تم تحديدها أثناء اختبار حالات سوء الاستخدام.

2.6.4 Challenges and Solutions / التحديات والحلول

A. Scenario Complexity / تعقيد السيناريو

Managing the complexity of detailed misuse scenarios by breaking them down into manageable steps. إدارة تعقيد سيناريوهات سوء الاستخدام المفصلة من خلال تقسيمها إلى خطوات يمكن التحكم فيها.

Examples: Developing step-by-step scenarios for complex attacks such as advanced persistent threats (APTs). تطوير سيناريوهات خطوة بخطوة لهجمات معقدة مثل التهديدات المستمرة المتقدمة (APTs).

B. Tool Limitations / قيود الأدوات

Addressing the limitations of testing tools by using multiple tools to cover different scenarios. معالجة قيود أدوات الاختبار من خلال استخدام أدوات متعددة لتغطية سيناريوهات مختلفة.

Examples: Combining tools like OWASP ZAP, Burp Suite, and Nessus to cover a broad range of misuse scenarios. دمج أدوات مثل OWASP ZAP وBurp Suite وNessus لتغطية مجموعة واسعة من سيناريوهات سوء الاستخدام.

C. Resource Constraints / قيود الموارد

Allocating sufficient resources, including personnel and technology, to effectively conduct misuse case testing. تخصيص الموارد الكافية بما في ذلك الأفراد والتكنولوجيا لإجراء اختبار حالات سوء الاستخدام بشكل فعال.

Examples: Automating parts of the testing process to reduce manual effort and optimize resource utilization. أتمتة أجزاء من عملية الاختبار لتقليل الجهد اليدوي وتحسين استخدام الموارد.

2.7. Coverage Analysis / تحليل التغطية

Coverage analysis measures the extent to which the code, functionalities, and paths of a system are tested to ensure comprehensive test coverage. يقيس تحليل التغطية مدى اختبار الشيفرة والوظائف والمسارات في النظام لضمان التغطية الشاملة للاختبار.

Purpose: To identify gaps in testing and ensure all critical components are adequately tested. لتحديد الفجوات في الاختبار وضمان اختبار جميع المكونات الحيوية بشكل كافٍ.

2.7.1 Types of Coverage / أنواع التغطية

A. Code Coverage / تغطية الشيفرة

Measuring the extent of code tested by unit and integration tests, including line coverage, branch coverage, and path coverage. قياس مدى الشيفرة التي تم اختبارها بواسطة اختبارات الوحدة والتكامل بما في ذلك تغطية السطر وتغطية الفروع وتغطية المسار.

Examples: Using code coverage tools to measure line coverage (percentage of code lines executed) and branch coverage (percentage of decision points tested). استخدام أدوات تغطية الشيفرة لقياس تغطية السطر (نسبة الأسطر البرمجية التي تم تنفيذها) وتغطية الفروع (نسبة نقاط القرار التي تم اختبارها).

B. Functional Coverage / تغطية الوظائف

Testing all defined functions and features to ensure they work as intended and meet specified requirements. اختبار جميع الوظائف والميزات المحددة لضمان عملها كما هو مقصود وتلبية المتطلبات المحددة.

Examples: Creating test cases for each function and feature in the system to verify that they perform correctly. إنشاء حالات اختبار لكل وظيفة وميزة في النظام للتحقق من أدائها بشكل صحيح.

C. Requirement Coverage / تغطية المتطلبات

Ensuring all requirements are tested by mapping tests to requirements and verifying that each requirement is covered. ضمان اختبار جميع المتطلبات من خلال ربط الاختبارات

بالمتطلبات والتحقق من تغطية كل متطلب.

Examples: Using requirement traceability matrices to map test cases to specific requirements and verify coverage. استخدام مصفوفات تتبع المتطلبات لربط حالات الاختبار بالمتطلبات المحددة والتحقق من التغطية.

2.7.2 Implementation Strategies / استراتيجيات التنفيذ

A. Tool Selection / اختيار الأدوات

Using coverage analysis tools such as code coverage tools and test management tools to measure and ensure comprehensive test coverage. استخدام أدوات تحليل التغطية مثل أدوات تغطية الشيفرة وأدوات إدارة الاختبار لقياس وضمان التغطية الشاملة للاختبار.

Examples: Selecting tools like JaCoCo, Clover, and TestRail to perform coverage analysis.اختيار الأدوات لإجراء تحليل التغطية

B. Coverage Criteria / معايير التغطية

Defining coverage criteria and thresholds to prioritize critical areas for coverage and ensure comprehensive testing. تحديد معايير التغطية والحدود لتحديد أولويات المناطق الحيوية للتغطية وضمان الاختبار الشامل.

Examples: Setting minimum coverage thresholds for line coverage, branch coverage, and functional coverage. تحديد حدود التغطية الدنيا لتغطية السطر وتغطية الفروع وتغطية الوظائف.

C. Gap Analysis / تحليل الفجوات

Identifying areas with insufficient coverage and creating tests to address gaps and ensure comprehensive coverage. تحديد المناطق ذات التغطية غير الكافية وإنشاء اختبارات لمعالجة الفجوات وضمان التغطية الشاملة.

Examples: Performing gap analysis to identify untested areas and developing additional test cases to cover them. إجراء تحليل الفجوات لتحديد المناطق غير المختبرة وتطوير حالات اختبار إضافية لتغطيتها.

2.7.3 Metrics and KPIs / المقاييس ومؤشرات الأداء الرئيسية (KPIs)

A. Coverage Percentage / نسبة التغطية

Calculating the percentage of code or functions covered by tests to measure the extent of test coverage. حساب نسبة الشيفرة أو الوظائف التي تم تغطيتها بواسطة الاختبارات لقياس مدى تغطية الاختبار.

Examples: Tracking the percentage of lines, branches, and functions covered by unit and integration tests. تتبع نسبة الأسطر والفروع والوظائف التي تم تغطيتها بواسطة اختبارات الوحدة والتكامل.

B. Test Effectiveness / فعالية الاختبار

Measuring the effectiveness of tests in detecting defects and ensuring high-quality software. قياس فعالية الاختبارات في الكشف عن العيوب وضمان جودة البرمجيات العالية.

Examples: Tracking the number of defects identified by tests and evaluating the effectiveness of different test cases. تتبع عدد العيوب التي تم تحديدها بواسطة الاختبارات وتقييم فعالية حالات الاختبار المختلفة.

C. Defect Density / كثافة العيوب

The number of defects found per unit of code or functionality to assess the quality of the codebase. عدد العيوب التي تم العثور عليها لكل وحدة من الشيفرة أو الوظائف لتقييم جودة قاعدة الشيفرة.

Examples: Calculating defect density to identify areas of the codebase that require improvement and more thorough testing. حساب كثافة العيوب لتحديد مناطق قاعدة الشيفرة التي تتطلب تحسينًا واختبارًا أكثر شمولاً.

2.7.4 Challenges and Solutions / التحديات والحلول

A. Coverage Gaps / فجوات التغطية

Identifying and addressing gaps in test coverage to ensure all critical components are adequately tested. تحديد ومعالجة الفجوات في تغطية الاختبار لضمان اختبار جميع المكونات الحيوية بشكل كافٍ.

Examples: Performing gap analysis to identify untested areas and developing additional test cases to cover them. إجراء تحليل الفجوات لتحديد المناطق غير المختبرة وتطوير حالات اختبار إضافية لتغطيتها.

Use Case: A QA team conducts gap analysis to identify and address gaps in test coverage, ensuring all critical functionalities are tested. يقوم فريق ضمان الجودة بإجراء تحليل الفجوات لتحديد ومعالجة الفجوات في تغطية الاختبار وضمان اختبار جميع الوظائف الحيوية.

B. Resource Constraints / قيود الموارد

Allocating sufficient resources, including personnel and technology, to effectively conduct coverage analysis and testing. تخصيص الموارد الكافية بما في ذلك الأفراد والتكنولوجيا لإجراء تحليل وتغطية الاختبار بشكل فعال.

Examples: Automating parts of the testing process to reduce manual effort and optimize resource utilization. أتمتة أجزاء من عملية الاختبار لتقليل الجهد اليدوي وتحسين استخدام الموارد.

Use Case: A QA team automates routine testing tasks to free up resources for more critical and complex testing activities. يقوم فريق ضمان الجودة بأتمتة المهام الاختبارية الروتينية لتحرير الموارد للأنشطة الاختبارية الأكثر حيوية وتعقيدًا.

C. Complex Systems / الأنظمة المعقدة

Managing coverage analysis and testing for complex and large systems by breaking them down into manageable components. إدارة تحليل وتغطية الاختبار للأنظمة المعقدة والكبيرة من خلال تقسيمها إلى مكونات يمكن التحكم فيها.

Examples: Dividing complex systems into smaller, more manageable components for targeted testing. تقسيم الأنظمة المعقدة إلى مكونات أصغر يمكن التحكم فيها بشكل أكبر للاختبار المستهدف.

Use Case: A QA team breaks down complex systems into manageable components to ensure thorough and targeted coverage analysis. يقوم فريق ضمان الجودة بتقسيم الأنظمة المعقدة إلى مكونات يمكن التحكم فيها لضمان تحليل تغطية شامل ومستهدف.

2.8. Interface Testing / اختبار الواجهات

Interface testing focuses on verifying the interactions between different components, systems, or applications to ensure they work together correctly. يركز اختبار الواجهات على التحقق من التفاعلات بين المكونات المختلفة أو الأنظمة أو التطبيقات لضمان عملها معًا بشكل صحيح.

Purpose: To ensure seamless integration and communication between components, reducing the risk of interface-related defects. لضمان التكامل السلس والتواصل بين المكونات وتقليل خطر العيوب المتعلقة بالواجهة.

2.8.1 Types of Interfaces / أنواع الواجهات

A. User Interface (UI) / واجهة المستخدم

Testing graphical user interfaces (GUIs) to ensure usability and functionality for end-users. اختبار واجهات المستخدم الرسومية لضمان سهولة الاستخدام والوظائف للمستخدمين النهائيين.

Examples: Checking the layout, buttons, and navigation of a web application to ensure they are intuitive and functional. فحص التخطيط والأزرار والتنقل في تطبيق الويب لضمان أنها سهلة الاستخدام وعملية.

B. Network Interface / واجهة الشبكة

Testing network communication and protocols to ensure data is transmitted correctly and securely. اختبار الاتصال الشبكي والبروتوكولات لضمان نقل البيانات بشكل صحيح وآمن.

Examples: Validating the functionality of network protocols such as TCP/IP and ensuring secure data transmission. التحقق من وظائف البروتوكولات الشبكية وضمان نقل البيانات بشكل آمن.

C. Application Programming Interface (API) / واجهة برمجة التطبيقات (API)

Testing API endpoints and interactions to ensure APIs function as expected and handle edge cases. اختبار نقاط نهاية واجهة برمجة التطبيقات والتفاعلات لضمان عمل واجهات برمجة التطبيقات كما هو متوقع ومعالجة الحالات الحديّة.

Examples: Sending requests to APIs to check response times and correctness under various conditions. إرسال طلبات إلى واجهات برمجة التطبيقات للتحقق من أوقات الاستجابة والدقة تحت ظروف مختلفة.

2.8.2 Implementation Strategies / استراتيجيات التنفيذ

A. Test Planning / تخطيط الاختبار

Defining test cases and scenarios for each interface type and prioritizing critical interfaces for testing. تحديد حالات الاختبار والسيناريوهات لكل نوع واجهة وتحديد أولويات الواجهات الحيوية للاختبار.

Examples: Creating detailed test plans for UI, network, and API testing, including scenarios for both typical and edge cases. إنشاء خطط اختبار مفصلة لاختبار واجهة المستخدم والشبكة وواجهة برمجة التطبيقات بما في ذلك السيناريوهات للحالات النموذجية والحالات الحديّة.

B. Tool Selection / اختيار الأدوات

Using specialized tools for UI, network, and API testing and integrating them with existing testing frameworks. استخدام أدوات متخصصة لاختبار واجهة المستخدم والشبكة وواجهة برمجة التطبيقات ودمجها مع أطر الاختبار الحالية.

Examples: Selecting tools like Selenium for UI testing لاختبار واجهة المستخدم, Wireshark for network testing لاختبار الشبكة, and Postman for API testing. لاختبار واجهة برمجة التطبيقات

C. Test Execution / تنفيذ الاختبار

Executing interface tests regularly and automating tests where possible to ensure consistency. تنفيذ اختبارات الواجهات بانتظام وأتمتة الاختبارات عند الإمكان لضمان الاتساق.

Examples: Running automated UI tests using Selenium and scheduled API tests using Postman collections.

2.8.3 Metrics and KPIs / المقاييس ومؤشرات الأداء الرئيسية (KPIs)

A. Interface Coverage / تغطية الواجهة

The percentage of interfaces tested to measure the extent of test coverage. نسبة الواجهات التي تم اختبارها لقياس مدى تغطية الاختبار.

Examples: Tracking the number of UI, network, and API interfaces tested to ensure comprehensive coverage. تتبع عدد واجهات المستخدم والشبكة وواجهة برمجة التطبيقات التي تم اختبارها لضمان التغطية الشاملة.

B. Response Time / وقت الاستجابة

Measuring the response time of interfaces to ensure they meet performance benchmarks. قياس وقت استجابة الواجهات لضمان تلبية معايير الأداء.

Examples: Tracking the response times of API calls and UI interactions to identify performance bottlenecks. تتبع أوقات استجابة نداءات واجهة برمجة التطبيقات والتفاعلات مع واجهة المستخدم لتحديد اختناقات الأداء.

C. Error Rates / معدلات الخطأ

Tracking the number of errors encountered during interface testing to identify and address issues. تتبع عدد الأخطاء التي تم مواجهتها أثناء اختبار الواجهات لتحديد ومعالجة المشكلات.

Examples: Monitoring error rates in API responses and UI interactions to ensure reliability and correctness. مراقبة معدلات الخطأ في استجابات واجهة برمجة التطبيقات والتفاعلات مع واجهة المستخدم لضمان الموثوقية والدقة.

2.8.4 Challenges and Solutions / التحديات والحلول

A. Complex Interactions / التفاعلات المعقدة

Managing complex interactions between multiple components by breaking them down into manageable test cases. إدارة التفاعلات المعقدة بين المكونات المتعددة من خلال تقسيمها إلى حالات اختبار يمكن التحكم فيها.

Examples: Developing step-by-step test cases for complex interactions such as multi-step API workflows or multi-page UI processes. تطوير حالات اختبار خطوة بخطوة للتفاعلات المعقدة مثل سير عمل واجهة برمجة التطبيقات متعدد الخطوات أو عمليات واجهة المستخدم متعددة الصفحات.

B. Tool Limitations / قيود الأدوات

Addressing limitations of testing tools by using multiple tools to cover different interfaces and scenarios. معالجة قيود أدوات الاختبار من خلال استخدام أدوات متعددة لتغطية الواجهات والسيناريوهات المختلفة.

Examples: Combining tools like Selenium for UI testing, Wireshark for network testing, and Postman for API testing.

C. Resource Constraints / قيود الموارد

Allocating sufficient resources, including personnel and technology, to effectively conduct interface testing. تخصيص الموارد الكافية بما في ذلك الأفراد والتكنولوجيا لإجراء اختبار الواجهات بشكل فعال.

Examples: Automating parts of the testing process to reduce manual effort and optimize resource utilization. أتمتة أجزاء من عملية الاختبار لتقليل الجهد اليدوي وتحسين استخدام الموارد.

2.9. Breach Attack Simulations / محاكاة هجمات الاختراق

Breach attack simulations involve mimicking cyberattacks on an organization's systems to evaluate the effectiveness of security defenses and response strategies. تشمل محاكاة هجمات الاختراق تقليد الهجمات السيبرانية على أنظمة المؤسسة لتقييم فعالية الدفاعات الأمنية واستراتيجيات الاستجابة.

Purpose: To identify vulnerabilities, improve incident response, and strengthen overall security posture. لتحديد الثغرات وتحسين الاستجابة للحوادث وتعزيز الوضع الأمني العام.

2.9.1 Types of Simulations / أنواع المحاكاة

A. Red Teaming / فريق الأحمر

Simulating advanced, realistic attacks by adversaries to test the organization's defenses and response capabilities. محاكاة الهجمات المتقدمة والواقعية من قبل الخصوم لاختبار دفاعات المنظمة وقدرات الاستجابة.

Examples: Conducting red team exercises to simulate a sophisticated phishing attack aimed at gaining unauthorized access to sensitive data. إجراء تمارين الفريق الأحمر لمحاكاة هجوم تصيد احتيالي متقدم يستهدف الحصول على وصول غير مصرح به إلى البيانات الحساسة.

B. Blue Teaming / فريق الأزرق

Defending against simulated attacks and evaluating the effectiveness of detection and response mechanisms. الدفاع ضد الهجمات المحاكية وتقييم فعالية آليات الكشف والاستجابة.

Examples: Conducting blue team exercises to test the organization's ability to

detect and respond to a simulated ransomware attack. إجراء تمارين الفريق الأزرق لاختبار قدرة المنظمة على الكشف والاستجابة لهجوم فدية محاكى.

C. Purple Teaming / فريق الأرجواني

Collaboration between red and blue teams to enhance both offensive and defensive strategies. التعاون بين فرق الأحمر والأزرق لتعزيز استراتيجيات الهجوم والدفاع.

Examples: Engaging in purple team exercises where red team members share insights with the blue team to improve overall security posture. المشاركة في تمارين الفريق الأرجواني حيث يشارك أعضاء الفريق الأحمر الأفكار مع الفريق الأزرق لتحسين الوضع الأمني العام.

2.9.2 Implementation Strategies / استراتيجيات التنفيذ

A. Scenario Development / تطوير السيناريوهات

Creating realistic and relevant attack scenarios, defining objectives, and setting success criteria for each simulation. إنشاء سيناريوهات هجومية واقعية وذات صلة وتحديد الأهداف ووضع معايير النجاح لكل محاكاة.

Examples: Developing scenarios for various types of attacks such as phishing, DDoS, and data exfiltration to test different aspects of security. تطوير سيناريوهات لأنواع مختلفة من الهجمات مثل التصيد الاحتيالي ومنع الوصول واستخراج البيانات لاختبار جوانب مختلفة من الأمان.

B. Tool Selection / اختيار الأدوات

Utilizing automated tools for conducting simulations and employing manual techniques for sophisticated and nuanced attacks. استخدام الأدوات الآلية لإجراء المحاكاة وتوظيف التقنيات اليدوية للهجمات المتطورة والدقيقة.

Examples: Selecting tools like Metasploit, Cobalt Strike, and custom scripts for conducting red team exercises and breach simulations. اختيار الأدوات والبرامج النصية المخصصة لإجراء تمارين الفريق الأحمر ومحاكاة الاختراق.

C. Execution / التنفيذ

Scheduling regular simulations to test and improve security measures, adjusting scenarios based on evolving threats and organizational changes. جدولة المحاكاة المنتظمة لاختبار وتحسين التدابير الأمنية وتعديل السيناريوهات بناءً على التهديدات المتطورة

والتغييرات التنظيمية.

Examples: Executing breach attack simulations quarterly to test the organization's incident response and update scenarios based on recent threat intelligence. تنفيذ محاكاة لهجمات الاختراق كل ثلاثة أشهر لاختبار استجابة الحوادث في المنظمة وتحديث السيناريوهات بناءً على استخبارات التهديدات الأخيرة.

2.9.3 Metrics and KPIs / المقاييس ومؤشرات الأداء الرئيسية (KPIs)

A. Detection Time / وقت الاكتشاف

Measuring the time taken to detect simulated attacks to assess the effectiveness of monitoring and alerting systems. قياس الوقت المستغرق لاكتشاف الهجمات المحاكية لتقييم فعالية أنظمة المراقبة والتنبيه.

Examples: Tracking the time from the initiation of an attack simulation to its detection by the security team. تتبع الوقت من بدء محاكاة الهجوم إلى اكتشافه من قبل فريق الأمان.

B. Response Time / وقت الاستجابة

Measuring the time taken to respond to simulated attacks to evaluate the efficiency of incident response processes. قياس الوقت المستغرق للاستجابة للهجمات المحاكية لتقييم كفاءة عمليات الاستجابة للحوادث.

Examples: Tracking the time from detection to the initiation of response actions during breach attack simulations. تتبع الوقت من الاكتشاف إلى بدء إجراءات الاستجابة خلال محاكاة هجمات الاختراق.

C. Success Rate / معدل النجاح

Percentage of attacks successfully detected and mitigated to assess the effectiveness of security defenses. نسبة الهجمات التي تم اكتشافها وتخفيفها بنجاح لتقييم فعالية الدفاعات الأمنية.

Examples: Calculating the success rate of detecting and mitigating various simulated attack scenarios. حساب معدل النجاح في اكتشاف وتخفيف سيناريوهات الهجوم المحاكية المختلفة.

2.9.4 Best Practices / أفضل الممارسات

A. Realistic Scenarios / السيناريوهات الواقعية

Simulating attacks that reflect current and emerging threats to ensure thorough testing of security defenses. محاكاة الهجمات التي تعكس التهديدات الحالية والناشئة لضمان اختبار شامل للدفاعات الأمنية.

Examples: Developing scenarios based on real-world incidents such as ransomware attacks and data breaches. تطوير سيناريوهات بناءً على الحوادث الواقعية مثل هجمات الفدية واختراقات البيانات.

B. Continuous Improvement / التحسين المستمر

Learning from each simulation to enhance defenses and response strategies, incorporating feedback and lessons learned. التعلم من كل محاكاة لتعزيز الدفاعات واستراتيجيات الاستجابة ودمج الملاحظات والدروس المستفادة.

Examples: Updating incident response plans based on insights gained from breach attack simulations. تحديث خطط الاستجابة للحوادث بناءً على الأفكار المكتسبة من محاكاة هجمات الاختراق.

C. Collaboration / التعاون

Encouraging collaboration between red and blue teams to share insights and strategies for improving overall security. تشجيع التعاون بين فرق الأحمر والأزرق لمشاركة الأفكار والاستراتيجيات لتحسين الأمن العام.

Examples: Conducting debriefing sessions where red and blue teams discuss findings and recommend improvements. إجراء جلسات تقييم حيث تناقش فرق الأحمر والأزرق النتائج وتوصي بالتحسينات.

2.9.5 Challenges and Solutions / التحديات والحلول

A. Scenario Complexity / تعقيد السيناريو

Managing the complexity of detailed and realistic attack scenarios by breaking them down into manageable steps. إدارة تعقيد السيناريوهات الهجومية المفصلة والواقعية من خلال تقسيمها إلى خطوات يمكن التحكم فيها.

Examples: Developing step-by-step scenarios for complex attacks such as advanced

persistent threats (APTs). تطوير سيناريوهات خطوة بخطوة لهجمات معقدة مثل التهديدات المستمرة المتقدمة

B. Tool Limitations / قيود الأدوات

Addressing limitations of simulation tools by using a combination of tools to cover different attack vectors. معالجة قيود أدوات المحاكاة من خلال استخدام مجموعة من الأدوات لتغطية نواقل الهجوم المختلفة.

Examples: Combining tools like Metasploit, Cobalt Strike, and custom scripts to cover various attack scenarios. دمج الأدوات والبرامج النصية المخصصة لتغطية سيناريوهات الهجوم المختلفة.

C. Resource Constraints / قيود الموارد

Allocating sufficient resources, including personnel and technology, to effectively conduct breach attack simulations. تخصيص الموارد الكافية بما في ذلك الأفراد والتكنولوجيا لإجراء محاكاة هجمات الاختراق بشكل فعال.

Examples: Automating parts of the simulation process to reduce manual effort and optimize resource utilization. أتمتة أجزاء من عملية المحاكاة لتقليل الجهد اليدوي وتحسين استخدام الموارد.

2.10. Compliance Checks / فحوصات الامتثال

Compliance checks involve verifying that an organization's systems, processes, and policies adhere to relevant laws, regulations, and standards. تشمل فحوصات الامتثال التحقق من أن أنظمة المؤسسة وعملياتها وسياساتها تلتزم بالقوانين واللوائح والمعايير ذات الصلة.

Purpose: To ensure legal and regulatory compliance, avoid penalties, and maintain organizational integrity and reputation. لضمان الامتثال القانوني والتنظيمي وتجنب العقوبات والحفاظ على نزاهة وسمعة المؤسسة.

2.10.1 Types of Compliance Checks / أنواع فحوصات الامتثال

A. Internal Audits / التدقيقات الداخلية

Conducting audits within the organization to ensure adherence to internal policies

and evaluate the effectiveness of internal controls and processes. إجراء التدقيقات داخل المنظمة لضمان الامتثال للسياسات الداخلية وتقييم فعالية الضوابط والعمليات الداخلية.

Examples: Performing regular internal audits to assess compliance with internal security policies and procedures. إجراء التدقيقات الداخلية بانتظام لتقييم الامتثال للسياسات والإجراءات الأمنية الداخلية.

B. External Audits / التدقيقات الخارجية

Engaging external auditors to provide an independent assessment of compliance with external standards and regulatory requirements. إشراك المدققين الخارجيين لتقديم تقييم مستقل للامتثال للمعايير الخارجية والمتطلبات التنظيمية.

Examples: Hiring external audit firms to conduct annual assessments of the organization's compliance with industry standards and regulations. استئجار شركات التدقيق الخارجية لإجراء تقييمات سنوية لامتثال المؤسسة للمعايير الصناعية واللوائح.

C. Automated Compliance Monitoring / مراقبة الامتثال الآلي

Using tools to continuously monitor compliance status, detect non-compliance issues in real-time, and generate alerts. استخدام الأدوات لمراقبة حالة الامتثال باستمرار، والكشف عن قضايا عدم الامتثال في الوقت الفعلي، وإصدار التنبيهات.

Examples: Implementing compliance management tools to monitor adherence to data protection regulations and generate alerts for non-compliance. تنفيذ أدوات إدارة الامتثال لمراقبة الامتثال للوائح حماية البيانات وإصدار التنبيهات لعدم الامتثال.

2.10.2 Implementation Strategies / استراتيجيات التنفيذ

A. Policy Development / تطوير السياسات

Developing comprehensive compliance policies and procedures aligned with relevant laws and regulations. تطوير سياسات وإجراءات الامتثال الشاملة المتوافقة مع القوانين واللوائح ذات الصلة.

Examples: Creating data protection policies to comply with GDPR and ensuring they are communicated to all employees. إنشاء سياسات حماية البيانات للامتثال لـ وضمان إبلاغها لجميع الموظفين.

B. Audit Planning / تخطيط التدقيق

Defining the scope, objectives, and frequency of compliance audits to ensure ongoing compliance. تحديد نطاق وأهداف وتواتر التدقيقات الامتثال لضمان الامتثال المستمر.

Examples: Scheduling annual compliance audits to assess adherence to industry standards and regulatory requirements. جدولة التدقيقات الامتثال السنوية لتقييم الامتثال للمعايير الصناعية والمتطلبات التنظيمية.

C. Tool Selection / اختيار الأدوات

Selecting and implementing compliance management tools to automate compliance checks and enhance efficiency and accuracy. اختيار وتنفيذ أدوات إدارة الامتثال لأتمتة فحوصات الامتثال وتعزيز الكفاءة والدقة.

Examples: Using tools like Symantec Control Compliance Suite and IBM OpenPages to automate compliance monitoring and reporting. استخدام الأدوات لأتمتة مراقبة الامتثال والتقارير.

2.10.3 Metrics and KPIs / المقاييس ومؤشرات الأداء الرئيسية (KPIs)

A. Compliance Rate / معدل الامتثال

The percentage of systems and processes that are compliant, used to measure overall compliance status. نسبة الأنظمة والعمليات التي تمتثل، تستخدم لقياس حالة الامتثال العامة.

Examples: Tracking the compliance rate to ensure that a high percentage of systems and processes adhere to relevant regulations. تتبع معدل الامتثال لضمان أن نسبة عالية من الأنظمة والعمليات تمتثل للوائح ذات الصلة.

B. Audit Findings / نتائج التدقيق

The number of findings per audit, used to measure the effectiveness of compliance audits and identify areas for improvement. عدد النتائج لكل تدقيق، يستخدم لقياس فعالية التدقيقات الامتثال وتحديد مجالات التحسين.

Examples: Tracking the number of audit findings to identify recurring issues and areas for improvement. تتبع عدد نتائج التدقيق لتحديد المشكلات المتكررة ومجالات التحسين.

C. Remediation Time / وقت التصحيح

The average time taken to address compliance issues, used to measure the efficiency of remediation efforts. الوقت المتوسط المستغرق لمعالجة قضايا الامتثال، يستخدم لقياس كفاءة جهود التصحيح.

Examples: Tracking remediation time to ensure that compliance issues are addressed promptly and efficiently. تتبع وقت التصحيح لضمان معالجة قضايا الامتثال بسرعة وكفاءة.

2.10.4 Best Practices / أفضل الممارسات

A. Regular Reviews / المراجعات الدورية

Conducting regular reviews of compliance policies and procedures to ensure they remain relevant and effective. إجراء مراجعات دورية لسياسات وإجراءات الامتثال لضمان بقائها ذات صلة وفعالة.

Examples: Reviewing compliance policies annually to ensure they align with current regulations and best practices. مراجعة سياسات الامتثال سنويًا لضمان توافقها مع اللوائح والممارسات الحالية.

B. Training and Awareness / التدريب والتوعية

Training employees on compliance requirements and promoting a culture of compliance within the organization. تدريب الموظفين على متطلبات الامتثال وتعزيز ثقافة الامتثال داخل المؤسسة.

Examples: Conducting regular training sessions on data protection regulations and compliance best practices. إجراء جلسات تدريبية منتظمة على لوائح حماية البيانات وأفضل ممارسات الامتثال.

C. Continuous Monitoring / المراقبة المستمرة

Continuously monitoring compliance status using automated tools to detect non-compliance issues in real-time. مراقبة حالة الامتثال باستمرار باستخدام الأدوات الآلية للكشف عن قضايا عدم الامتثال في الوقت الفعلي.

IEC 61511-1 Clause 15 and Cyber Security

Nicholas Houghton · 6 years ago

Managing Cyber Threat: UAE Cybersecurity Strategy...

Saleh Omeir · 4 years ago

AMS achieves ISO 27001 certification

Dan Richards · 3 years ago

Examples: Implementing continuous compliance monitoring tools to ensure ongoing adherence to data protection regulations. تنفيذ أدوات المراقبة المستمرة للامتثال لضمان الامتثال المستمر للوائح حماية البيانات.

2.10.5 Challenges and Solutions / التحديات والحلول

A. Regulatory Complexity / تعقيد اللوائح

Managing complex and evolving regulations by keeping policies and procedures up-to-date. إدارة اللوائح المعقدة والمتطورة من خلال تحديث السياسات والإجراءات بانتظام.

Examples: Regularly reviewing and updating compliance policies to reflect changes

in regulations and standards. مراجعة وتحديث سياسات الامتثال بانتظام لتعكس التغييرات في اللوائح والمعايير.

B. Resource Constraints / قيود الموارد

Allocating sufficient resources, including personnel and technology, to effectively conduct compliance activities. تخصيص الموارد الكافية بما في ذلك الأفراد والتكنولوجيا لإجراء أنشطة الامتثال بشكل فعال.

Examples: Automating compliance checks to reduce manual effort and optimize resource utilization. أتمتة فحوصات الامتثال لتقليل الجهد اليدوي وتحسين استخدام الموارد.

C. Cross-Departmental Coordination / التنسيق بين الإدارات

Ensuring coordination between different departments to promote collaboration on compliance issues. ضمان التنسيق بين الإدارات المختلفة لتعزيز التعاون في قضايا الامتثال.

Examples: Establishing cross-departmental compliance committees to ensure consistent implementation of compliance policies. إنشاء لجان الامتثال بين الإدارات لضمان تنفيذ سياسات الامتثال بشكل متسق.

Multiple Choice Questions:

1. What is the primary purpose of a vulnerability assessment?

a. To assess security policies

b. To identify security weaknesses that could be exploited by attackers and prioritize them for remediation

c. To evaluate external security controls

d. To ensure compliance with internal standards

2. What is a blind testing approach?

a. The tester has full knowledge of the target

b. The tester has no prior knowledge of the target

c. The tester has partial knowledge of the target

d. The tester and defenders both have full knowledge of the test

3. How does a credentialed scan differ from an unauthenticated scan?

a. Credentialed scans are conducted with access credentials, while unauthenticated scans are conducted without access credentials

b. Unauthenticated scans provide deeper insights, while credentialed scans identify surface vulnerabilities

c. Both scans are conducted without access credentials

d. Credentialed scans are only conducted on external systems

4. What is the purpose of banner grabbing and fingerprinting?

a. To test internal security policies

b. To gather information about a system to identify potential vulnerabilities

c. To perform credentialed scans

d. To ensure compliance with regulatory standards

5. What does CVSS stand for?

a. Common Vulnerability Scanning System

b. Common Vulnerability Scoring System

c. Continuous Vulnerability Scoring System

d. Credentialed Vulnerability Scoring System

Answers and Explanation:

1. b. To identify security weaknesses that could be exploited by attackers and prioritize them for remediation

Explanation: Vulnerability assessment aims to identify security weaknesses and prioritize them for remediation.

يهدف تقييم الثغرات الأمنية إلى تحديد نقاط الضعف الأمنية وترتيبها حسب الأولوية للإصلاح

2. b. The tester has no prior knowledge of the target

Explanation: Blind testing simulates an external attacker with no insider information.

الاختبار الأعمى يحاكي مهاجمًا خارجيًا بدون معلومات داخلية

3. a. Credentialed scans are conducted with access credentials, while unauthenticated scans are conducted without access credentials

Explanation: Credentialed scans provide deeper insights, while unauthenticated scans identify surface vulnerabilities.

توفر المسوح المصادق عليها رؤى أعمق، بينما تحدد المسوح غير المصادق عليها نقاط الضعف السطحية

4. b. To gather information about a system to identify potential vulnerabilities

Explanation: Banner grabbing and fingerprinting gather system information for vulnerability identification.

التقاط البانر والتعرف على البصمة يجمع معلومات النظام لتحديد نقاط الضعف

5. b. Common Vulnerability Scoring System

Explanation: CVSS is a framework for rating the severity of vulnerabilities.

CVSS هو إطار لتقييم خطورة الثغرات الأمنية

---

3. Collect Security Process Data / جمع بيانات عملية الأمان

Collecting security process data involves gathering information related to security activities, processes, and events within an organization. يشمل جمع بيانات عملية الأمان جمع المعلومات المتعلقة بأنشطة الأمان والعمليات والأحداث داخل المؤسسة.

Purpose: To monitor and evaluate the effectiveness of security controls and processes, identify areas for improvement, and ensure compliance with policies and regulations. لمراقبة وتقييم فعالية الضوابط والعمليات الأمنية وتحديد مجالات التحسين وضمان الامتثال للسياسات واللوائح.

3.1. Account Management / إدارة الحسابات

Account management involves the creation, maintenance, and deletion of user accounts within an organization's systems. تشمل إدارة الحسابات إنشاء وصيانة وحذف حسابات المستخدمين داخل أنظمة المؤسسة.

Purpose: To ensure that only authorized users have access to systems and data, and that their access is appropriately managed. لضمان أن المستخدمين المصرح لهم فقط يمكنهم الوصول إلى الأنظمة والبيانات، وأنه يتم إدارة وصولهم بشكل مناسب.

3.1.1 Components / المكونات

A. User Provisioning / توفير المستخدمين

The process of creating user accounts and assigning appropriate access rights and permissions. عملية إنشاء حسابات المستخدمين وتعيين حقوق الوصول والصلاحيات المناسبة.

Examples: Creating user accounts for new employees and granting them access to necessary systems and applications. إنشاء حسابات المستخدمين للموظفين الجدد ومنحهم الوصول إلى الأنظمة والتطبيقات اللازمة.

B. Access Controls / ضوابط الوصول

Mechanisms and policies used to control who can access specific resources and what actions they can perform. الآليات والسياسات المستخدمة للتحكم في من يمكنه الوصول إلى الموارد المحددة وما هي الإجراءات التي يمكنهم تنفيذها.

Examples: Implementing role-based access control (RBAC) to ensure users have access only to resources necessary for their roles. تطبيق التحكم في الوصول المستند إلى الأدوار لضمان حصول المستخدمين على الوصول إلى الموارد اللازمة فقط لأدوارهم.

C. Account Deactivation / تعطيل الحساب

The process of disabling user accounts when they are no longer needed or when a user leaves the organization. عملية تعطيل حسابات المستخدمين عندما لا تكون هناك حاجة إليها أو عندما يترك المستخدم المؤسسة.

Examples: Deactivating the accounts of former employees to prevent unauthorized access to systems and data. تعطيل حسابات الموظفين السابقين لمنع الوصول غير المصرح به إلى الأنظمة والبيانات.

3.1.2 Best Practices / أفضل الممارسات

A. Regular Review of User Access / المراجعة المنتظمة لوصول المستخدمين

Conducting regular reviews of user access rights and permissions to ensure they are appropriate and up-to-date. إجراء مراجعات منتظمة لحقوق وصلاحيات وصول المستخدمين لضمان أنها مناسبة ومحدثة.

Examples: Performing quarterly access reviews to verify that users have the appropriate access based on their current roles. إجراء مراجعات للوصول ربع سنوية للتحقق من أن المستخدمين لديهم الوصول المناسب بناءً على أدوارهم الحالية.

B. Strong Authentication Mechanisms / آليات المصادقة القوية

Implementing robust authentication methods such as multi-factor authentication (MFA) to enhance account security. تطبيق طرق مصادقة قوية مثل المصادقة متعددة العوامل (MFA) لتعزيز أمان الحساب.

Examples: Requiring MFA for accessing sensitive systems and data to ensure that only authorized users can gain access. طلب المصادقة متعددة العوامل للوصول إلى الأنظمة والبيانات الحساسة لضمان أن المستخدمين المصرح لهم فقط يمكنهم الوصول.

C. Least Privilege Principle / مبدأ الحد الأدنى من الامتيازات

Granting users the minimum level of access necessary to perform their job functions to reduce security risks. منح المستخدمين الحد الأدنى من الوصول اللازم لأداء وظائفهم لتقليل المخاطر الأمنية.

Examples: Implementing the least privilege principle to ensure that users only have access to the resources they need for their roles. تطبيق مبدأ الحد الأدنى من الامتيازات لضمان أن المستخدمين لديهم الوصول إلى الموارد التي يحتاجونها فقط لأدوارهم.

3.2. Management Review and Approval / مراجعة الإدارة والموافقة

Management review and approval is the process by which organizational leaders evaluate and approve policies, procedures, and significant changes. تشمل مراجعة الإدارة والموافقة العملية التي يقوم من خلالها قادة المؤسسة بتقييم السياسات والإجراءات والتغييرات الهامة والموافقة عليها.

Purpose: To ensure that changes and policies align with organizational goals and compliance requirements. لضمان توافق التغييرات والسياسات مع أهداف المؤسسة ومتطلبات الامتثال.

3.2.1 Components / المكونات

A. Policy Reviews / مراجعات السياسات

Evaluating existing policies to ensure they remain effective and align with organizational goals and regulatory requirements. تقييم السياسات الحالية لضمان بقائها فعالة ومتوافقة مع أهداف المؤسسة والمتطلبات التنظيمية.

Examples: Conducting annual reviews of security policies to ensure they reflect the latest industry standards and regulations. إجراء مراجعات سنوية لسياسات الأمان لضمان أنها تعكس أحدث المعايير الصناعية واللوائح.

B. Change Management / إدارة التغيير

Managing and documenting significant changes to systems, processes, and policies to ensure they are properly authorized and controlled. إدارة وتوثيق التغييرات الهامة في الأنظمة والعمليات والسياسات لضمان أنها معتمدة ومسيطر عليها بشكل صحيح.

Examples: Implementing a change management process to track and approve changes to critical systems and applications. تطبيق عملية إدارة التغيير لتتبع واعتماد التغييرات في الأنظمة والتطبيقات الحيوية.

C. Audit and Compliance Review / مراجعة التدقيق والامتثال

Conducting regular audits and compliance reviews to ensure adherence to internal policies and external regulations. إجراء التدقيقات ومراجعات الامتثال بانتظام لضمان الامتثال للسياسات الداخلية واللوائح الخارجية.

Examples: Scheduling quarterly compliance reviews to assess adherence to data protection regulations and internal security policies. جدولة مراجعات الامتثال الفصلية لتقييم الامتثال للوائح حماية البيانات والسياسات الأمنية الداخلية.

3.2.2 Best Practices / أفضل الممارسات

A. Regularly Scheduled Reviews / المراجعات المجدولة بانتظام

Scheduling regular reviews of policies, procedures, and changes to ensure they remain effective and aligned with organizational goals. جدولة المراجعات الدورية للسياسات والإجراءات والتغييرات لضمان بقائها فعالة ومتوافقة مع أهداف المؤسسة.

Examples: Conducting quarterly reviews of security policies to ensure they align with the latest regulatory requirements and industry best practices. إجراء مراجعات ربع سنوية لسياسات الأمان لضمان توافقها مع أحدث المتطلبات التنظيمية وأفضل الممارسات الصناعية.

B. Comprehensive Documentation / التوثيق الشامل

Maintaining detailed documentation of policies, procedures, and changes to ensure transparency and accountability. الحفاظ على توثيق شامل للسياسات والإجراءات والتغييرات لضمان الشفافية والمساءلة.

Examples: Documenting all changes to critical systems and policies to ensure they are properly tracked and controlled. توثيق جميع التغييرات في الأنظمة والسياسات الحيوية لضمان تتبعها والسيطرة عليها بشكل صحيح.

C. Stakeholder Involvement / إشراك أصحاب المصلحة

Involving relevant stakeholders in the review and approval process to ensure comprehensive evaluation and buy-in. إشراك أصحاب المصلحة المعنيين في عملية المراجعة والموافقة لضمان التقييم الشامل والدعم.

Examples: Including representatives from different departments in the policy review process to ensure all perspectives are considered. إشراك ممثلين من الأقسام المختلفة في عملية مراجعة السياسات لضمان أخذ جميع وجهات النظر في الاعتبار.

3.3. Key Performance and Risk Indicators / مؤشرات الأداء الرئيسية والمخاطر

Key performance indicators (KPIs) and key risk indicators (KRIs) are metrics used to measure the effectiveness and risks associated with an organization's operations. المؤشرات الرئيسية للأداء والمؤشرات الرئيسية للمخاطر هي مقاييس تستخدم لقياس فعالية ومخاطر العمليات المرتبطة بمؤسسة.

Purpose: To monitor performance, identify areas of risk, and guide decision-making. لمراقبة الأداء، وتحديد مناطق المخاطر، وتوجيه اتخاذ القرارات.

3.3.1 Types of Indicators / أنواع المؤشرات

A. Financial KPIs / المؤشرات المالية للأداء

Metrics that measure financial performance, such as revenue, profit margins, and return on investment (ROI). مقاييس لقياس الأداء المالي، مثل الإيرادات، وهامش الربح، والعائد على الاستثمار

Examples: Tracking monthly revenue growth and comparing it against targets to measure financial success. تتبع نمو الإيرادات الشهري ومقارنته بالأهداف لقياس النجاح المالي.

Use Case: A financial department uses financial KPIs to monitor the organization's economic health and inform strategic decisions. يستخدم قسم المالية المؤشرات المالية للأداء لمراقبة الصحة الاقتصادية للمؤسسة وإبلاغ القرارات الاستراتيجية.

B. Operational KPIs / المؤشرات التشغيلية للأداء

Metrics that measure operational efficiency, such as production output, process efficiency, and operational costs. مقاييس لقياس الكفاءة التشغيلية، مثل إنتاجية الإنتاج، وكفاءة العمليات، وتكاليف التشغيل.

Examples: Measuring the efficiency of production lines by tracking output per hour and downtime. قياس كفاءة خطوط الإنتاج من خلال تتبع الإنتاجية لكل ساعة ووقت التعطل.

Use Case: An operations team uses operational KPIs to optimize production processes and reduce operational costs. يستخدم فريق العمليات المؤشرات التشغيلية للأداء لتحسين عمليات الإنتاج وتقليل تكاليف التشغيل.

C. Compliance KRIs / مؤشرات المخاطر للامتثال

Metrics that measure the risk of non-compliance with regulations and standards, such as the number of compliance violations and audit findings. مقاييس لقياس مخاطر عدم الامتثال للوائح والمعايير، مثل عدد انتهاكات الامتثال ونتائج التدقيق.

Examples: Tracking the number of compliance violations detected during audits to identify areas of regulatory risk. تتبع عدد انتهاكات الامتثال التي تم اكتشافها أثناء التدقيقات لتحديد مناطق المخاطر التنظيمية.

Use Case: A compliance team uses compliance KRIs to monitor regulatory risk and ensure adherence to legal requirements. يستخدم فريق الامتثال مؤشرات المخاطر للامتثال لمراقبة المخاطر التنظيمية وضمان الامتثال للمتطلبات القانونية.

3.3.2 Best Practices / أفضل الممارسات

A. Regular Monitoring and Reporting / المراقبة والتقارير الدورية

Continuously monitoring KPIs and KRIs and regularly reporting the findings to ensure timely decision-making. مراقبة المؤشرات الرئيسية للأداء (KPIs) والمؤشرات الرئيسية للمخاطر (KRIs) باستمرار والإبلاغ عن النتائج بانتظام لضمان اتخاذ القرارات في الوقت المناسب.

Examples: Generating monthly reports on key performance and risk indicators to provide management with up-to-date insights. إعداد تقارير شهرية عن المؤشرات الرئيسية للأداء والمخاطر لتزويد الإدارة برؤى محدثة.

Use Case: A management team uses regular monitoring and reporting of KPIs and KRIs to inform strategic planning and risk management. يستخدم فريق الإدارة المراقبة والتقارير الدورية للمؤشرات الرئيسية للأداء (KPIs) والمؤشرات الرئيسية للمخاطر (KRIs) لإبلاغ التخطيط الاستراتيجي وإدارة المخاطر.

B. Benchmarking against Industry Standards / مقارنة الأداء بالمعايير الصناعية

Comparing organizational KPIs and KRIs against industry standards to identify areas for improvement. مقارنة المؤشرات الرئيسية للأداء والمؤشرات الرئيسية للمخاطر الخاصة بالمؤسسة مع المعايير الصناعية لتحديد مجالات التحسين.

Examples: Assessing operational efficiency by benchmarking production metrics against industry averages. تقييم الكفاءة التشغيلية من خلال مقارنة مقاييس الإنتاج

بمتوسطات الصناعة.

Use Case: An organization benchmarks its performance metrics against industry standards to identify best practices and areas for improvement. تقوم المؤسسة بمقارنة مقاييس الأداء الخاصة بها مع المعايير الصناعية لتحديد أفضل الممارسات ومجالات التحسين.

C. Continuous Improvement / التحسين المستمر

Regularly reviewing and updating KPIs and KRIs to ensure they remain relevant and effective. مراجعة وتحديث المؤشرات الرئيسية للأداء والمؤشرات الرئيسية للمخاطر بانتظام لضمان بقائها ذات صلة وفعالة.

Examples: Periodically adjusting performance metrics based on changes in organizational goals or industry conditions. تعديل مقاييس الأداء بشكل دوري بناءً على التغيرات في أهداف المؤسسة أو الظروف الصناعية.

Use Case: An organization regularly updates its KPIs and KRIs to reflect evolving business priorities and regulatory requirements. تقوم المؤسسة بتحديث المؤشرات الرئيسية للأداء والمؤشرات الرئيسية للمخاطر بانتظام لتعكس أولويات العمل المتطورة والمتطلبات التنظيمية.

3.4. Backup Verification Data / التحقق من بيانات النسخ الاحتياطي

Backup verification involves checking that data backups are accurate, complete, and can be restored successfully. يشمل التحقق من النسخ الاحتياطي التحقق من دقة واكتمال النسخ الاحتياطية للبيانات وإمكانية استعادتها بنجاح.

Purpose: To ensure that data can be recovered in the event of data loss, corruption, or disaster. لضمان إمكانية استعادة البيانات في حالة فقدان البيانات أو تلفها أو حدوث كارثة.

3.4.1 Components / المكونات

A. Backup Scheduling / جدولة النسخ الاحتياطي

Planning and scheduling regular backups to ensure data is consistently and reliably backed up. تخطيط وجدولة النسخ الاحتياطية بانتظام لضمان نسخ البيانات احتياطيًا بشكل متسق وموثوق.

Examples: Implementing daily backups for critical systems and weekly backups for

less critical data. تطبيق النسخ الاحتياطية اليومية للأنظمة الحيوية والنسخ الاحتياطية الأسبوعية للبيانات الأقل أهمية.

B. Data Integrity Checks / فحوصات سلامة البيانات

Verifying the accuracy and completeness of backup data to ensure it matches the original data. التحقق من دقة واكتمال بيانات النسخ الاحتياطي لضمان تطابقها مع البيانات الأصلية.

Examples: Performing checksum verification on backup files to detect any corruption or alterations. إجراء التحقق من قيمة التحقق على ملفات النسخ الاحتياطي لاكتشاف أي تلف أو تغييرات.

C. Restore Testing / اختبار الاستعادة

Regularly testing the restoration process to ensure that backups can be successfully recovered. اختبار عملية الاستعادة بانتظام لضمان إمكانية استعادة النسخ الاحتياطية بنجاح.

Examples: Performing quarterly restore tests to verify that data can be restored from backups without issues. إجراء اختبارات الاستعادة الفصلية للتحقق من إمكانية استعادة البيانات من النسخ الاحتياطية دون مشاكل.

3.4.2 Best Practices / أفضل الممارسات

A. Regular Verification Processes / عمليات التحقق الدورية

Implementing regular verification processes to ensure the accuracy and completeness of backup data. تطبيق عمليات التحقق الدورية لضمان دقة واكتمال بيانات النسخ الاحتياطي.

Examples: Scheduling monthly data integrity checks and quarterly restore tests to maintain reliable backups. جدولة فحوصات سلامة البيانات الشهرية واختبارات الاستعادة الفصلية للحفاظ على النسخ الاحتياطية الموثوقة.

B. Maintaining Backup Logs / الحفاظ على سجلات النسخ الاحتياطي

Keeping detailed logs of backup activities to track and analyze the backup process. الحفاظ على سجلات مفصلة لأنشطة النسخ الاحتياطي لتتبع وتحليل عملية النسخ الاحتياطي.

Examples: Logging all backup operations, including schedules, success or failure status, and any errors encountered. تسجيل جميع عمليات النسخ الاحتياطي، بما في ذلك

الجداول الزمنية، وحالة النجاح أو الفشل، وأي أخطاء تم مواجهتها.

C. Offsite Storage of Backups / التخزين خارج الموقع للنسخ الاحتياطية

Storing backup data in an offsite location to protect against onsite disasters. تخزين بيانات النسخ الاحتياطي في موقع خارجي لحمايتها من الكوارث في الموقع.

Examples: Using cloud storage or an offsite data center to store backup copies of critical data. استخدام التخزين السحابي أو مركز البيانات الخارجي لتخزين نسخ احتياطية من البيانات الحيوية.

3.5. Training and Awareness / التدريب والتوعية

Training and awareness programs educate employees about security policies, procedures, and best practices. تقوم برامج التدريب والتوعية بتعليم الموظفين حول السياسات والإجراءات وأفضل الممارسات الأمنية.

Purpose: To reduce human errors, enhance security posture, and ensure compliance with policies. لتقليل الأخطاء البشرية، وتعزيز الوضع الأمني، وضمان الامتثال للسياسات.

3.5.1 Components / المكونات

A. Security Awareness Training / التدريب على الوعي الأمني

Programs designed to educate employees about security threats, policies, and best practices. برامج مصممة لتعليم الموظفين حول التهديدات الأمنية والسياسات وأفضل الممارسات.

Examples: Conducting regular security awareness sessions to inform employees about phishing attacks and safe online practices. إجراء جلسات التوعية الأمنية بانتظام لإبلاغ الموظفين حول هجمات التصيد الاحتيالي والممارسات الآمنة عبر الإنترنت.

B. Role-Based Training / التدريب المستند إلى الأدوار

Training tailored to the specific security responsibilities of different roles within the organization. التدريب المصمم خصيصًا لمسؤوليات الأمان المحددة للأدوار المختلفة داخل المؤسسة.

Examples: Providing specialized training for IT staff on secure coding practices and for HR staff on data privacy regulations. تقديم تدريب متخصص لفريق تكنولوجيا

المعلومات حول ممارسات الترميز الآمن ولفريق الموارد البشرية حول لوائح الخصوصية.

C. Phishing Simulations / محاكاة التصيد الاحتيالي

Simulating phishing attacks to test employees' awareness and response to such threats. محاكاة هجمات التصيد الاحتيالي لاختبار وعي الموظفين واستجابتهم لمثل هذه التهديدات.

Examples: Conducting periodic phishing simulations to identify employees who may need additional training. إجراء محاكاة تصيد احتيالي دورية لتحديد الموظفين الذين قد يحتاجون إلى تدريب إضافي.

3.5.2 Best Practices / أفضل الممارسات

A. Regular and Updated Training Sessions / جلسات التدريب المنتظمة والمحدثة

Conducting training sessions regularly and updating them to reflect new threats and changes in security policies. إجراء جلسات التدريب بانتظام وتحديثها لتعكس التهديدات الجديدة والتغييرات في السياسات الأمنية.

Examples: Scheduling quarterly security training sessions to keep employees informed about the latest security threats and best practices. جدولة جلسات التدريب الأمني الفصلية لإبقاء الموظفين على اطلاع بأحدث التهديدات الأمنية وأفضل الممارسات.

B. Interactive and Engaging Training Methods / طرق التدريب التفاعلية والجذابة

Using interactive and engaging training methods to enhance learning and retention. استخدام طرق التدريب التفاعلية والجذابة لتعزيز التعلم والاحتفاظ بالمعلومات.

Examples: Incorporating gamification and hands-on activities into security training to make it more engaging and effective. دمج الألعاب والأنشطة العملية في التدريب الأمني لجعله أكثر جاذبية وفعالية.

C. Measuring Training Effectiveness / قياس فعالية التدريب

Assessing the effectiveness of training programs through feedback, tests, and performance metrics. تقييم فعالية برامج التدريب من خلال التغذية الراجعة والاختبارات ومقاييس الأداء.

Examples: Conducting post-training assessments and surveys to gather feedback and measure the impact of training. إجراء التقييمات والاستطلاعات بعد التدريب لجمع

التغذية الراجعة وقياس تأثير التدريب.

3.6. Disaster Recovery (DR) and Business Continuity (BC) / استعادة البيانات واستمرارية الأعمال

DR and BC involve planning and preparation to ensure an organization can recover from disasters and continue operations with minimal disruption. تشمل استعادة البيانات واستمرارية الأعمال التخطيط والتحضير لضمان قدرة المؤسسة على التعافي من الكوارث واستمرار العمليات مع أقل قدر من الانقطاع.

Purpose: To protect organizational assets, minimize downtime, and ensure continuity of critical operations. لحماية أصول المؤسسة وتقليل وقت التوقف وضمان استمرارية العمليات الحيوية.

3.6.1 Components / المكونات

A. Disaster Recovery Planning / تخطيط استعادة البيانات

Developing plans and procedures to recover data and systems in the event of a disaster. تطوير خطط وإجراءات لاستعادة البيانات والأنظمة في حالة حدوث كارثة.

Examples: Creating a detailed disaster recovery plan that includes data backup, system restoration, and communication procedures. إنشاء خطة استعادة البيانات مفصلة تشمل النسخ الاحتياطي للبيانات واستعادة النظام وإجراءات الاتصال.

B. Business Impact Analysis / تحليل تأثير الأعمال

Assessing the potential impact of disruptions on business operations to prioritize recovery efforts. تقييم التأثير المحتمل للانقطاعات على العمليات التجارية لتحديد أولويات جهود الاستعادة.

Examples: Conducting a business impact analysis to identify critical systems and processes and their recovery time objectives (RTOs). إجراء تحليل تأثير الأعمال لتحديد الأنظمة والعمليات الحيوية وأهداف وقت الاستعادة الخاصة بها.

C. Continuity Strategies / استراتيجيات الاستمرارية

Developing strategies to ensure continuous operation of critical business functions during and after a disaster. تطوير استراتيجيات لضمان استمرارية العمليات التجارية الحيوية أثناء وبعد الكارثة.

Examples: Implementing redundant systems, backup power supplies, and remote work capabilities to ensure business continuity. تطبيق أنظمة احتياطية، وإمدادات الطاقة الاحتياطية، وقدرات العمل عن بعد لضمان استمرارية الأعمال.

3.6.2 Best Practices / أفضل الممارسات

A. Regular DR and BC Plan Testing / اختبار خطة استعادة البيانات واستمرارية الأعمال بانتظام

Regularly testing disaster recovery and business continuity plans to ensure they are effective and up-to-date. اختبار خطط استعادة البيانات واستمرارية الأعمال بانتظام لضمان فعاليتها وتحديثها.

Examples: Conducting annual disaster recovery drills and business continuity exercises to test the effectiveness of plans. إجراء تدريبات سنوية لاستعادة البيانات وتمارين استمرارية الأعمال لاختبار فعالية الخطط.

B. Keeping Plans Up-to-Date / الحفاظ على تحديث الخطط

Regularly reviewing and updating disaster recovery and business continuity plans to reflect changes in the organization and its environment. مراجعة وتحديث خطط استعادة البيانات واستمرارية الأعمال بانتظام لتعكس التغييرات في المؤسسة وبيئتها.

Examples: Updating plans to account for new systems, changes in business processes, and evolving threats. تحديث الخطط لأخذ الأنظمة الجديدة في الاعتبار، والتغييرات في العمليات التجارية، والتهديدات المتطورة.

C. Employee Training and Awareness / تدريب وتوعية الموظفين

Training employees on disaster recovery and business continuity procedures to ensure they understand their roles and responsibilities. تدريب الموظفين على إجراءات استعادة البيانات واستمرارية الأعمال لضمان فهمهم لأدوارهم ومسؤولياتهم.

Examples: Conducting regular training sessions and drills to familiarize employees with the disaster recovery and business continuity plans. إجراء جلسات تدريبية وتمارين منتظمة لتعريف الموظفين بخطط استعادة البيانات واستمرارية الأعمال.

Multiple Choice Questions:

1. What is the primary purpose of account management?

a. To create new user accounts

b. To ensure that only authorized users have access to systems and data

c. To delete old user accounts

d. To monitor user activity

2. Why is management review and approval important?

a. To conduct vulnerability assessments

b. To ensure that changes and policies align with organizational goals and compliance requirements

c. To manage user accounts

d. To provide security training

3. What are KPIs and KRIs used for?

a. To create new security policies

b. To measure the effectiveness and risks associated with an organization's operations

c. To test backup restores

d. To conduct security audits

4. What is the purpose of backup verification?

a. To create new backups

b. To ensure that data backups are accurate, complete, and can be restored successfully

c. To train employees

d. To

4. Why are training and awareness programs important?

a. To create new security policies

b. To educate employees about security policies, procedures, and best practices

c. To manage user accounts

d. To ensure data backups are complete

Answers and Explanation:

1. b. To ensure that only authorized users have access to systems and data

Explanation: Account management ensures that only authorized users have access to systems and data, maintaining security and preventing unauthorized access.تضمن إدارة الحسابات أن يكون لدى المستخدمين المصرح لهم فقط حق الوصول إلى الأنظمة والبيانات، مما يحافظ على الأمان ويمنع الوصول غير المصرح به

2. b. To ensure that changes and policies align with organizational goals and compliance requirements

Explanation: Management review and approval ensure that all changes and policies are in line with the organization's goals and comply with regulatory requirements.تضمن مراجعة الإدارة والموافقة أن تكون جميع التغييرات والسياسات متوافقة مع أهداف المؤسسة ومتطلبات الامتثال التنظيمية

3. b. To measure the effectiveness and risks associated with an organization's operations

Explanation: KPIs and KRIs are used to measure the effectiveness and risks of an organization's operations, helping to monitor performance and identify areas for

تستخدم مؤشرات الأداء الرئيسية ومؤشرات المخاطر الرئيسية لقياس فعالية.improvement المخاطر المرتبطة بعمليات المؤسسة، مما يساعد في مراقبة الأداء وتحديد مجالات التحسين

4. b. To ensure that data backups are accurate, complete, and can be restored successfully

Explanation: Backup verification ensures that data backups are accurate, complete, and can be restored successfully, providing data integrity and availability in case of data loss.يضمن التحقق من النسخ الاحتياطي أن تكون النسخ الاحتياطية للبيانات دقيقة وكاملة ويمكن استعادتها بنجاح، مما يوفر سلامة البيانات وتوافرها في حالة فقدان البيانات

5. b. To educate employees about security policies, procedures, and best practices

Explanation: Training and awareness programs educate employees about security policies, procedures, and best practices, reducing human errors and enhancing overall security.تُعَلِّم برامج التدريب والتوعية الموظفين حول السياسات والإجراءات والممارسات الأمنية الأفضل، مما يقلل من الأخطاء البشرية ويعزز الأمان العام

---

4. Analyze Test Output and Generate Report / تحليل نتائج الاختبار وتوليد التقرير

Analyzing test output involves evaluating the results of security tests and assessments to identify vulnerabilities and weaknesses. يشمل تحليل نتائج الاختبار تقييم نتائج الاختبارات الأمنية والتقييمات لتحديد الثغرات والنقاط الضعيفة.

Purpose: To develop remediation plans, handle exceptions, and ensure ethical disclosure of findings. لتطوير خطط التصحيح، والتعامل مع الاستثناءات، وضمان الإفصاح الأخلاقي عن النتائج.

4.1 Remediation / التصحيح

Remediation involves taking corrective actions to fix identified vulnerabilities and weaknesses in an organization's systems and processes. يشمل التصحيح اتخاذ الإجراءات

التصحيحية لإصلاح الثغرات والنقاط الضعيفة المحددة في أنظمة وعمليات المؤسسة.

Purpose: To eliminate security risks, ensure compliance, and improve the overall security posture of the organization. للقضاء على المخاطر الأمنية، وضمان الامتثال، وتحسين الوضع الأمني العام للمؤسسة.

4.1.1 Components / المكونات

A. Vulnerability Assessment / تقييم الثغرات

The process of identifying, quantifying, and prioritizing vulnerabilities in an organization's systems and applications. عملية تحديد وتقييم وإعطاء الأولوية للثغرات في أنظمة وتطبيقات المؤسسة.

Examples: Conducting regular vulnerability assessments using tools like Nessus and Qualys to identify and prioritize security vulnerabilities. إجراء تقييمات الثغرات بانتظام باستخدام أدوات لتحديد وإعطاء الأولوية للثغرات الأمنية.

B. Corrective Action Plan / خطة الإجراءات التصحيحية

Developing and implementing a plan to address identified vulnerabilities and weaknesses. تطوير وتنفيذ خطة لمعالجة الثغرات والنقاط الضعيفة المحددة.

Examples: Creating a corrective action plan that includes specific steps, timelines, and responsibilities for addressing vulnerabilities. إنشاء خطة الإجراءات التصحيحية تشمل الخطوات المحددة والجداول الزمنية والمسؤوليات لمعالجة الثغرات.

C. Implementation of Fixes / تنفيذ الإصلاحات

Applying the necessary patches, updates, and changes to fix identified vulnerabilities. تطبيق التصحيحات والتحديثات والتغييرات اللازمة لإصلاح الثغرات المحددة.

Examples: Applying security patches to systems and applications to fix known vulnerabilities and prevent exploitation. تطبيق التصحيحات الأمنية على الأنظمة والتطبيقات لإصلاح الثغرات المعروفة ومنع استغلالها.

4.1.2 Best Practices / أفضل الممارسات

A. Timely Identification and Response / تحديد والاستجابة في الوقت المناسب

Quickly identifying and responding to vulnerabilities to minimize the risk of exploitation. تحديد الثغرات والاستجابة لها بسرعة لتقليل خطر الاستغلال.

Examples: Implementing automated vulnerability scanning to quickly identify and prioritize vulnerabilities for remediation. تطبيق الفحص الآلي للثغرات لتحديد الثغرات بسرعة وإعطاء الأولوية لتصحيحها.

B. Prioritization of Remediation Efforts / إعطاء الأولوية لجهود التصحيح

Prioritizing remediation efforts based on the severity and potential impact of vulnerabilities. إعطاء الأولوية لجهود التصحيح بناءً على شدة وتأثير الثغرات المحتمل.

Examples: Focusing on critical vulnerabilities that pose the highest risk to the organization and addressing them first. التركيز على الثغرات الحرجة التي تشكل أعلى خطر على المؤسسة ومعالجتها أولاً.

C. Regular Verification and Validation / التحقق والتحقق بانتظام

Regularly verifying and validating that remediation efforts have been successful and vulnerabilities have been fixed. التحقق بانتظام من نجاح جهود التصحيح وإصلاح الثغرات.

Examples: Conducting follow-up scans and tests to ensure that vulnerabilities have been properly addressed. إجراء الفحوصات والاختبارات اللاحقة لضمان معالجة الثغرات بشكل صحيح.

4.2 Exception Handling / التعامل مع الاستثناءات

Exception handling involves managing and documenting deviations from standard procedures or policies, often due to special circumstances. يشمل التعامل مع الاستثناءات إدارة وتوثيق الانحرافات عن الإجراءات أو السياسات القياسية، غالبًا بسبب الظروف الخاصة.

Purpose: To ensure that exceptions are properly authorized, documented, and managed to maintain security and compliance. لضمان أن يتم تفويض وتوثيق وإدارة الاستثناءات بشكل صحيح للحفاظ على الأمان والامتثال.

4.2.1 Components / المكونات

A. Exception Request Process / عملية طلب الاستثناء

The process by which employees can request exceptions to standard policies or procedures. العملية التي يمكن من خلالها للموظفين طلب استثناءات من السياسات أو الإجراءات القياسية.

Examples: Creating a formal process for requesting exceptions, including forms, approvals, and documentation. إنشاء عملية رسمية لطلب الاستثناءات، بما في ذلك النماذج والموافقات والتوثيق.

B. Approval and Documentation / الموافقة والتوثيق

Ensuring that all exceptions are properly approved and documented to maintain transparency and accountability. ضمان أن جميع الاستثناءات معتمدة وموثقة بشكل صحيح للحفاظ على الشفافية والمساءلة.

Examples: Requiring managerial approval for exceptions and maintaining detailed records of approved exceptions. طلب موافقة المديرين على الاستثناءات والحفاظ على سجلات مفصلة للاستثناءات المعتمدة.

C. Monitoring and Review / المراقبة والمراجعة

Regularly monitoring and reviewing exceptions to ensure they remain justified and do not pose security risks. مراقبة ومراجعة الاستثناءات بانتظام لضمان بقائها مبررة وعدم تشكلها مخاطر أمنية.

Examples: Conducting periodic reviews of exceptions to ensure they are still necessary and do not compromise security. إجراء مراجعات دورية للاستثناءات لضمان بقائها ضرورية وعدم تعريض الأمن للخطر.

4.2.2 Best Practices / أفضل الممارسات

A. Clear Exception Handling Policies / سياسات واضحة للتعامل مع الاستثناءات

Establishing clear policies and procedures for handling exceptions to ensure consistency and accountability. وضع سياسات وإجراءات واضحة للتعامل مع الاستثناءات لضمان الاتساق والمساءلة.

Examples: Creating written policies that outline the process for requesting, approving, and documenting exceptions. إنشاء سياسات مكتوبة تحدد عملية طلب، واعتماد، وتوثيق الاستثناءات.

B. Strict Approval Procedures / إجراءات الموافقة الصارمة

Implementing strict approval procedures to ensure that exceptions are properly evaluated and authorized. تطبيق إجراءات موافقة صارمة لضمان تقييم وتفويض الاستثناءات بشكل صحيح.

Examples: Requiring multiple levels of approval for high-risk exceptions to ensure thorough evaluation. طلب مستويات متعددة من الموافقات على الاستثناءات العالية الخطورة لضمان التقييم الشامل.

C. Regular Review of Exceptions / المراجعة الدورية للاستثناءات

Conducting regular reviews of granted exceptions to ensure they remain necessary and justified. إجراء مراجعات دورية للاستثناءات الممنوحة لضمان بقائها ضرورية ومبررة.

Examples: Reviewing exceptions annually to determine if they are still needed and if they pose any new risks. مراجعة الاستثناءات سنويًا لتحديد ما إذا كانت لا تزال ضرورية وإذا كانت تشكل أي مخاطر جديدة.

4.3 Ethical Disclosure / الإفصاح الأخلاقي

Ethical disclosure involves the responsible reporting of security vulnerabilities and incidents to appropriate parties. يشمل الإفصاح الأخلاقي الإبلاغ المسؤول عن الثغرات الأمنية والحوادث للأطراف المناسبة.

Purpose: To promote transparency, accountability, and the timely mitigation of security risks. لتعزيز الشفافية والمساءلة والتخفيف في الوقت المناسب من المخاطر الأمنية.

4.3.1 Components / المكونات

A. Reporting Mechanism / آلية الإبلاغ

Establishing a formal mechanism for reporting security vulnerabilities and incidents. إنشاء آلية رسمية للإبلاغ عن الثغرات والحوادث الأمنية.

Examples: Creating a dedicated email address or online portal for reporting security issues. إنشاء عنوان بريد إلكتروني مخصص أو بوابة إلكترونية للإبلاغ عن المشكلات الأمنية.

B. Disclosure Policies / سياسات الإفصاح

Developing policies that outline the process for disclosing security vulnerabilities

and incidents. تطوير سياسات تحدد عملية الإفصاح عن الثغرات والحوادث الأمنية.

Examples: Creating a policy that specifies how, when, and to whom security vulnerabilities should be reported. إنشاء سياسة تحدد كيفية وموعد ولمن يجب الإبلاغ عن الثغرات الأمنية.

C. Coordination with Stakeholders / التنسيق مع أصحاب المصلحة

Coordinating with relevant stakeholders, including customers, partners, and regulatory bodies, to ensure effective communication and resolution of security issues. التنسيق مع أصحاب المصلحة المعنيين، بما في ذلك العملاء والشركاء والهيئات التنظيمية، لضمان التواصل الفعال وحل القضايا الأمنية.

Examples: Notifying affected customers of a security breach and coordinating with regulatory bodies to comply with reporting requirements. إبلاغ العملاء المتأثرين بخرق أمني والتنسيق مع الهيئات التنظيمية للامتثال لمتطلبات الإبلاغ.

4.3.2 Best Practices / أفضل الممارسات

A. Establishing Clear Disclosure Guidelines / وضع إرشادات واضحة للإفصاح

Creating clear guidelines for the responsible disclosure of security vulnerabilities and incidents. وضع إرشادات واضحة للإفصاح المسؤول عن الثغرات والحوادث الأمنية.

Examples: Developing a disclosure policy that outlines the steps for reporting and addressing security issues. تطوير سياسة إفصاح تحدد الخطوات للإبلاغ عن القضايا الأمنية ومعالجتها.

B. Ensuring Confidentiality and Integrity / ضمان السرية والنزاهة

Protecting the confidentiality and integrity of reported security vulnerabilities and incidents. حماية سرية ونزاهة الثغرات والحوادث الأمنية المبلغ عنها.

Examples: Implementing secure communication channels for reporting security issues to ensure the information is protected. تطبيق قنوات اتصال آمنة للإبلاغ عن القضايا الأمنية لضمان حماية المعلومات.

C. Promoting Responsible Reporting / تشجيع الإبلاغ المسؤول

Encouraging employees and stakeholders to report security vulnerabilities and incidents responsibly. تشجيع الموظفين وأصحاب المصلحة على الإبلاغ عن الثغرات

والحوادث الأمنية بشكل مسؤول.

Examples: Providing training on the importance of responsible reporting and the proper channels for reporting security issues. تقديم التدريب حول أهمية الإبلاغ المسؤول والقنوات المناسبة للإبلاغ عن القضايا الأمنية.

Multiple Choice Questions:

1. What is the primary purpose of analyzing test output and generating reports?

a. To conduct vulnerability assessments

b. To evaluate the effectiveness of security measures and provide recommendations for improvement

c. To create new security policies

d. To manage user accounts

2. What is remediation in the context of security testing?

a. Creating new backups

b. Taking corrective actions to fix identified vulnerabilities and weaknesses

c. Conducting security audits

d. Training employees

3. Why is exception handling important?

a. To document and manage deviations from standard procedures or policies

b. To create new security policies

c. To test backup restores

d. To educate employees about security policies

4. What is the purpose of ethical disclosure?

a. To train employees

b. To responsibly report security vulnerabilities and incidents to appropriate parties

c. To conduct internal audits

d. To ensure data backups are complete

5. What are some examples of remediation actions?

a. Documenting security policies

b. Applying patches to fix software vulnerabilities and updating security configurations

c. Conducting security training sessions

d. Managing user accounts

Answers and Explanation:

1. b. To evaluate the effectiveness of security measures and provide recommendations for improvement

Explanation: Analyzing test output and generating reports help evaluate the effectiveness of security measures and provide actionable recommendations for improvement.يساعد تحليل نتائج الاختبار وإنشاء التقارير في تقييم فعالية التدابير الأمنية وتقديم توصيات قابلة للتنفيذ للتحسين

2. b. Taking corrective actions to fix identified vulnerabilities and weaknesses

Explanation: Remediation involves taking corrective actions to address identified vulnerabilities and weaknesses in an organization's systems and processes.يشمل الإصلاح اتخاذ إجراءات تصحيحية لمعالجة الثغرات ونقاط الضعف المحددة في أنظمة وعمليات المؤسسة

3. a. To document and manage deviations from standard procedures or policies

Explanation: Exception handling is important to document and manage deviations from standard procedures or policies due to special circumstances.التعامل مع الاستثناءات مهم لتوثيق وإدارة الانحرافات عن الإجراءات أو السياسات القياسية بسبب ظروف خاصة

4. b. To responsibly report security vulnerabilities and incidents to appropriate parties

Explanation: Ethical disclosure involves responsibly reporting security vulnerabilities and incidents to affected organizations and relevant authorities.يشمل الإفصاح الأخلاقي الإبلاغ المسؤول عن الثغرات والحوادث الأمنية للمؤسسات المتأثرة والسلطات ذات الصلة

5. b. Applying patches to fix software vulnerabilities and updating security configurations

Explanation: Remediation actions include applying patches to fix software vulnerabilities and updating security configurations to strengthen defenses.تشمل إجراءات الإصلاح تطبيق التصحيحات لإصلاح الثغرات البرمجية وتحديث تكوينات الأمان لتعزيز الدفاعات

---

5. Facilitate Incident Handling / تسهيل التعامل مع الحوادث

Facilitating incident handling involves managing and responding to security incidents to minimize impact and restore normal operations. يشمل تسهيل التعامل مع الحوادث إدارة والاستجابة للحوادث الأمنية لتقليل التأثير واستعادة العمليات الطبيعية.

Purpose: To effectively respond to security incidents, mitigate risks, and prevent future incidents. للاستجابة بفعالية للحوادث الأمنية، وتخفيف المخاطر، ومنع الحوادث المستقبلية.

5.1 Incident Response Plan / خطة الاستجابة للحوادث

An incident response plan is a documented strategy for identifying, managing, and responding to security incidents. تشمل خطة الاستجابة للحوادث استراتيجية موثقة لتحديد وإدارة والاستجابة للحوادث الأمنية.

Purpose: To ensure a structured and effective response to security incidents, minimizing damage and recovery time. لضمان استجابة منظمة وفعالة للحوادث الأمنية، وتقليل الأضرار ووقت الاستعادة.

5.1.1 Components / المكونات

A. Incident Identification / تحديد الحوادث

The process of detecting and recognizing security incidents through monitoring and alerts. عملية اكتشاف والتعرف على الحوادث الأمنية من خلال المراقبة والتنبيهات.

Examples: Using intrusion detection systems (IDS) and security information and event management (SIEM) tools to identify potential incidents. استخدام أنظمة كشف التسلل وأدوات إدارة معلومات وأحداث الأمان لتحديد الحوادث المحتملة.

B. Incident Classification / تصنيف الحوادث

Categorizing security incidents based on their severity, impact, and urgency to prioritize response efforts. تصنيف الحوادث الأمنية بناءً على شدتها وتأثيرها وعاجليتها لإعطاء الأولوية لجهود الاستجابة.

Examples: Classifying incidents into categories such as critical, high, medium, and low based on their potential impact on operations. تصنيف الحوادث إلى فئات مثل حرجة، عالية، متوسطة، ومنخفضة بناءً على تأثيرها المحتمل على العمليات.

C. Response Procedures / إجراءات الاستجابة

Documented steps and actions to be taken in response to specific types of security incidents. خطوات وإجراءات موثقة لاتخاذها في الاستجابة لأنواع محددة من الحوادث الأمنية.

Examples: Developing response procedures for different types of incidents, such as malware infections, data breaches, and DDoS attacks. تطوير إجراءات الاستجابة لأنواع مختلفة من الحوادث، مثل إصابات البرمجيات الخبيثة، اختراقات البيانات، وهجمات

5.1.2 Best Practices / أفضل الممارسات

A. Regular Plan Updates / تحديثات الخطة المنتظمة

Regularly reviewing and updating the incident response plan to ensure it remains effective and relevant. مراجعة وتحديث خطة الاستجابة للحوادث بانتظام لضمان بقائها فعالة وذات صلة.

Examples: Updating the incident response plan annually to incorporate lessons learned from past incidents and changes in the threat landscape. تحديث خطة الاستجابة للحوادث سنويًا لتضمين الدروس المستفادة من الحوادث السابقة والتغييرات في مشهد التهديدات.

B. Incident Response Training / تدريب الاستجابة للحوادث

Providing regular training for the incident response team to ensure they are prepared to handle security incidents. توفير التدريب المنتظم لفريق الاستجابة للحوادث لضمان استعدادهم للتعامل مع الحوادث الأمنية.

Examples: Conducting incident response drills and tabletop exercises to train the team on handling different types of incidents. إجراء تدريبات الاستجابة للحوادث وتمارين الطاولة لتدريب الفريق على التعامل مع أنواع مختلفة من الحوادث.

C. Collaboration with External Entities / التعاون مع الكيانات الخارجية

Coordinating with external entities, such as law enforcement, regulatory bodies, and security vendors, during incident response. التنسيق مع الكيانات الخارجية، مثل إنفاذ القانون، الهيئات التنظيمية، ومزودي الأمن، أثناء الاستجابة للحوادث.

Examples: Collaborating with law enforcement to investigate a major security breach and coordinating with security vendors for threat intelligence. التعاون مع إنفاذ القانون للتحقيق في خرق أمني كبير والتنسيق مع مزودي الأمن للحصول على استخبارات التهديدات.

5.2 Incident Mitigation / التخفيف من الحوادث

Incident mitigation involves taking actions to contain and reduce the impact of a security incident. يشمل التخفيف من الحوادث اتخاذ إجراءات لاحتواء وتقليل تأثير الحادث الأمني.

Purpose: To minimize the damage caused by security incidents and prevent them from spreading. لتقليل الأضرار الناجمة عن الحوادث الأمنية ومنع انتشارها.

5.2.1 Components / المكونات

A. Containment Strategies / استراتيجيات الاحتواء

Methods and techniques used to isolate and contain security incidents to prevent further damage. الأساليب والتقنيات المستخدمة لعزل واحتواء الحوادث الأمنية لمنع المزيد من الأضرار.

Examples: Isolating infected systems from the network to prevent malware from spreading. عزل الأنظمة المصابة عن الشبكة لمنع انتشار البرمجيات الخبيثة.

B. Eradication Procedures / إجراءات الإزالة

Steps to remove the root cause of a security incident and eliminate its presence from the affected systems. خطوات لإزالة السبب الجذري للحادث الأمني والقضاء على وجوده في الأنظمة المتأثرة.

Examples: Removing malware from infected systems and closing security gaps that allowed the incident to occur. إزالة البرمجيات الخبيثة من الأنظمة المصابة وإغلاق الثغرات الأمنية التي سمحت بحدوث الحادث.

C. Recovery Processes / عمليات الاستعادة

Steps to restore normal operations and recover data and systems to their pre-incident state. خطوات لاستعادة العمليات الطبيعية واستعادة البيانات والأنظمة إلى حالتها قبل الحادث.

Examples: Restoring data from backups and rebuilding systems to a known good state after a security incident. استعادة البيانات من النسخ الاحتياطية وإعادة بناء الأنظمة إلى حالة جيدة معروفة بعد الحادث الأمني.

5.2.2 Best Practices / أفضل الممارسات

A. Comprehensive Mitigation Plans / خطط التخفيف الشاملة

Developing detailed mitigation plans that outline the steps to be taken during

different types of security incidents. تطوير خطط تخفيف شاملة تحدد الخطوات الواجب اتخاذها أثناء أنواع مختلفة من الحوادث الأمنية.

Examples: Creating mitigation plans for various scenarios, such as ransomware attacks, data breaches, and insider threats. إنشاء خطط تخفيف لسيناريوهات مختلفة، مثل هجمات الفدية، اختراقات البيانات، والتهديدات الداخلية.

B. Regular Testing and Drills / الاختبارات والتدريبات المنتظمة

Regularly testing and conducting drills to ensure that mitigation plans are effective and that the team is prepared. اختبار وإجراء تدريبات بانتظام لضمان فعالية خطط التخفيف واستعداد الفريق.

Examples: Conducting regular drills to test the effectiveness of containment and eradication procedures. إجراء تدريبات منتظمة لاختبار فعالية إجراءات الاحتواء والإزالة.

C. Collaboration and Communication / التعاون والتواصل

Ensuring effective collaboration and communication between different teams and stakeholders during incident mitigation. ضمان التعاون والتواصل الفعال بين الفرق المختلفة وأصحاب المصلحة أثناء التخفيف من الحوادث.

Examples: Facilitating communication between the incident response team, IT department, and management during an incident. تسهيل التواصل بين فريق الاستجابة للحوادث، وقسم تكنولوجيا المعلومات، والإدارة أثناء الحادث.

Multiple Choice Questions:

1. What is the primary purpose of conducting security audits?

a. To create new security policies

b. To evaluate an organization's security posture and ensure compliance with standards

c. To manage user accounts

d. To monitor network traffic

2. What is an internal audit?

a. An audit conducted by independent third parties

b. An audit conducted by the organization itself to evaluate its own security controls

c. An audit conducted on vendors and partners

d. An audit conducted by regulatory authorities

3. Why are external audits important?

a. To provide an unbiased evaluation of the organization's security posture

b. To manage internal security controls

c. To create new security policies

d. To monitor user activity

4. What is the focus of third-party audits?

a. Evaluating internal security controls

b. Assessing the security measures of vendors and partners

c. Managing on-premise security infrastructure

d. Monitoring cloud-based services

5. What are some examples of internal audit activities?

a. Hiring external auditors

b. Conducting internal reviews of security policies, procedures, and incident response plans

c. Performing security assessments on vendors

d. Conducting security awareness training sessions

Answers and Explanation:

1. b. To evaluate an organization's security posture and ensure compliance with standards

Explanation: The primary purpose of conducting security audits is to evaluate an organization's security posture and ensure compliance with security policies, standards, and regulatory requirements.الهدف الرئيسي من إجراء التدقيقات الأمنية هو تقييم الوضع الأمني للمؤسسة وضمان الامتثال للسياسات والمعايير الأمنية والمتطلبات التنظيمية

2. b. An audit conducted by the organization itself to evaluate its own security controls

Explanation: Internal audits are conducted by the organization itself to evaluate its own security controls and processes.تُجرى التدقيقات الداخلية من قبل المؤسسة نفسها لتقييم ضوابطها وعملياتها الأمنية

3. a. To provide an unbiased evaluation of the organization's security posture

Explanation: External audits are important because they provide an unbiased evaluation of the organization's security posture, helping to ensure objectivity and compliance with industry standards.التدقيقات الخارجية مهمة لأنها توفر تقييمًا غير متحيز للوضع الأمني للمؤسسة، مما يساعد على ضمان الموضوعية والامتثال لمعايير الصناعة

4. b. Assessing the security measures of vendors and partners

Explanation: Third-party audits focus on assessing the security measures of vendors and partners to ensure they meet the organization's standards and do not introduce risks.تركز التدقيقات للأطراف الثالثة على تقييم التدابير الأمنية للبائعين والشركاء لضمان تلبيتها لمعايير المؤسسة وعدم تقديم مخاطر

5. b. Conducting internal reviews of security policies, procedures, and incident response plans

Explanation: Internal audit activities include conducting internal reviews of security policies, procedures, and incident response plans to ensure compliance and identify areas for improvement.تشمل أنشطة التدقيق الداخلية إجراء مراجعات داخلية للسياسات والإجراءات الأمنية وخطط الاستجابة للحوادث لضمان الامتثال وتحديد مجالات التحسين

6. Reporting and Documentation / الإبلاغ والتوثيق

Reporting and documentation involve creating detailed records of security activities, incidents, and responses. يشمل الإبلاغ والتوثيق إنشاء سجلات مفصلة للأنشطة الأمنية والحوادث والاستجابات.

Purpose: To ensure transparency, accountability, and continuous improvement in security practices. لضمان الشفافية والمساءلة والتحسين المستمر في الممارسات الأمنية.

6.1 Incident Reporting / الإبلاغ عن الحوادث

Incident reporting involves documenting security incidents and communicating them to relevant stakeholders. يشمل الإبلاغ عن الحوادث توثيق الحوادث الأمنية وإبلاغها إلى أصحاب المصلحة المعنيين.

Purpose: To ensure that security incidents are properly documented, communicated, and addressed. لضمان توثيق الحوادث الأمنية وإبلاغها ومعالجتها بشكل صحيح.

6.1.1 Components / المكونات

A. Incident Reporting Procedures / إجراءات الإبلاغ عن الحوادث

Establishing formal procedures for reporting security incidents to ensure consistency and thorough documentation. إنشاء إجراءات رسمية للإبلاغ عن الحوادث الأمنية لضمان الاتساق والتوثيق الشامل.

Examples: Creating a standardized incident report template and defining the steps for reporting incidents. إنشاء قالب تقرير حادث معياري وتحديد الخطوات للإبلاغ عن الحوادث.

B. Incident Tracking Systems / أنظمة تتبع الحوادث

Implementing systems to track and manage security incidents from detection to resolution. تطبيق أنظمة لتتبع وإدارة الحوادث الأمنية من الاكتشاف إلى الحل.

Examples: Using an incident tracking system to log incidents, track their status, and document the resolution process. استخدام نظام تتبع الحوادث لتسجيل الحوادث وتتبع حالتها وتوثيق عملية الحل.

C. Communication Protocols / بروتوكولات الاتصال

Defining protocols for communicating security incidents to relevant stakeholders, including management and external entities. تحديد بروتوكولات لإبلاغ الحوادث الأمنية إلى أصحاب المصلحة المعنيين، بما في ذلك الإدارة والكيانات الخارجية.

Examples: Establishing communication protocols for notifying management, legal, and regulatory bodies about significant security incidents. إنشاء بروتوكولات الاتصال لإبلاغ الإدارة والجهات القانونية والتنظيمية عن الحوادث الأمنية الهامة.

6.1.2 Best Practices / أفضل الممارسات

A. Detailed and Accurate Reporting / الإبلاغ المفصل والدقيق

Ensuring that incident reports are detailed, accurate, and include all relevant information. ضمان أن تكون تقارير الحوادث مفصلة ودقيقة وتشمل جميع المعلومات ذات الصلة.

Examples: Including detailed descriptions of the incident, actions taken, and the final resolution in incident reports. تضمين أوصاف مفصلة للحادث، والإجراءات المتخذة، والحل النهائي في تقارير الحوادث.

B. Timely Reporting / الإبلاغ في الوقت المناسب

Reporting security incidents promptly to ensure timely communication and response. الإبلاغ عن الحوادث الأمنية على الفور لضمان التواصل والاستجابة في الوقت المناسب.

Examples: Implementing procedures that require incidents to be reported within a specified time frame, such as within 24 hours of detection. تطبيق إجراءات تتطلب الإبلاغ عن الحوادث خلال إطار زمني محدد، مثل 24 ساعة من الاكتشاف.

C. Confidentiality of Reports / سرية التقارير

Ensuring the confidentiality of incident reports to protect sensitive information and maintain trust. ضمان سرية تقارير الحوادث لحماية المعلومات الحساسة والحفاظ على الثقة.

Examples: Using secure systems for storing and sharing incident reports to prevent unauthorized access. استخدام أنظمة آمنة لتخزين ومشاركة تقارير الحوادث لمنع الوصول غير المصرح به.

6.2 Post-Incident Analysis / تحليل ما بعد الحوادث

Post-incident analysis involves reviewing and analyzing security incidents to identify lessons learned and improve future responses. يشمل تحليل ما بعد الحوادث مراجعة وتحليل الحوادث الأمنية لتحديد الدروس المستفادة وتحسين الاستجابات المستقبلية.

Purpose: To identify root causes, improve incident response procedures, and prevent future incidents. لتحديد الأسباب الجذرية، وتحسين إجراءات الاستجابة للحوادث، ومنع الحوادث المستقبلية.

6.2.1 Components / المكونات

A. Incident Debriefings / جلسات مناقشة الحوادث

Conducting debriefing sessions with incident response teams to review the incident and response efforts. إجراء جلسات مناقشة مع فرق الاستجابة للحوادث لمراجعة الحادث وجهود الاستجابة.

Examples: Holding debriefing meetings after significant incidents to discuss what happened, what worked, and what could be improved. عقد اجتماعات مناقشة بعد الحوادث الكبيرة لمناقشة ما حدث، وما نجح، وما يمكن تحسينه.

الأفكار والتغذية الراجعة من فريق الاستجابة وتحديد مجالات التحسين.

B. Root Cause Analysis / تحليل السبب الجذري

Investigating the underlying causes of security incidents to understand how and why they occurred. التحقيق في الأسباب الجذرية للحوادث الأمنية لفهم كيفية ولماذا حدثت.

Examples: Conducting root cause analysis to identify vulnerabilities or process failures that contributed to a security incident. إجراء تحليل السبب الجذري لتحديد الثغرات أو إخفاقات العمليات التي ساهمت في الحادث الأمني.

C. Lessons Learned Documentation / توثيق الدروس المستفادة

Documenting lessons learned from security incidents to improve future incident response efforts. توثيق الدروس المستفادة من الحوادث الأمنية لتحسين جهود الاستجابة للحوادث المستقبلية.

Examples: Creating a lessons learned report that summarizes key findings and

recommendations for improving incident response. إنشاء تقرير الدروس المستفادة يلخص النتائج الرئيسية والتوصيات لتحسين الاستجابة للحوادث.

6.2.2 Best Practices / أفضل الممارسات

A. Comprehensive Analysis / التحليل الشامل

Conducting a thorough and comprehensive analysis of security incidents to understand all contributing factors. إجراء تحليل شامل للحوادث الأمنية لفهم جميع العوامل المساهمة.

Examples: Reviewing all aspects of an incident, including technical, procedural, and human factors, to gain a complete understanding. مراجعة جميع جوانب الحادث، بما في ذلك العوامل التقنية والإجرائية والبشرية، للحصول على فهم كامل.

B. Regular Review and Updates / المراجعة والتحديثات المنتظمة

Regularly reviewing and updating post-incident analysis procedures to ensure they remain effective and relevant. مراجعة وتحديث إجراءات تحليل ما بعد الحوادث بانتظام لضمان بقائها فعالة وذات صلة.

Examples: Updating analysis procedures annually to incorporate new methodologies and address changes in the threat landscape. تحديث إجراءات التحليل سنويًا لتضمين منهجيات جديدة ومعالجة التغييرات في مشهد التهديدات.

C. Sharing Findings and Recommendations / مشاركة النتائج والتوصيات

Sharing findings and recommendations from post-incident analysis with relevant stakeholders to promote transparency and improvement. مشاركة النتائج والتوصيات من تحليل ما بعد الحوادث مع أصحاب المصلحة المعنيين لتعزيز الشفافية والتحسين.

Examples: Providing regular reports to management and other stakeholders summarizing key findings and recommended actions. تقديم تقارير منتظمة للإدارة وأصحاب المصلحة الآخرين تلخص النتائج الرئيسية والإجراءات الموصى بها.

Multiple Choice Questions:

1. What is the primary purpose of vulnerability scanning?

a. To conduct security audits

b. To identify known vulnerabilities in systems and applications

c. To train employees

d. To manage user accounts

2. What is penetration testing?

a. Creating new security policies

b. Simulating cyber-attacks to identify vulnerabilities

c. Conducting internal audits

d. Managing network infrastructure

3. Why are security audits important?

a. To document user activity

b. To evaluate and ensure compliance with security policies, procedures, and controls

c. To train employees on security policies

d. To manage cloud-based services

4. What is the purpose of code review in security assessments?

a. To create new user accounts

b. To identify security vulnerabilities in source code and ensure best practices are followed

c. To conduct penetration testing

d. To simulate real-world attack scenarios

5. What are some examples of vulnerability scanning tools?

a. SonarQube and Checkmarx

b. Nessus, OpenVAS, and Qualys

c. Nessus and Red Team exercises

d. Qualys and Ethical Hacking

Answers and Explanation:

1. b. To identify known vulnerabilities in systems and applications

Explanation: Vulnerability scanning involves using automated tools to identify known vulnerabilities in systems and applications.يشمل مسح الثغرات الأمنية استخدام أدوات آلية لتحديد الثغرات المعروفة في الأنظمة والتطبيقات

2. b. Simulating cyber-attacks to identify vulnerabilities

Explanation: Penetration testing involves simulating cyber-attacks to identify vulnerabilities that could be exploited by attackers.يشمل اختبار الاختراق محاكاة الهجمات الإلكترونية لتحديد الثغرات التي يمكن أن يستغلها المهاجمون

3. b. To evaluate and ensure compliance with security policies, procedures, and controls

Explanation: Security audits are important because they evaluate and ensure compliance with security policies, procedures, and controls.التدقيقات الأمنية مهمة لأنها تقيّم وتضمن الامتثال للسياسات والإجراءات والضوابط الأمنية

4. b. To identify security vulnerabilities in source code and ensure best practices are followed

Explanation: Code review in security assessments involves examining source code to identify vulnerabilities and ensure best practices are followed.يشمل مراجعة الشيفرة

البرمجية في التقييمات الأمنية فحص الشيفرة المصدرية لتحديد الثغرات الأمنية وضمان اتباع أفضل الممارسات

5. b. Nessus, OpenVAS, and Qualys

Explanation: Vulnerability scanning tools include Nessus, OpenVAS, and Qualys.تشمل أدوات مسح الثغرات الأمنية

Conclusion / الخاتمة

Security assessment and testing are crucial components of a robust cybersecurity strategy. By designing and validating assessment, test, and audit strategies, organizations can identify and mitigate vulnerabilities, ensure compliance, and improve their overall security posture. Conducting thorough security controls testing, collecting and analyzing security process data, and facilitating effective incident handling and recovery processes are essential for maintaining the integrity, confidentiality, and availability of systems and data. Regular reviews, updates, and continuous improvement efforts help organizations stay ahead of evolving threats and ensure a proactive approach to security management.

تعد تقييمات الأمان والاختبار مكونات أساسية لاستراتيجية قوية للأمن السيبراني من خلال تصميم وتأكيد استراتيجيات التقييم والاختبار والتدقيق يمكن للمؤسسات تحديد وتخفيف الثغرات وضمان الامتثال وتحسين وضعها الأمني العام يعد إجراء اختبارات شاملة للتحكم في الأمان وجمع وتحليل بيانات عمليات الأمان وتسهيل التعامل الفعال مع الحوادث وعمليات الاستعادة أمورًا ضرورية للحفاظ على سلامة وسرية وتوافر الأنظمة والبيانات تساعد المراجعات المنتظمة والتحديثات والجهود المستمرة للتحسين المؤسسات على البقاء في طليعة التهديدات المتطورة وضمان نهج استباقي لإدارة الأمان

Omar Abdelqawey 3w

Telecom/Information Security Principal Consultant, ISO 27001 LA ,CRISC,Risk & Compliance and signalling firewall ...

جزاك الله خيرا

و جعله علما صالحا يُنتفع به
و اثر صالحا لك في الدنيا و الاخرة

Like · Reply | 1 Reaction

Creds 3w

Lovely to see! Great share. Keep going. Keep coding. We are cheering you on along the way! 🥳 🎉

Like · Reply | 1 Reaction

Musab Khalifa 4w
Cybersecurity Engineer | 6xCompTIA Sec+, CySA+, Pen Test+, CNSP , CNVP, CSAP | CCNP | 3xFortinet NSE4, FCA, ...

جزاك الله خيرا

Like · Reply | 1 Reaction

Wala Suliman 4w
CISSP, CISM, CRISC, PMP, eCTHPv2, CASP+, Pentest+, Security+, CCSKv5, ITIL, COBIT, ISO27K, AWSx2, AZ-500

جزاك الله خيراً ونفع بك

Like · Reply | 1 Reaction

See more comments

More articles by this author

Module 7: Security Operations / إدارة عمليات...
Aug 5, 2024

CISSP Module 5: Identity and Access Management...
Jul 8, 2024

CISSP Module 4: Communication and...
Jul 1, 2024

See all

Insights from the community

Security Testing

What are the main steps and deliverables of a security testing plan?

Threat & Vulnerability Management

How do you document and track the remediation of the vulnerabilities you identify?

Information Security Management

What are the most effective ISM frameworks and standards to follow in your industry?

Cybersecurity

What are the different types of security testing?

Cybersecurity

What are the common limitations of security testing?

Incident Response

How do you stay informed about the latest patches and vulnerabilities?

Show more

Others also viewed

How to achieve a high quality information security assessment?

Alex Feng · 6y

ISO/IEC 27001 Information Security Management

Samir Abu Tahoun, Ph.D · 9y

Planning for Information Security Testing—A Practical Approach

Karina K. · 7y

Propel Your Career with an IBITGQ ISO 27001 Qualification

IBITGQ · 2mo

ICS-CERT Advisory Dashboard Summary for April 11 - 15, 2022

Dan Ricci · 2y

Incident Response and Security Operations on the Move

Prof Bill Buchanan OBE FRSE · 6y

Show more

Explore topics

Sales

Marketing

Business Administration

HR Management

Content Management

Engineering

Soft Skills

See All

إدارة عمليات الامن السيبراني
Security Assessment and Testing

Emad M. Abdelhamid • 2nd
Technical Leader | SME IT Security Design @ Cisco - CX EMEA . ...
View my portfolio
+ Follow
3w • Edited •

السلام عليكم ورحمة الله وبركاته
اليوم بإذن الله سنقوم بشرح مختصر لفصل هو الأهم في الجانب العملي لشهادة ال CISSP
وهو الفصل السابع والذى يتحدث عن إدارة عمليات الامن السيبراني حيث يغطي هذا الفصل مبادئ وممارسات عمليات الأمن السيبرانى ويركز على فهم وتنفيذ عمليات الأمان الفعالة، وإدارة الحوادث الأمنية، وضمان المراقبة المستمرة وتحسين التدابير الأمنية.
الهدف هو تزويد المحترفين بالمعرفة والمهارات اللازمة للحفاظ على الوضع الأمني لمؤسساتهم وتعزيزه

ويحتوى على 15 جزء

1. فهم والامتثال للتحقيقات Understand and Comply with Investigations.
2. إجراء أنشطة التسجيل والمراقبة Conduct Logging and Monitoring Activities.
3. أداء إدارة التكوين Perform Configuration Management (CM).
4. تطبيق مفاهيم عمليات الأمان الأساسية Apply Foundational Security Operations Concepts.
5. تطبيق حماية الموارد Apply Resource Protection.
6. إجراء إدارة الحوادث Conduct Incident Management.
7. تشغيل وصيانة إجراءات الكشف والوقاية Operate and Maintain Detection and Preventative Measures.
8. تنفيذ ودعم إدارة التصحيحات والثغرات Implement and Support Patch and Vulnerability Management.
9. فهم والمشاركة في عمليات إدارة التغيير Understand and Participate in Change Management Processes.
10. تنفيذ استراتيجيات التعافي Implement Recovery Strategies.
11. تنفيذ عمليات التعافي من الكوارث Implement Disaster Recovery (DR) Processes.
12. اختبار خطة التعافي من الكوارث Test Disaster Recovery Plan (DRP).
13. المشاركة في تخطيط واستمرار الأعمال والتدريبات Participate in Business Continuity (BC) Planning and Exercises.
14. تنفيذ وإدارة الأمن المادي Implement and Manage Physical Security.
15. معالجة مخاوف الأمان والسلامة للموظفين Address Personnel Safety and Security Concerns.

المقالات

For Module 1 : https://lnkd.in/dkkyFGdW
For Module 2 : https://lnkd.in/dNUWhiJs
For Module 3: https://lnkd.in/dsqBXhEc
For Module 4: https://lnkd.in/d_DBAm4h
For Module 5: https://lnkd.in/dGPDeKWF
For Module 6: https://lnkd.in/dZHHJKJx
For Module 7: https://lnkd.in/d_JswW5W
For Module 8: https://lnkd.in/dQsQHqgR

Resources - المصادر

1- Official (ISC)² CISSP Study Guide
2- CISSP (ISC)² Official Practice Tests
3- CISSP All-in-One Exam Guide by Shon Harris
4- Cybrary – CISSP Training by Kelly Handerhan https://lnkd.in/d4zrAkJz
5- Oreilly – CISSP Training by Sari Greene https://lnkd.in/dANS-hVc.
6- CISSP bundles by Thor Pedersen https://lnkd.in/d2tpqaJk
7- CISSP MindMaps YouTube Playlist from Destination Certification https://lnkd.in/deJM44xX

Emad M. Abdelhamid's Post

Emad M. Abdelhamid
Technical Leader | SME IT Security Design @ Cisco - CX EMEA . CCIE#58413 | CCDE#20230008 | CISM®| CISA...
3w · Edited

السلام عليكم ورحمة الله
اليوم بإذن الله سنقوم ب
CISSP
وهو الفصل السابع والذ
عمليات الأمن السيبراني
المستمرة وتحسين التدابي
الهدف هو تزويد المحترفي

صل مبادئ وممارسات
منية، وضمان المراقبة

اتهم وتعزيزه

ويحتوى على 15 جزء

ن الأساسية

1. with Investigations
2. onitoring Activities
3. Management (CM)
4. erations Concepts
5. esource Protection
6. dent Management
7. entative Measures
8. bility Management
9. gement Processes

خراءات الكشف والوقاية
رة التصحيحات والثغرات
ة في عمليات إدارة

التغيير
10. Recovery Strategies
11. very (DR) Processes
12. ecovery Plan (DRP)
13. nning and Exercises

طيط واستمرار الأعمال

والتدريبات
14. Implement and Manage Physical Security تنفيذ وإدارة الأمن المادي
15. Address Personnel Safety and Security Concerns معالجة مخاوف الأمان والسلامة للموظفين

المقالات، بإذن الله، ستكون مقدمة جيدة للتحضير للشهادة. ولكنها غير كافية وتحتاج للتحضير بالتفصيل من المصادر المذكورة في نهاية كل مقال.

These articles, once completed, will serve as a good introduction to preparing for the certification. However, they are not sufficient on their own and will require detailed preparation from the sources mentioned at the end of each article.

تابعونا في المقالات القادمة لاستكمال شرح باقي الفصول، مع مزيد من الأمثلة والأسئلة التوضيحية التي تساعدكم في التحضير للشهادة بشكل أفضل

Follow us in the upcoming articles to complete the explanation of the remaining chapters, with more examples and clarifying questions that will help you better prepare for the CISSP certificate.

For Module 1 : https://lnkd.in/dkkyFGdW
For Module 2 : https://lnkd.in/dNUWhiJs
For Module 3: https://lnkd.in/dsqBXhEc
For Module 4: https://lnkd.in/d_DBAm4h
For Module 5: https://lnkd.in/dGPDeKWF
For Module 6: https://lnkd.in/dZHHJKJx

#CISSP
#Investigations
#EvidenceHandling
#Logging
#Monitoring
#SecurityEvents
#PatchManagement
#VulnerabilityManagement
#IncidentManagement
#IR
#DRP
#BCP
#PhysicalSecurity
#SAISG

Module 7: Security Operations / إدارة عمليات الامن السيبراني
Emad M. Abdelhamid on LinkedIn

116 · 6 Comments

Like Comment Share

Musab Khalifa 3w
Cybersecurity Engineer | 6xCompTIA Sec+, CySA+, Pen Test+, CNSP , CNVP, CSAP | CCNP | 3xFortinet NSE4, ...
جزاك الله خيرا

Like · Reply | 1 Reaction

Wala Suliman 3w
CISSP, CISM, CRISC, PMP, eCTHPv2, CASP+, Pentest+, Security+, CCSKv5, ITIL, COBIT, ISO27K, AWSx2, AZ-500
جزاك الله خيرا ونفع بك

Like · Reply | 1 Reaction

izzeddine mahboub
Network Engineer

3w

بارك الله فيك

Like · Reply | 1 Reaction

See more comments

To view or add a comment, sign in

12,680 followers

307 Posts · 11 Articles

View Profile Follow

More from this author

Module 7: Security Operations / إدارة عمليات الامن السيبراني
Emad M. Abdelhamid · 3w

Module 6: Security Assessment and Testing تقييم الأمان والاختبار
Emad M. Abdelhamid · 1mo

CISSP Module 5: Identity and Access Management (IAM) إدارة الهوية والوصول
Emad M. Abdelhamid · 1mo

Explore topics

Sales

Marketing

Business Administration

HR Management

Content Management

Engineering

Soft Skills

See All

Emad M. Abdelhamid • 2nd
Technical Leader | SME IT Security Design @ Cisco - CX EMEA . ...
View my portfolio
3w • Edited •

+ Follow ...

السلام عليكم ورحمة الله وبركاته
تم بحمد الله انهاء الشرح المختصر للمادة العلمية لشهادة مهندس أمن نظم معلومات معتمد Certified information systems security professional hashtag#CISSP

أسئل الله العظيم ان يكون هذا العمل خالص لوجهه، وادعوا كل من أستفد من المادة العلمية الدعاء ل أمي وأبى بالرحمة .

في هذا المقال قمنا بشرح مختصر للفصل الثامن والأخير من شهادة ال hashtag#CISSP
وهو بعنوان أمن تطوير البرمجيات و يغطي هذا الفصل الجوانب الأساسية لدمج الأمان في عمليات تطوير البرمجيات .
فهم هذه المفاهيم ضروري لضمان إنشاء تطبيقات برمجية آمنة ومرنة .
حيث سيوجهك هذا الفصل خلال دمج الأمان في دورة حياة تطوير البرمجيات وتطبيق ضوابط الأمان وتقييم فعالية أمان البرمجيات وتقييم تأثير الأمان للبرمجيات المكتسبة وأمان قواعد البيانات وتنفيذ إرشادات ومعايير الترميز الآمن.
ويحتوى على سبع أجزاء :
1. Understand and integrate security in the Software Development Life Cycle (SDLC) - فهم ودمج الأمان في دورة حياة تطوير البرمجيات
2. Identify and apply security controls in software development ecosystems - تحديد وتطبيق ضوابط الأمان في بيئات تطوير البرمجيات
3. Assess the effectiveness of software security - تقييم فعالية أمان البرمجيات
4. Assess security impact of acquired software - تقييم تأثير الأمان للبرمجيات المكتسبة
5. Databases Security - أمان قواعد البيانات
6. Define and apply secure coding guidelines and standards - تعريف وتطبيق إرشادات ومعايير الترميز الآمن
7. Application Security Controls - ضوابط أمان التطبيقات

المقالات، بإذن الله مقدمة جيدة للتحضير للشهادة. ولكنها غير كافية وتحتاج للتحضير بالتفصيل من المصادر المذكورة في نهاية كل مقال.

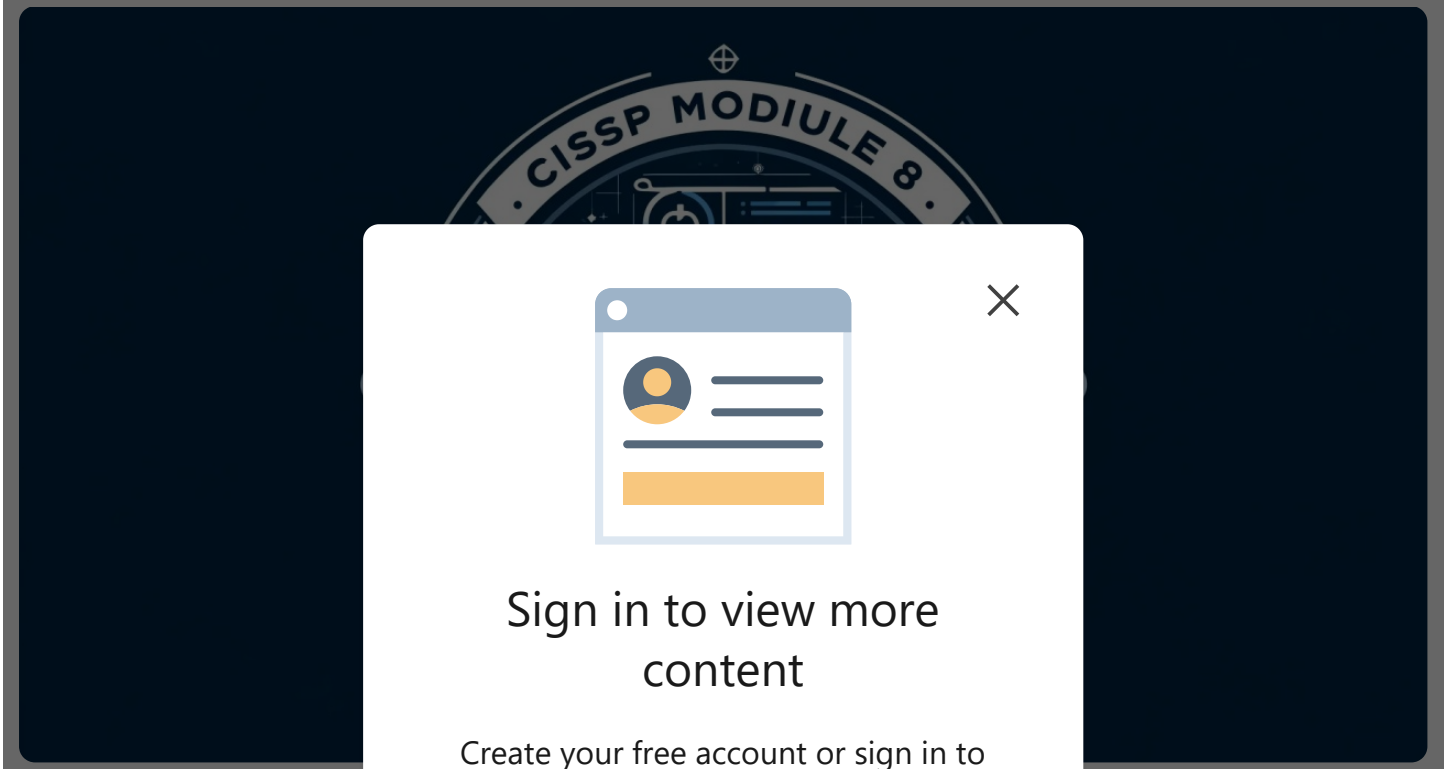
These articles, once completed, will serve as a good introduction to preparing for the certification. However, they are not sufficient on their own and will require detailed preparation from the sources mentioned at the end of each article.

المقالات السابقة

For Module 1 : https://lnkd.in/dkkyFGdW
For Module 2 : https://lnkd.in/dNUWhiJs
For Module 3: https://lnkd.in/dsqBXhEc
For Module 4: https://lnkd.in/d_DBAm4h
For Module 5: https://lnkd.in/dGPDeKWF
For Module 6: https://lnkd.in/dZHHJKJx
For Module 7: https://lnkd.in/d_JswW5W
For Module 8: https://lnkd.in/dQsQHqgR

Resources - المصادر

1- Official (ISC)² CISSP Study Guide
2- CISSP (ISC)² Official Practice Tests
3- CISSP All-in-One Exam Guide by Shon Harris
4- Cybrary – CISSP Training by Kelly Handerhan https://lnkd.in/d4zrAkJz
5- Oreilly – CISSP Training by Sari Greene https://lnkd.in/dANS-hVc.
6- CISSP bundles by Thor Pedersen https://lnkd.in/d2tpqaJk
7- CISSP MindMaps YouTube Playlist from Destination Certification https://lnkd.in/deJM44xX



Module 8: ecurity ... البرمجيات -

Emad M. Ab
Technical Lead
CCIE#58413 | ™ |
ISO27001 LA |
Published Aug

Introduction مقدمة

This module covers essential aspects of integrating security into software development processes.

Understanding these concepts is crucial for ensuring the creation of secure and resilient software applications.

Development Life Cycle (SDLC), the application of security controls, the assessment of software security effectiveness, the evaluation of acquired software's security impact, database security, and the implementation of secure coding guidelines and standards.

تغطي هذه الوحدة الجوانب الأساسية لدمج الأمان في عمليات تطوير البرمجيات

فهم هذه المفاهيم ضروري لضمان إنشاء تطبيقات برمجية آمنة ومرنة

ستوجهك الوحدة خلال دمج الأمان في دورة حياة تطوير البرمجيات وتطبيق ضوابط الأمان وتقييم فعالية أمان البرمجيات وتقييم تأثير الأمان للبرمجيات المكتسبة وأمان قواعد البيانات وتنفيذ إرشادات ومعايير الترميز الآمن

Module Content Brief

1. **Understand and integrate security in the Software Development Life Cycle (SDLC) فهم ودمج الأمان في دورة حياة تطوير البرمجيات**

In this section, you'll explore how to incorporate security measures throughout the Software Development Life Cycle (SDLC), ensuring that security is considered at every phase, from planning and design to implementation, testing, deployment, and maintenance.

في هذا القسم ستستكشف كيفية دمج تدابير الأمان طوال دورة حياة تطوير البرمجيات لضمان مراعاة الأمان في كل مرحلة بدءًا من التخطيط والتصميم وحتى التنفيذ والاختبار والنشر والصيانة

2. **Identify and apply security controls in software development ecosystems تحديد وتطبيق ضوابط الأمان في بيئات تطوير البرمجيات**

This section focuses on identifying, implementing, and managing security controls within software development environments. It includes understanding the various types of security controls and their roles in protecting software during development.

يركز هذا القسم على تحديد وتنفيذ وإدارة ضوابط الأمان داخل بيئات تطوير البرمجيات ويتضمن فهم الأنواع المختلفة من ضوابط الأمان ودورها في حماية البرمجيات أثناء التطوير

3. **Assess the effectiveness of software security تقييم فعالية أمان البرمجيات**

Learn to evaluate the effectiveness of security measures implemented in software

applications. This involves conducting security assessments, code reviews, and vulnerability testing to ensure that security requirements are met.

تعلم كيفية تقييم فعالية التدابير الأمنية التي تم تنفيذها في تطبيقات البرمجيات يشمل ذلك إجراء تقييمات أمنية ومراجعات الكود واختبار الثغرات لضمان تلبية متطلبات الأمان

4. **Assess security impact of acquired software تقييم تأثير الأمان للبرمجيات المكتسبة**

Understand how to assess the security risks associated with acquiring third-party software. This includes evaluating the software's security posture, compliance with industry standards, and potential vulnerabilities.

فهم كيفية تقييم المخاطر الأمنية المرتبطة باكتساب البرمجيات من أطراف ثالثة يشمل ذلك تقييم وضع الأمان في البرمجيات والامتثال للمعايير الصناعية والثغرات المحتملة

5. **Databases Security أمان قواعد البيانات**

This section covers the security measures necessary to protect databases, focusing on data integrity, confidentiality, and availability. You'll learn about database encryption, access controls, and regular security audits.

يغطي هذا القسم التدابير الأمنية اللازمة لحماية قواعد البيانات مع التركيز على سلامة البيانات وسريتها وتوافرها ستتعلم عن تشفير قواعد البيانات وضوابط الوصول والمراجعات الأمنية الدورية

6. **Define and apply secure coding guidelines and standards تعريف وتطبيق إرشادات ومعايير الترميز الآمن**

Explore the best practices for secure coding, including understanding and applying secure coding standards and guidelines to prevent vulnerabilities such as SQL injection, cross-site scripting, and buffer overflows.

استكشف أفضل الممارسات للترميز الآمن بما في ذلك فهم وتطبيق معايير وإرشادات الترميز الآمن لمنع الثغرات مثل حقن SQL والبرمجة النصية عبر المواقع وتجاوزات الذاكرة

7. Application Security Controls ضوابط أمان التطبيقات

Application security controls are measures designed to protect applications from security threats and vulnerabilities. This section discusses various types of controls including authentication, authorization, and input validation to ensure the security of applications.

ضوابط أمان التطبيقات هي تدابير مصممة لحماية التطبيقات من التهديدات الأمنية والثغرات. يناقش هذا القسم أنواعًا مختلفة من الضوابط بما في ذلك التوثيق، التفويض، والتحقق من المدخلات لضمان أمان التطبيقات

---

1. Understand and integrate security in the Software Development Life Cycle (SDLC) فهم ودمج الأمان في دورة حياة تطوير البرمجيات

Security integration in the Software Development Life Cycle (SDLC) is essential to ensure that software is developed with security as a core component. It involves embedding security practices into each phase of the SDLC to protect against threats and vulnerabilities.

يعد دمج الأمان في دورة حياة تطوير البرمجيات أمرًا ضروريًا لضمان تطوير البرمجيات مع اعتبار الأمان مكونًا أساسيًا يتضمن دمج ممارسات الأمان في كل مرحلة من مراحل دورة حياة تطوير البرمجيات للحماية من التهديدات والثغرات

1.1 SDLC Components مكونات دورة حياة تطوير البرمجيات

The SDLC consists of several key phases, each with its own set of security considerations. Understanding these components helps ensure that security is maintained throughout the software development process.

تتكون دورة حياة تطوير البرمجيات من عدة مراحل رئيسية لكل منها مجموعة من اعتبارات الأمان يساهم فهم هذه المكونات في ضمان الحفاظ على الأمان طوال عملية تطوير البرمجيات

1.1.1 Plan & Mgmt. Approval التخطيط والموافقة الإدارية

This phase involves defining the project’s scope, objectives, and budget. It also includes gaining management approval to proceed with the project. Security objectives should be established at this stage to guide the development process.

تشمل هذه المرحلة تحديد نطاق المشروع وأهدافه وميزانيته كما تتضمن الحصول على موافقة الإدارة للبدء في المشروع ينبغي تحديد الأهداف الأمنية في هذه المرحلة لتوجيه عملية التطوير

Example مثال A development team defines security requirements for a new e-commerce platform during the planning phase, ensuring that data protection and compliance are prioritized from the start.

يحدد فريق التطوير متطلبات الأمان لمنصة تجارة إلكترونية جديدة أثناء مرحلة التخطيط لضمان إعطاء الأولوية لحماية البيانات والامتثال منذ البداية

1.1.2 Requirements Gathering جمع المتطلبات

In this phase, the specific needs of the software are identified, including security requirements. This ensures that the software will meet both functional and security needs.

في هذه المرحلة يتم تحديد الاحتياجات المحددة للبرمجيات بما في ذلك متطلبات الأمان يضمن ذلك تلبية البرمجيات للاحتياجات الوظيفية والأمنية على حد سواء

Example مثال Gathering requirements for a healthcare application includes specifying the need for encryption to protect patient data.

يشمل جمع متطلبات تطبيق الرعاية الصحية تحديد الحاجة إلى التشفير لحماية بيانات المرضى

1.1.3 Architecture & Design العمارة والتصميم

During this phase, the overall structure of the software is designed. Security architecture is developed to ensure that the software is built on a secure foundation, incorporating security controls like encryption, authentication, and access controls.

أثناء هذه المرحلة يتم تصميم الهيكل العام للبرمجيات يتم تطوير العمارة الأمنية لضمان بناء البرمجيات على أساس آمن من خلال تضمين ضوابط الأمان مثل التشفير والمصادقة والتحكم في الوصول

Example مثال Designing a secure architecture for an online banking system includes implementing multi-factor authentication and secure data storage.

يتضمن تصميم عمارة آمنة لنظام مصرفي عبر الإنترنت تنفيذ المصادقة متعددة العوامل وتخزين البيانات بشكل آمن

1.1.4 Development التطوير

In the development phase, the actual coding of the software takes place. Secure coding practices must be followed to prevent introducing vulnerabilities into the

software.

في مرحلة التطوير يتم كتابة الكود الفعلي للبرمجيات يجب اتباع ممارسات الترميز الآمن لمنع إدخال الثغرات في البرمجيات

Example مثال Developers implement input validation in a web application to prevent SQL injection attacks.

ينفذ المطورون التحقق من صحة الإدخال في تطبيق ويب لمنع هجمات حقن

1.1.5 Testing الاختبار

Testing involves evaluating the software to identify and fix security vulnerabilities. This includes both manual and automated testing methods such as penetration testing, code reviews, and security scans.

يشمل الاختبار تقييم البرمجيات لتحديد وإصلاح الثغرات الأمنية يتضمن ذلك أساليب الاختبار اليدوية والآلية مثل اختبار الاختراق ومراجعات الكود والفحوصات الأمنية

Example مثال A security team performs penetration testing on a newly developed mobile application to identify vulnerabilities before the application is released to users.

يقوم فريق الأمان بإجراء اختبار اختراق لتطبيق جوال تم تطويره حديثًا لتحديد الثغرات قبل طرح التطبيق للمستخدمين

1.1.6 Deployment النشر

During deployment, the software is released to the production environment. Security measures include configuring firewalls, applying security patches, and monitoring the environment for any unusual activity.

أثناء النشر يتم طرح البرمجيات في بيئة الإنتاج تشمل التدابير الأمنية تكوين الجدران النارية وتطبيق التصحيحات الأمنية ومراقبة البيئة لأي نشاط غير عادي

Example مثال Deploying an online banking system with firewall rules to block unauthorized access and monitoring tools to detect potential intrusions.

نشر نظام مصرفي عبر الإنترنت مع قواعد جدار ناري لحظر الوصول غير المصرح به وأدوات

مراقبة للكشف عن التسللات المحتملة

1.1.7 Maintenance الصيانة

Maintenance involves regularly updating and patching the software to address newly discovered security vulnerabilities and ensuring the system continues to function securely.

تشمل الصيانة تحديث البرمجيات بانتظام وإصلاح الثغرات الأمنية المكتشفة حديثًا وضمان استمرار النظام في العمل بشكل آمن

Example مثال A company issues regular software updates for its operating system to patch security vulnerabilities and improve system stability.

تصدر شركة تحديثات منتظمة لنظام التشغيل الخاص بها لإصلاح الثغرات الأمنية وتحسين استقرار النظام

1.2 Development methodologies منهجيات التطوير

Development methodologies guide how software is developed, with security integrated throughout the process. Different methodologies, like Agile and Waterfall, have specific approaches to incorporating security.

توجه منهجيات التطوير كيفية تطوير البرمجيات مع دمج الأمان في جميع مراحل العملية تتمتع منهجيات مختلفة مثل أجايل والشلال بأساليب محددة لدمج الأمان

1.2.1 Agile أجايل

Agile is an iterative development methodology that emphasizes flexibility and collaboration. Security is integrated continuously through practices such as secure sprints and regular security reviews.

أجايل هي منهجية تطوير تكرارية تركز على المرونة والتعاون يتم دمج الأمان باستمرار من خلال ممارسات مثل سباقات الأمان والمراجعات الأمنية المنتظمة

A. Sprints سباقات

In Agile, development is divided into sprints, short periods during which specific features are developed and tested. Security is addressed in each sprint to ensure ongoing protection.

في أجايل يتم تقسيم التطوير إلى سباقات فترات قصيرة يتم خلالها تطوير واختبار ميزات محددة يتم معالجة الأمان في كل سباق لضمان الحماية المستمرة

Example مثال During a sprint, the development team implements multi-factor authentication for a new feature, ensuring security is built into the process from the beginning.

خلال سباق يقوم فريق التطوير بتنفيذ المصادقة متعددة العوامل لميزة جديدة مما يضمن بناء الأمان في العملية منذ البداية

B. Scrum Master قائد سكرم

The Scrum Master facilitates Agile processes, ensuring that security practices are integrated into each sprint and that the development team follows secure coding guidelines.

يسهل قائد سكرم عمليات أجايل مما يضمن دمج ممارسات الأمان في كل سباق واتباع فريق التطوير لإرشادات البرمجة الآمنة

Example مثال A Scrum Master organizes a security review meeting at the end of each sprint to discuss potential security issues and ensure they are addressed in the next sprint.

ينظم قائد سكرم اجتماع مراجعة أمني في نهاية كل سباق لمناقشة المشكلات الأمنية المحتملة وضمان معالجتها في السباق التالي

1.2.2 Waterfall الشلال

Waterfall is a linear development methodology where each phase must be completed before moving on to the next. Security must be thoroughly integrated at each stage since going back to previous phases is challenging.

الشلال هو منهجية تطوير خطية حيث يجب إكمال كل مرحلة قبل الانتقال إلى المرحلة التالية يجب دمج الأمان بشكل شامل في كل مرحلة حيث يصعب العودة إلى المراحل السابقة

Example مثال In the Waterfall model, security requirements are fully defined during the requirements phase, and security testing is conducted thoroughly during the testing phase.

في نموذج الشلال يتم تحديد المتطلبات الأمنية بشكل كامل خلال مرحلة المتطلبات ويتم إجراء الاختبارات الأمنية بشكل شامل خلال مرحلة الاختبار

1.2.3 DevOps التطوير والتشغيل

DevOps combines development, quality assurance, and operations into a continuous integration and delivery process. Security is integrated as a shared responsibility among all teams.

يجمع التطوير والتشغيل بين التطوير وضمان الجودة والعمليات في عملية التكامل والتسليم المستمر يتم دمج الأمان كمسؤولية مشتركة بين جميع الفرق

A. Combine Dev, QA & Ops دمج التطوير وضمان الجودة والعمليات

In DevOps, development, quality assurance, and operations teams work together, ensuring that security is a continuous and integrated part of the development process.

في التطوير والتشغيل تعمل فرق التطوير وضمان الجودة والعمليات معًا مما يضمن أن يكون الأمان جزءًا مستمرًا ومتكاملًا من عملية التطوير

Example مثال A DevOps team automates security testing during the continuous integration process, catching vulnerabilities early in the development cycle.

يقوم فريق التطوير والتشغيل بأتمتة الاختبارات الأمنية خلال عملية التكامل المستمر مما يكتشف الثغرات مبكرًا في دورة التطوير

B. DevSecOps التطوير والأمان والتشغيل

DevSecOps extends DevOps by explicitly including security as part of the development and operations process, ensuring that security is built in from the start.

يمتد التطوير والأمان والتشغيل من خلال إدراج الأمان بشكل صريح كجزء من عملية التطوير

والعمليات مما يضمن بناء الأمان من البداية

Example مثال A DevSecOps team implements automated security checks at every stage of the software development pipeline, ensuring security is not an afterthought.

يقوم فريق التطوير والأمان والتشغيل بتنفيذ الفحوصات الأمنية الآلية في كل مرحلة من مراحل تطوير البرمجيات مما يضمن عدم اعتبار الأمان أمرًا لاحقًا

1.2.4 Scaled Agile Framework إطار أجايل الموسع

The Scaled Agile Framework (SAFe) applies Agile principles to large organizations, ensuring that security practices scale across multiple teams and projects.

يطبق إطار أجايل الموسع مبادئ أجايل على المؤسسات الكبيرة مما يضمن توسع ممارسات الأمان عبر فرق ومشاريع متعددة

Example مثال A large enterprise uses SAFe to coordinate security practices across various development teams working on different components of the same product.

تستخدم مؤسسة كبيرة إطار أجايل الموسع لتنسيق ممارسات الأمان عبر فرق تطوير مختلفة تعمل على مكونات مختلفة من نفس المنتج

1.2.5 Certification الشهادات

Certification in software development methodologies ensures that teams are trained in secure development practices and can apply them consistently.

تضمن الشهادات في منهجيات تطوير البرمجيات تدريب الفرق على ممارسات التطوير الآمنة وتمكنهم من تطبيقها بشكل متسق

Example مثال A development team earns certification in Agile methodology, ensuring they follow best practices for secure and efficient software development.

يحصل فريق تطوير على شهادة في منهجية أجايل مما يضمن اتباعهم لأفضل الممارسات لتطوير البرمجيات الآمنة والفعالة

1.2.6 Canary

Canary deployment involves releasing a small portion of software updates to a subset of users before a full-scale deployment, allowing for real-world security testing with minimal risk.

يتضمن نشر كاناري إصدار جزء صغير من تحديثات البرمجيات لمجموعة فرعية من المستخدمين قبل النشر الكامل مما يسمح بإجراء اختبارات أمان في العالم الحقيقي بأقل قدر من المخاطر

Example مثال A company releases a canary update of its new app version to 5% of its users to monitor for security issues before rolling it out to everyone.

تطلق شركة تحديثًا كاناري لإصدار تطبيقها الجديد إلى 5% من مستخدميها لمراقبة المشكلات الأمنية قبل طرحه للجميع

1.3 Maturity models نماذج النضج

Maturity models assess the effectiveness and maturity of security practices in software development. They provide a framework for continuous improvement.

تقيّم نماذج النضج فعالية ونضج ممارسات الأمان في تطوير البرمجيات توفر هذه النماذج إطارًا للتحسين المستمر

1.3.1 Capability Maturity Model (CMM) نموذج نضج القدرات

CMM is a model that describes the stages of maturity in software development processes. It helps organizations improve their processes by providing a structured path for growth.

نموذج نضج القدرات هو نموذج يصف مراحل النضج في عمليات تطوير البرمجيات يساعد المنظمات على تحسين عملياتها من خلال توفير مسار منظم للنمو

Example مثال An organization uses CMM to move from an ad hoc approach to software development to a more defined and repeatable process.

تستخدم منظمة نموذج نضج القدرات للانتقال من نهج عشوائي لتطوير البرمجيات إلى عملية أكثر تحديدًا وقابلة للتكرار

1.3.2 Software Assurance Maturity Model (SAMM) نموذج نضج ضمان البرمجيات

SAMM provides a framework to assess and improve the security assurance level of software development processes. It guides organizations in integrating security throughout the development lifecycle.

يوفر نموذج نضج ضمان البرمجيات إطارًا لتقييم وتحسين مستوى ضمان الأمان في عمليات تطوير البرمجيات يرشد المنظمات في دمج الأمان في دورة التطوير بأكملها

Example مثال A company adopts SAMM to improve its software development security by assessing current practices and identifying areas for improvement.

تعتمد شركة نموذج نضج ضمان البرمجيات لتحسين أمان تطوير البرمجيات من خلال تقييم الممارسات الحالية وتحديد مجالات التحسين

1.3.3 Obfuscation التشويش

Obfuscation involves making code difficult to understand to protect it from reverse engineering and unauthorized access. It's used to safeguard intellectual property and sensitive logic in software.

يتضمن التشويش جعل الكود صعب الفهم لحمايته من الهندسة العكسية والوصول غير المصرح به يستخدم لحماية الملكية الفكرية والمنطق الحساس في البرمجيات

Example مثال A software company obfuscates its source code before releasing it to prevent competitors from easily copying its proprietary algorithms.

تشوش شركة برمجيات الكود المصدري قبل إصداره لمنع المنافسين من نسخ خوارزمياتها الخاصة بسهولة

1.4 Operation and maintenance التشغيل والصيانة

Operation and maintenance involve ongoing security practices after software deployment. This includes monitoring, patching, and regular updates to address new vulnerabilities.

تشمل التشغيل والصيانة ممارسات الأمان المستمرة بعد نشر البرمجيات يتضمن ذلك المراقبة والتحديثات المنتظمة لمعالجة الثغرات الجديدة

Example مثال A company regularly updates its software to patch newly discovered vulnerabilities and ensure ongoing compliance with security standards.

تقوم شركة بتحديث برمجياتها بانتظام لإصلاح الثغرات المكتشفة حديثًا وضمان الامتثال المستمر للمعايير الأمنية

1.5 Change management إدارة التغيير

Change management is the process of managing changes to software in a controlled and systematic manner. It ensures that security is not compromised during updates or modifications.

إدارة التغيير هي عملية إدارة التغييرات في البرمجيات بطريقة منظمة ومنهجية تضمن عدم المساس بالأمان أثناء التحديثات أو التعديلات

Example مثال A change management process requires security testing and approval before any changes are made to a live application, preventing unintended security vulnerabilities.

تتطلب عملية إدارة التغيير إجراء اختبارات أمنية وموافقة قبل إجراء أي تغييرات على تطبيق قيد التشغيل مما يمنع الثغرات الأمنية غير المقصودة

1.6 Integrated Product Team الفريق المتكامل للمنتج

An Integrated Product Team (IPT) brings together members from different disciplines, including security, to collaborate on developing and maintaining secure software.

يجمع الفريق المتكامل للمنتج أعضاء من تخصصات مختلفة بما في ذلك الأمان للتعاون في تطوير وصيانة البرمجيات الآمنة

Example مثال An IPT for a new software project includes developers, security experts, and operations staff, ensuring that security considerations are integrated from the start.

يشمل الفريق المتكامل للمنتج لمشروع برمجي جديد مطورين وخبراء أمان وموظفي عمليات مما يضمن دمج الاعتبارات الأمنية من البداية

1.7 Disposal التخلص

Disposal is the process of securely removing software and its data at the end of its

lifecycle. It ensures that sensitive information is completely erased and cannot be recovered.

التخلص هو عملية إزالة البرمجيات وبياناتها بأمان في نهاية دورة حياتها يضمن ذلك مسح المعلومات الحساسة تمامًا وعدم إمكانية استرجاعها

Example مثال When a company decommissions an old software application, it uses secure wiping methods to ensure all customer data is permanently deleted.

عند إيقاف تشغيل تطبيق برمجي قديم تستخدم شركة طرق مسح آمنة لضمان حذف جميع بيانات العملاء بشكل دائم

Use Case: Secure Deployment of a New Web Application

A financial institution is developing a new web application for its customers to manage their accounts online. The development team follows the SDLC, with a focus on integrating security throughout each phase. After the development phase, the team performs comprehensive testing, including penetration testing and code reviews, to identify and mitigate vulnerabilities. Once testing is complete, the application is deployed to the production environment with security configurations such as firewall rules and monitoring tools in place. Regular maintenance is planned to update the application and address any emerging security threats. By following these steps, the institution ensures the secure deployment and ongoing protection of its web application.

حالة استخدام نشر تطبيق ويب جديد بأمان تقوم مؤسسة مالية بتطوير تطبيق ويب جديد لعملائها لإدارة حساباتهم عبر الإنترنت يتبع فريق التطوير دورة حياة تطوير البرمجيات مع التركيز على دمج الأمان في كل مرحلة بعد مرحلة التطوير يقوم الفريق بإجراء اختبارات شاملة بما في ذلك اختبار الاختراق ومراجعات الكود لتحديد الثغرات ومعالجتها بمجرد اكتمال الاختبار يتم نشر التطبيق في بيئة الإنتاج مع تهيئة الجدران النارية وأدوات المراقبة المخطط لها يتم التخطيط لصيانة منتظمة لتحديث التطبيق ومعالجة أي تهديدات أمنية جديدة من خلال اتباع هذه الخطوات تضمن المؤسسة نشر تطبيق الويب الخاص بها بأمان وحمايته المستمرة

Multiple-Choice Questions

1. Which phase of the SDLC involves defining the project’s scope, objectives, and budget?

- A. Development
- B. Testing
- C. Plan & Mgmt. Approval
- D. Deployment

2. In which development methodology is the development process divided into sprints?

- A. Waterfall
- B. Agile
- C. DevOps
- D. Scaled Agile Framework

3. What is the main focus of DevSecOps?

- A. Development and operations only
- B. Combining quality assurance and security
- C. Integrating security into the development and operations process
- D. Scaling security practices

4. Which maturity model assesses the security assurance level of software development processes?

- A. CMM
- B. SAMM
- C. SAFe

- D. Waterfall

5. What is the purpose of obfuscation in software development?

- A. To improve performance
- B. To protect code from reverse engineering
- C. To simplify code maintenance
- D. To enhance user interface design

Answers and Explanations

1. C Plan & Mgmt. Approval is the phase where the project's scope, objectives, and budget are defined. Security goals are also set during this phase to ensure proper planning for security measures.

تشمل مرحلة التخطيط والموافقة الإدارية تحديد نطاق المشروع وأهدافه وميزانيته وتحديد أهداف الأمان لضمان التخطيط السليم للتدابير الأمنية

2. B Agile divides the development process into sprints, allowing for iterative development and continuous integration of security practices.

تقسم أجايل عملية التطوير إلى سباقات مما يسمح بالتطوير التكراري ودمج ممارسات الأمان باستمرار

3. C DevSecOps focuses on integrating security into both the development and operations processes, ensuring that security is a continuous priority.

يركز التطوير والأمان والتشغيل على دمج الأمان في كل من عمليات التطوير والعمليات مما يضمن أن يكون الأمان أولوية مستمرة

4. B The Software Assurance Maturity Model (SAMM) assesses and improves the

security assurance level of software development processes.

يقوم نموذج نضج ضمان البرمجيات بتقييم وتحسين مستوى ضمان الأمان في عمليات تطوير البرمجيات

5. B Obfuscation protects code from reverse engineering by making it difficult to understand, safeguarding intellectual property and sensitive logic.

يحمي التشويش الكود من الهندسة العكسية من خلال جعله صعب الفهم مما يحمي الملكية الفكرية والمنطق الحساس

---

2. Identify and apply security controls in software development ecosystems تحديد وتطبيق ضوابط الأمان في بيئات تطوير البرمجيات

Security controls are critical in ensuring that software is developed securely, protecting it from potential threats throughout its lifecycle. These controls must be identified and applied within the software development ecosystem to mitigate risks and ensure robust security.

تعد ضوابط الأمان ضرورية لضمان تطوير البرمجيات بشكل آمن وحمايتها من التهديدات المحتملة طوال دورة حياتها يجب تحديد وتطبيق هذه الضوابط في بيئة تطوير البرمجيات للتخفيف من المخاطر وضمان الأمان القوي

2.1 Security Requirements متطلبات الأمان

Security requirements are the foundation of a secure software development process. They ensure that the software meets the necessary standards for confidentiality, integrity, and availability, which are essential for protecting data and ensuring system reliability.

تعد متطلبات الأمان أساس عملية تطوير البرمجيات الآمنة حيث تضمن أن البرمجيات تلبي المعايير الضرورية للسرية والسلامة والتوافر وهو أمر أساسي لحماية البيانات وضمان موثوقية النظام

2.1.1 Confidentiality السرية

Confidentiality ensures that sensitive information is not disclosed to unauthorized individuals or systems. It is typically enforced through encryption, access controls, and secure authentication methods.

تضمن السرية عدم الكشف عن المعلومات الحساسة للأفراد أو الأنظمة غير المصرح لهم عادة ما يتم تطبيقها من خلال التشفير وضوابط الوصول وطرق المصادقة الآمنة

Example مثال A healthcare application uses encryption to protect patient records, ensuring that only authorized personnel can access sensitive information.

يستخدم تطبيق الرعاية الصحية التشفير لحماية سجلات المرضى مما يضمن أن الأفراد المصرح لهم فقط هم من يمكنهم الوصول إلى المعلومات الحساسة

2.1.2 Integrity السلامة

Integrity ensures that data is accurate and has not been tampered with. It is maintained through checksums, digital signatures, and other validation mechanisms that detect unauthorized modifications.

تضمن السلامة دقة البيانات وعدم العبث بها يتم الحفاظ عليها من خلال التحقق من التحقق من صحة البيانات والتواقيع الرقمية وآليات التحقق الأخرى التي تكتشف التعديلات غير المصرح بها

Example مثال A financial transaction system uses digital signatures to verify that data has not been altered during transmission.

يستخدم نظام المعاملات المالية التوقيعات الرقمية للتحقق من عدم تعديل البيانات أثناء النقل

2.1.3 Availability التوافر

Availability ensures that systems and data are accessible when needed. It involves implementing redundancy, backup solutions, and disaster recovery plans to prevent downtime and data loss.

يضمن التوافر أن تكون الأنظمة والبيانات متاحة عند الحاجة يشمل ذلك تنفيذ الحلول الاحتياطية وخطط استعادة الكوارث لمنع التوقف وفقدان البيانات

Example مثال An online service provider implements redundant servers and data

backups to ensure that services remain available even during hardware failures.

يطبق مزود الخدمة عبر الإنترنت خوادم احتياطية ونسخ احتياطية للبيانات لضمان استمرار توفر الخدمات حتى أثناء فشل الأجهزة

2.2 Secure Design Principles مبادئ التصميم الآمن

Secure design principles are guidelines that help developers build software that is resistant to security threats. These principles include defense in depth, least privilege, and fail-safe defaults, among others.

تعد مبادئ التصميم الآمن إرشادات تساعد المطورين في بناء برمجيات مقاومة للتهديدات الأمنية وتشمل هذه المبادئ الدفاع في العمق والحد الأدنى من الامتيازات والافتراضات الآمنة

2.2.1 Defense in Depth الدفاع في العمق

Defense in depth is a security strategy that involves layering multiple security measures to protect systems. This approach ensures that even if one control fails, others will still provide protection.

الدفاع في العمق هو استراتيجية أمنية تشمل طبقات متعددة من التدابير الأمنية لحماية الأنظمة تضمن هذه الاستراتيجية أنه حتى إذا فشل أحد الضوابط فإن الضوابط الأخرى ستظل توفر الحماية

Example مثال A company implements firewalls, intrusion detection systems, and regular security audits to create a multi-layered defense strategy.

تقوم شركة بتطبيق جدران نارية وأنظمة كشف التسلل ومراجعات أمنية منتظمة لإنشاء استراتيجية دفاع متعددة الطبقات

2.2.2 Least Privilege الحد الأدنى من الامتيازات

The principle of least privilege dictates that users and systems should only have the minimum level of access necessary to perform their functions. This reduces the risk of unauthorized access and potential misuse.

ينص مبدأ الحد الأدنى من الامتيازات على أن المستخدمين والأنظمة يجب أن يكون لديهم فقط الحد الأدنى من الوصول الضروري لأداء وظائفهم يقلل ذلك من خطر الوصول غير المصرح به

وسوء الاستخدام المحتمل

Example مثال A database administrator is given access only to the specific databases they manage, rather than the entire system, to minimize the risk of data breaches.

يتم منح مسؤول قاعدة البيانات حق الوصول فقط إلى قواعد البيانات المحددة التي يديرها بدلاً من النظام بأكمله لتقليل خطر اختراق البيانات

2.2.3 Fail-Safe Defaults الافتراضات الآمنة

Fail-safe defaults ensure that in the event of a failure, the system defaults to a secure state, minimizing potential damage. This principle is essential for maintaining security during unexpected situations.

تضمن الافتراضات الآمنة أنه في حالة الفشل يعود النظام إلى حالة آمنة مما يقلل من الضرر المحتمل يعتبر هذا المبدأ ضروريًا للحفاظ على الأمان أثناء الحالات غير المتوقعة

Example مثال A web application automatically logs users out after a period of inactivity, ensuring that unauthorized users cannot access the system if a session is left open.

يقوم تطبيق الويب بتسجيل خروج المستخدمين تلقائيًا بعد فترة من عدم النشاط مما يضمن أن المستخدمين غير المصرح لهم لا يمكنهم الوصول إلى النظام إذا تم ترك الجلسة مفتوحة

2.3 Programming languages and Secure Programming لغات البرمجة والبرمجة الآمنة

Choosing the right programming language and following secure coding practices are crucial for developing secure software. This section explores key aspects such as input validation, session management, and polymorphism.

يعد اختيار لغة البرمجة المناسبة واتباع ممارسات الترميز الآمن أمرًا بالغ الأهمية لتطوير البرمجيات الآمنة يستعرض هذا القسم الجوانب الرئيسية مثل التحقق من صحة الإدخال وإدارة الجلسات وتعدد الأشكال

2.3.1 Input Validation التحقق من صحة الإدخال

Input validation is a process that ensures that user input is checked for correctness

and security before it is processed by the application. This helps prevent common security vulnerabilities such as SQL injection.

التحقق من صحة الإدخال هو عملية تضمن فحص إدخال المستخدم للتحقق من صحته وأمانه قبل معالجته بواسطة التطبيق يساعد ذلك في منع الثغرات الأمنية الشائعة

Example مثال A web application validates user input to ensure that it does not contain any malicious code that could be used for an SQL injection attack.

يتحقق تطبيق الويب من صحة إدخال المستخدم للتأكد من أنه لا يحتوي على أي كود ضار يمكن استخدامه لهجوم الحقن

2.3.2 Session Management إدارة الجلسات

Session management involves handling the user sessions securely, ensuring that they are not hijacked or manipulated by attackers. Proper session management includes secure session tokens, timeouts, and protection against session fixation.

تشمل إدارة الجلسات التعامل مع جلسات المستخدمين بشكل آمن لضمان عدم اختطافها أو التلاعب بها من قبل المهاجمين تتضمن إدارة الجلسات المناسبة الرموز الزمنية الآمنة وفترات انتهاء الصلاحية والحماية من تثبيت الجلسات

Example مثال A banking application generates a unique, secure session token for each user session, which is invalidated after the user logs out.

يقوم تطبيق مصرفي بإنشاء رمز جلسة فريد وآمن لكل جلسة مستخدم يتم إبطال صلاحيته بعد تسجيل خروج المستخدم

2.3.3 Polymorphism تعدد الأشكال

Polymorphism is a programming concept that allows methods to do different things based on the object they are acting upon. In secure programming, polymorphism can be used to enhance security by implementing different security measures depending on the context.

تعدد الأشكال هو مفهوم برمجي يسمح للأساليب بأداء أشياء مختلفة بناءً على الكائن الذي تعمل عليه في البرمجة الآمنة يمكن استخدام تعدد الأشكال لتعزيز الأمان من خلال تنفيذ تدابير أمان مختلفة حسب السياق

Example مثال A secure application implements different authentication methods depending on the user's role, utilizing polymorphism to tailor security to the user's needs.

يطبق تطبيق آمن أساليب مصادقة مختلفة حسب دور المستخدم ويستخدم تعدد الأشكال لتخصيص الأمان وفقًا لاحتياجات المستخدم

2.4 Libraries المكتبات

Libraries are collections of pre-written code that developers can use to save time and effort. When using libraries, it is crucial to ensure that they are secure and do not introduce vulnerabilities into the software.

المكتبات هي مجموعات من الأكواد المكتوبة مسبقًا التي يمكن للمطورين استخدامها لتوفير الوقت والجهد عند استخدام المكتبات من الضروري التأكد من أنها آمنة ولا تقدم ثغرات في البرمجيات

Example مثال A development team uses a third-party encryption library that has been thoroughly vetted for security vulnerabilities to ensure secure data handling.

يستخدم فريق التطوير مكتبة تشفير خارجية تم التحقق منها جيدًا للثغرات الأمنية لضمان معالجة البيانات بأمان

2.5 Tool sets مجموعات الأدوات

Tool sets include the software and utilities used throughout the development process, such as code editors, debuggers, and version control systems. Secure tool sets are essential for maintaining the integrity of the development environment.

تشمل مجموعات الأدوات البرمجيات والأدوات المساعدة المستخدمة طوال عملية التطوير مثل محررات الأكواد ومصححات الأخطاء وأنظمة التحكم في الإصدارات تعد الأدوات الآمنة ضرورية للحفاظ على سلامة بيئة التطوير

Example مثال A software development team uses a secure version control system that tracks changes and ensures that all code is reviewed and approved before it is merged.

يستخدم فريق تطوير البرمجيات نظام تحكم في الإصدارات آمن يتتبع التغييرات ويضمن مراجعة جميع الأكواد والموافقة عليها قبل دمجها

2.6 Integrated Development Environment بيئة التطوير المتكاملة

An Integrated Development Environment (IDE) is a software suite that combines common developer tools into a single graphical user interface. A secure IDE can help prevent coding errors and vulnerabilities by providing features such as code analysis and debugging.

بيئة التطوير المتكاملة هي مجموعة برمجيات تجمع بين أدوات المطورين الشائعة في واجهة مستخدم رسومية واحدة يمكن أن تساعد بيئة التطوير الآمنة في منع أخطاء البرمجة والثغرات من خلال توفير ميزات مثل تحليل الأكواد وتصحيح الأخطاء

Example مثال A developer uses an IDE with built-in security features like static code analysis, which helps identify potential security issues during the coding process.

يستخدم مطور بيئة تطوير متكاملة مع ميزات أمان مدمجة مثل تحليل الأكواد الثابتة مما يساعد في تحديد المشكلات الأمنية المحتملة أثناء عملية البرمجة

2.7 Runtime وقت التشغيل

Runtime refers to the period during which a program is running. It is essential to secure the runtime environment to prevent attacks such as buffer overflows, which can occur when an application is running.

يشير وقت التشغيل إلى الفترة التي يكون فيها البرنامج قيد التشغيل من الضروري تأمين بيئة وقت التشغيل لمنع الهجمات مثل تجاوز المخزن المؤقت التي يمكن أن تحدث عند تشغيل التطبيق

Example مثال A secure runtime environment includes safeguards such as runtime memory protection to prevent attacks like buffer overflows.

تشمل بيئة وقت التشغيل الآمنة ضمانات مثل حماية الذاكرة أثناء وقت التشغيل لمنع الهجمات مثل تجاوز المخزن المؤقت

2.8 Continuous Integration and Continuous Delivery (CI/CD) التكامل المستمر والتسليم المستمر

Continuous Integration and Continuous Delivery (CI/CD) are practices that automate the process of integrating code changes and delivering them to production. Secure CI/CD pipelines ensure that security checks are integrated into the development

process.

التكامل المستمر والتسليم المستمر هي ممارسات تقوم بأتمتة عملية دمج تغييرات الأكواد وتسليمها إلى الإنتاج تضمن الأنابيب الآمنة للتكامل المستمر والتسليم المستمر دمج فحوصات الأمان في عملية التطوير

Example مثال A development team integrates automated security testing into their CI/CD pipeline, ensuring that code is continuously checked for vulnerabilities before being deployed.

يقوم فريق التطوير بدمج اختبارات الأمان التلقائية في أنابيب التكامل المستمر والتسليم المستمر الخاصة بهم مما يضمن فحص الأكواد باستمرار للثغرات الأمنية قبل نشرها

2.9 Software Configuration Management إدارة تكوين البرمجيات

Software Configuration Management (SCM) involves tracking and controlling changes in the software. Secure SCM practices ensure that changes are properly authorized, documented, and tested before being implemented.

تشمل إدارة تكوين البرمجيات تتبع ومراقبة التغييرات في البرمجيات تضمن ممارسات إدارة التكوين الآمنة أن التغييرات قد تمت الموافقة عليها بشكل صحيح وتم توثيقها واختبارها قبل تنفيذها

Example مثال A development team uses SCM tools to track all changes to the software, ensuring that only authorized modifications are implemented after thorough testing.

يستخدم فريق التطوير أدوات إدارة التكوين لتتبع جميع التغييرات في البرمجيات مما يضمن تنفيذ التعديلات المصرح بها فقط بعد اختبارها بشكل دقيق

2.10 Code repositories مستودعات الأكواد

Code repositories are storage locations where developers can keep their code. Secure code repositories prevent unauthorized access, ensure version control, and protect the integrity of the codebase.

مستودعات الأكواد هي مواقع تخزين يمكن للمطورين الاحتفاظ بأكوادهم فيها تمنع مستودعات الأكواد الآمنة الوصول غير المصرح به وتضمن التحكم في الإصدارات وتحمي سلامة قاعدة الأكواد

Example مثال A development team uses a secure, cloud-based code repository with multi-factor authentication to ensure that only authorized team members can access the code.

يستخدم فريق تطوير مستودع أكواد آمن قائم على السحابة مع المصادقة متعددة العوامل لضمان وصول أعضاء الفريق المصرح لهم فقط إلى الأكواد

2.11 Application security testing اختبارات أمان التطبيقات

Application security testing is essential for identifying vulnerabilities within software before it is deployed. There are various types of testing, including Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and Interactive Application Security Testing (IAST).

تعد اختبارات أمان التطبيقات ضرورية لتحديد الثغرات داخل البرمجيات قبل نشرها توجد أنواع مختلفة من الاختبارات بما في ذلك اختبار أمان التطبيقات الثابتة واختبار أمان التطبيقات الديناميكية واختبار أمان التطبيقات التفاعلي

2.11.1 Static Application Security Testing (SAST) اختبار أمان التطبيقات الثابتة

SAST involves analyzing the source code of an application to identify potential security vulnerabilities without executing the code. It helps detect issues early in the development process.

يشمل اختبار أمان التطبيقات الثابتة تحليل كود المصدر لتطبيق لتحديد الثغرات الأمنية المحتملة دون تنفيذ الكود يساعد في اكتشاف المشكلات في وقت مبكر من عملية التطوير

Example مثال A development team runs SAST tools on their codebase to detect and fix security vulnerabilities before moving on to the testing phase.

يشغل فريق تطوير أدوات اختبار أمان التطبيقات الثابتة على قاعدة الأكواد الخاصة بهم لاكتشاف وإصلاح الثغرات الأمنية قبل الانتقال إلى مرحلة الاختبار

2.11.2 Dynamic Application Security Testing (DAST) اختبار أمان التطبيقات الديناميكية

DAST involves testing the running application to identify vulnerabilities that occur

during execution. This method helps uncover issues such as cross-site scripting (XSS) and SQL injection.

يشمل اختبار أمان التطبيقات الديناميكية اختبار التطبيق أثناء التشغيل لتحديد الثغرات التي تحدث أثناء التنفيذ يساعد هذا الأسلوب في كشف المشكلات

Example مثال A security team conducts DAST on a web application to identify and remediate issues like cross-site scripting (XSS) before it goes live.

يقوم فريق الأمان بإجراء اختبار أمان التطبيقات الديناميكية على تطبيق ويب لتحديد ومعالجة المشكلات

2.11.3 Software composition analysis, Interactive Application Security Test (IAST) اختبار أمان التطبيقات التفاعلي وتحليل مكونات البرمجيات

IAST combines elements of both SAST and DAST by analyzing an application in real-time as it is running, providing a comprehensive view of security vulnerabilities.

يجمع اختبار أمان التطبيقات التفاعلي بين عناصر من اختبار أمان التطبيقات الثابتة واختبار أمان التطبيقات الديناميكية من خلال تحليل التطبيق في الوقت الفعلي أثناء تشغيله مما يوفر رؤية شاملة للثغرات الأمنية

Example مثال A development team uses IAST tools to analyze their application in real-time during testing, ensuring that both code-level and runtime vulnerabilities are addressed.

يستخدم فريق تطوير أدوات اختبار أمان التطبيقات التفاعلي لتحليل تطبيقاتهم في الوقت الفعلي أثناء الاختبار مما يضمن معالجة الثغرات الأمنية على مستوى الكود ووقت التشغيل

Use Case: Integrating Security Controls Across the Development Lifecycle حالة الاستخدام: دمج ضوابط الأمان عبر دورة حياة التطوير

A financial software development team is tasked with creating a new online banking platform. Security is a top priority, so they begin by identifying security requirements based on confidentiality, integrity, and availability. During the design phase, they implement secure design principles like defense in depth and least privilege. They choose a programming language that supports input validation and session management to further secure the application.

The team leverages a secure Integrated Development Environment (IDE) with built-in security features and uses SCM tools to track all code changes. During development, they regularly use SAST tools to identify potential vulnerabilities in the codebase. Once the application is running, they perform DAST and IAST to ensure runtime security.

Finally, the team uses a secure code repository with multi-factor authentication to protect the integrity of their codebase. Throughout the CI/CD pipeline, security testing is automated to ensure continuous security validation.

This comprehensive approach ensures that security controls are integrated across the entire software development lifecycle, protecting the platform from potential threats and vulnerabilities.

يتم تكليف فريق تطوير البرمجيات المالية بإنشاء منصة مصرفية عبر الإنترنت جديدة الأمن هو الأولوية القصوى لذلك يبدأون بتحديد متطلبات الأمان بناءً على السرية والسلامة والتوافر خلال مرحلة التصميم يقومون بتطبيق مبادئ التصميم الآمن مثل الدفاع في العمق والحد الأدنى من الامتيازات يختارون لغة برمجة تدعم التحقق من صحة الإدخال وإدارة الجلسات لتأمين التطبيق بشكل أكبر

يستفيد الفريق من بيئة تطوير متكاملة آمنة مع ميزات أمان مدمجة ويستخدمون أدوات إدارة تكوين البرمجيات لتتبع جميع تغييرات الكود أثناء التطوير يستخدمون بانتظام أدوات اختبار أمان التطبيقات الثابتة لتحديد الثغرات المحتملة في قاعدة الأكواد بمجرد تشغيل التطبيق يقومون بإجراء اختبار أمان التطبيقات الديناميكية واختبار أمان التطبيقات التفاعلي لضمان أمان وقت التشغيل

أخيرًا يستخدم الفريق مستودع أكواد آمن مع مصادقة متعددة العوامل لحماية سلامة قاعدة الأكواد الخاصة بهم طوال أنابيب التكامل المستمر والتسليم المستمر يتم أتمتة اختبارات الأمان لضمان التحقق المستمر من الأمان

يضمن هذا النهج الشامل دمج ضوابط الأمان عبر دورة حياة تطوير البرمجيات بأكملها مما يحمي المنصة من التهديدات والثغرات الأمنية المحتملة

Multiple-Choice Questions

1. **Which security principle focuses on providing minimum necessary access to users?**

- A. Fail-Safe Defaults

- B. Defense in Depth
- C. Least Privilege
- D. Continuous Integration

2. **Which type of security testing analyzes an application without executing the code?**

- A. DAST
- B. SAST
- C. IAST
- D. SCM

3. **What is the main goal of using secure programming languages in software development?**

- A. Increase application speed
- B. Simplify code management
- C. Reduce security vulnerabilities
- D. Improve user interface design

4. **Which of the following is NOT a secure design principle?**

- A. Defense in Depth
- B. Least Privilege
- C. Fail-Safe Defaults
- D. Open Access

5. **What does Continuous Integration (CI) primarily focus on in the development process?**

- A. Integrating code changes automatically
- B. Delivering code to production manually
- C. Writing code without version control
- D. Securing runtime environments

Answers and Explanations

1. **1 C Least Privilege**

Explanation: The principle of least privilege ensures that users are granted the minimum level of access required to perform their tasks, reducing the risk of unauthorized access or damage. مبدأ الامتيازات الأقل يضمن منح المستخدمين أدنى مستوى من الوصول المطلوب لأداء مهامهم مما يقلل من مخاطر الوصول غير المصرح به أو الضرر

2. **2 B SAST**

Explanation: Static Application Security Testing (SAST) analyzes the source code of an application without executing it to identify potential security vulnerabilities. اختبار أمان التطبيقات الثابتة يحلل كود المصدر للتطبيق دون تنفيذه لتحديد الثغرات الأمنية المحتملة

3. **3 C Reduce security vulnerabilities**

Explanation: Secure programming languages help minimize security vulnerabilities by providing features that prevent common coding errors and protect against attacks. تساعد لغات البرمجة الآمنة في تقليل الثغرات الأمنية من خلال توفير ميزات تمنع أخطاء البرمجة الشائعة وتحمي من الهجمات

4. **4 D Open Access**

Explanation: Open Access is not a secure design principle. Secure design principles include defense in depth, least privilege, and fail-safe defaults, which focus on minimizing security risks. الوصول المفتوح ليس مبدأً لتصميم الأمان مبادئ التصميم الآمن تشمل الدفاع في العمق والامتيازات الأقل والإعدادات الافتراضية الآمنة التي تركز على تقليل مخاطر الأمان

5. **5 A Integrating code changes automatically**

Explanation: Continuous Integration (CI) focuses on automating the integration of code changes, allowing developers to detect and fix issues early in the development process. يركز التكامل المستمر على أتمتة دمج تغييرات الكود مما يسمح للمطورين باكتشاف وإصلاح المشكلات في وقت مبكر من عملية التطوير

---

3. Assess the Effectiveness of Software Security | تقييم فعالية أمان البرمجيات

Assessing the effectiveness of software security involves evaluating the measures and controls in place to protect software from threats and vulnerabilities. This ensures that the software remains secure throughout its lifecycle and that any security gaps are identified and addressed promptly. This process is crucial for maintaining the integrity, confidentiality, and availability of software systems.

تقييم فعالية أمان البرمجيات يتضمن تقييم التدابير والضوابط الموجودة لحماية البرمجيات من التهديدات والثغرات الأمنية يضمن ذلك بقاء البرمجيات آمنة طوال دورة حياتها وأن يتم تحديد أي فجوات أمنية ومعالجتها على الفور هذه العملية ضرورية للحفاظ على سلامة وسرية وتوافر أنظمة البرمجيات

3.1. Auditing and Logging of Changes | التدقيق وتسجيل التغييرات

Auditing and logging are critical components of software security that provide visibility into changes made to software systems. Auditing involves reviewing and analyzing logs and records to ensure that software changes comply with security policies and standards. Logging, on the other hand, involves the systematic

recording of events and changes in the software environment, allowing for real-time monitoring and historical analysis.

التدقيق وتسجيل التغييرات هما مكونان أساسيان لأمان البرمجيات يوفران رؤية للتغييرات التي يتم إجراؤها على أنظمة البرمجيات يتضمن التدقيق مراجعة وتحليل السجلات للتأكد من أن تغييرات البرمجيات تتوافق مع السياسات والمعايير الأمنية من ناحية أخرى يتضمن تسجيل التغييرات التوثيق المنهجي للأحداث والتغييرات في بيئة البرمجيات مما يسمح بالمراقبة في الوقت الحقيقي والتحليل التاريخي

Example 1:

Consider a financial application that handles sensitive transactions. Each change in the application, whether it is a code update or a configuration change, is logged. Security audits are conducted regularly to review these logs and ensure that all changes adhere to the company's security policies. If a suspicious change is detected, it is flagged for further investigation.

ضع في اعتبارك تطبيقًا ماليًا يتعامل مع المعاملات الحساسة يتم تسجيل كل تغيير في التطبيق سواء كان تحديثًا للشفرة أو تغييرًا في التكوين تُجرى عمليات تدقيق أمني بانتظام لمراجعة هذه السجلات والتأكد من أن جميع التغييرات تتماشى مع سياسات الأمان الخاصة بالشركة إذا تم اكتشاف تغيير مريب يتم تحديده لمزيد من التحقيق

Example 2:

In an e-commerce platform, all modifications to customer data, such as changes to payment information or shipping addresses, are logged automatically. These logs are reviewed periodically by the security team to ensure that no unauthorized changes have occurred. If any irregular activity is detected, it is flagged and investigated to prevent potential fraud or data breaches.

في منصة للتجارة الإلكترونية يتم تسجيل جميع التعديلات على بيانات العملاء تلقائيًا مثل التغييرات في معلومات الدفع أو عناوين الشحن تقوم فرق الأمان بمراجعة هذه السجلات بشكل دوري للتأكد من عدم حدوث أي تغييرات غير مصرح بها إذا تم اكتشاف أي نشاط غير منتظم يتم تحديده والتحقيق فيه لمنع الاحتيال المحتمل أو خروقات البيانات

Example 3:

A large enterprise uses a centralized logging system that aggregates logs from all its software applications. This system allows security teams to monitor changes across the entire organization in real-time. For instance, if a configuration file for a critical application is modified outside of normal business hours, the system triggers an

alert for immediate review and action.

تستخدم مؤسسة كبيرة نظام تسجيل مركزي يقوم بتجميع السجلات من جميع تطبيقات البرمجيات الخاصة بها يتيح هذا النظام لفرق الأمان مراقبة التغييرات في جميع أنحاء المؤسسة في الوقت الفعلي على سبيل المثال إذا تم تعديل ملف تكوين لتطبيق حرج خارج ساعات العمل العادية يقوم النظام بتشغيل تنبيه للمراجعة الفورية واتخاذ الإجراءات

3.2. Risk Analysis and Mitigation | تحليل المخاطر والتخفيف منها

Risk analysis involves identifying potential security risks in software and evaluating their impact and likelihood. This process helps in understanding the vulnerabilities that could be exploited and the potential consequences. Mitigation strategies are then developed to reduce or eliminate these risks. Effective risk analysis and mitigation ensure that security threats are managed proactively, minimizing their impact on the software system.

تحليل المخاطر يتضمن تحديد المخاطر الأمنية المحتملة في البرمجيات وتقييم تأثيرها واحتمال حدوثها تساعد هذه العملية في فهم الثغرات التي يمكن استغلالها والعواقب المحتملة يتم بعد ذلك تطوير استراتيجيات التخفيف للحد من هذه المخاطر أو القضاء عليها يضمن تحليل المخاطر والتخفيف الفعال إدارة التهديدات الأمنية بشكل استباقي مما يقلل من تأثيرها على نظام البرمجيات

Example 1:

In a healthcare system, patient data is highly sensitive. Through risk analysis, the system identifies potential threats such as unauthorized access to patient records. To mitigate this risk, the system implements strong access controls, encryption, and regular security updates to protect patient data from unauthorized access or breaches.

في نظام الرعاية الصحية تكون بيانات المرضى شديدة الحساسية من خلال تحليل المخاطر يحدد النظام التهديدات المحتملة مثل الوصول غير المصرح به إلى سجلات المرضى لتقليل هذه المخاطر ينفذ النظام ضوابط وصول قوية وتشفيرًا وتحديثات أمنية منتظمة لحماية بيانات المرضى من الوصول غير المصرح به أو الاختراقات

Example 2:

In a banking system, risk analysis identifies that using outdated encryption protocols could expose customer transactions to interception. To mitigate this risk, the bank upgrades its encryption standards to the latest industry-approved protocols,

ensuring that all data transmitted between the bank and its customers is securely encrypted.

في نظام مصرفي يحدد تحليل المخاطر أن استخدام بروتوكولات تشفير قديمة يمكن أن يعرض معاملات العملاء للاعتراض لتقليل هذا الخطر يقوم البنك بترقية معايير التشفير الخاصة به إلى أحدث البروتوكولات المعتمدة من الصناعة مما يضمن تشفير جميع البيانات المرسلة بين البنك وعملائه بشكل آمن

Example 3:

A software company developing a new healthcare application performs a risk analysis to identify potential threats to patient data. They discover that improper access control settings could allow unauthorized personnel to view sensitive patient information. As a mitigation measure, the company implements role-based access control (RBAC), ensuring that only authorized medical staff can access patient records.

تقوم شركة برمجيات تطور تطبيقًا صحيًا جديدًا بإجراء تحليل للمخاطر لتحديد التهديدات المحتملة لبيانات المرضى يكتشفون أن إعدادات التحكم في الوصول غير الصحيحة يمكن أن تسمح للأشخاص غير المصرح لهم بعرض معلومات المريض الحساسة كإجراء تخفيفي تقوم الشركة بتنفيذ تحكم في الوصول قائم على الأدوار مما يضمن أن الموظفين الطبيين المصرح لهم فقط يمكنهم الوصول إلى سجلات المرضى

Use Case | دراسة حالة

In an enterprise software development project, the security team conducts a comprehensive risk analysis to identify potential threats to the software being developed. They identify that unauthorized changes to the software could lead to data breaches. To mitigate this risk, they implement a robust auditing and logging system that tracks all changes made to the software. Regular audits are conducted to ensure compliance with security policies.

في مشروع تطوير البرمجيات في مؤسسة تجري فرق الأمان تحليل مخاطر شامل لتحديد التهديدات المحتملة للبرمجيات قيد التطوير يحددون أن التغييرات غير المصرح بها في البرمجيات يمكن أن تؤدي إلى اختراقات البيانات لتقليل هذه المخاطر يقومون بتنفيذ نظام تدقيق وتسجيل قوي يتتبع جميع التغييرات التي تم إجراؤها على البرمجيات تُجرى عمليات تدقيق بانتظام لضمان الامتثال للسياسات الأمنية

Multiple-Choice Questions

1. **Which process involves reviewing and analyzing logs to ensure software changes comply with security policies?**

- A. Risk Analysis
- B. Auditing
- C. Mitigation
- D. Logging

2. **What is the primary goal of risk analysis in software security?**

- A. Improve user experience
- B. Identify and evaluate security risks
- C. Increase software speed
- D. Automate software testing

3. **Which of the following is a key component of effective risk mitigation?**

- A. Strong access controls
- B. Code optimization
- C. User interface design
- D. Feature enhancement

4. **What does logging in software security primarily help with?**

- A. Recording events and changes

- B. Improving software performance
- C. Managing user roles
- D. Developing new features

5. **Which of the following is a common outcome of a security audit?**

- A. Identification of compliance issues
- B. Increased software functionality
- C. Improved user interface
- D. Faster code execution

Answers and Explanations

1. **1 B Auditing**

Explanation: Auditing involves reviewing and analyzing logs and records to ensure that software changes comply with security policies and standards. يتضمن التدقيق مراجعة وتحليل السجلات للتأكد من أن تغييرات البرمجيات تتوافق مع السياسات والمعايير الأمنية

2. **2 B Identify and evaluate security risks**

- **Explanation:** The primary goal of risk analysis is to identify potential security risks in software and evaluate their impact and likelihood. الهدف الرئيسي من تحليل المخاطر هو تحديد المخاطر الأمنية المحتملة في البرمجيات وتقييم تأثيرها واحتمال حدوثها

3. **3 A Strong access controls**

Explanation: Strong access controls are a key component of risk mitigation, helping to reduce or eliminate security risks by restricting unauthorized access. ضوابط الوصول القوية هي مكون رئيسي لتخفيف المخاطر حيث تساعد في تقليل المخاطر الأمنية أو

القضاء عليها من خلال تقييد الوصول غير المصرح به

4. **4 A Recording events and changes**

Explanation: Logging helps with the systematic recording of events and changes in the software environment, allowing for real-time monitoring and historical analysis. يساعد تسجيل التغييرات في التوثيق المنهجي للأحداث والتغييرات في بيئة البرمجيات مما يسمح بالمراقبة في الوقت الحقيقي والتحليل التاريخي

5. **5 A Identification of compliance issues**

Explanation: A common outcome of a security audit is the identification of compliance issues, which can then be addressed to improve the overall security posture. النتيجة الشائعة للتدقيق الأمني هي تحديد مشكلات الامتثال والتي يمكن معالجتها بعد ذلك لتحسين الوضع الأمني العام

---

4. Assess Security Impact of Acquired Software | تقييم تأثير أمان البرمجيات المكتسبة

Assessing the security impact of acquired software is a critical process in safeguarding an organization's environment from potential vulnerabilities. This assessment ensures that any software integrated into the system aligns with the organization’s security standards and does not introduce new risks. The process involves evaluating vendors, assessing contracts, and analyzing different types of software, including COTS, open-source, third-party, managed services, and cloud services.

تقييم تأثير أمان البرمجيات المكتسبة هو عملية حاسمة في حماية بيئة المؤسسة من الثغرات الأمنية المحتملة. يضمن هذا التقييم أن أي برمجيات مدمجة في النظام تتماشى مع معايير الأمان الخاصة بالمؤسسة ولا تقدم مخاطر جديدة. تتضمن العملية تقييم البائعين وتقييم العقود وتحليل أنواع مختلفة من البرمجيات بما في ذلك الجاهزة، مفتوحة المصدر، الطرف الثالث، الخدمات المدارة، والخدمات السحابية.

4.1. Acquire Software | اكتساب البرمجيات

Acquiring software involves selecting, evaluating, and implementing software solutions that meet the specific needs of an organization. A thorough security assessment during this phase ensures that the selected software does not introduce vulnerabilities.

يتضمن اكتساب البرمجيات اختيار وتقييم وتنفيذ حلول البرمجيات التي تلبي احتياجات المؤسسة المحددة. يضمن التقييم الأمني الشامل خلال هذه المرحلة أن البرمجيات المختارة لا تقدم ثغرات أمنية.

4.1.1. Assess Vendors | تقييم البائعين

Vendor assessment is crucial for determining the security posture of the software provider. This involves evaluating the vendor's security practices, history of incidents, compliance with industry standards, and ability to support the organization’s security needs.

تقييم البائعين أمر بالغ الأهمية لتحديد وضع الأمان لمزود البرمجيات. يتضمن ذلك تقييم ممارسات الأمان الخاصة بالبائع، وتاريخه في الحوادث، والامتثال للمعايير الصناعية، وقدرته على دعم احتياجات الأمان الخاصة بالمؤسسة.

Example: | مثال:

A healthcare provider considering a new electronic health records (EHR) system conducts a vendor assessment by reviewing the vendor’s past security incidents, certifications like HIPAA compliance, and security support capabilities.

يقوم مقدم الرعاية الصحية الذي يفكر في نظام جديد للسجلات الصحية الإلكترونية بإجراء تقييم للبائع من خلال مراجعة الحوادث الأمنية السابقة للبائع، والشهادات مثل الامتثال لقانون ، وقدرات دعم الأمان.

4.1.2. Contract SLA | اتفاقية مستوى الخدمة للعقد

The Service Level Agreement (SLA) outlines the expectations and responsibilities between the organization and the software vendor. It should include specific clauses addressing data protection, incident response, and compliance with relevant regulations.

تحدد اتفاقية مستوى الخدمة التوقعات والمسؤوليات بين المؤسسة ومزود البرمجيات. يجب أن تتضمن بنودًا محددة تتعلق بحماية البيانات، والاستجابة للحوادث، والامتثال للوائح ذات الصلة.

Example: | مثال:

A financial institution negotiates an SLA with a software vendor that includes mandatory encryption standards and stipulates a maximum 4-hour response time to any security breach.

تقوم مؤسسة مالية بالتفاوض على اتفاقية مستوى الخدمة مع مزود البرمجيات تتضمن معايير التشفير الإلزامية وتنص على حد أقصى قدره ٤ ساعات للاستجابة لأي خرق أمني.

4.2. Commercial Off-The-Shelf (COTS) | البرمجيات الجاهزة

COTS software is pre-built and available for purchase by the general public. While cost-effective and widely used, it may not always align with specific security requirements, necessitating a thorough security review before adoption.

البرمجيات الجاهزة هي برمجيات جاهزة ومتاحة للشراء من قبل الجمهور العام. على الرغم من أنها فعالة من حيث التكلفة وتستخدم على نطاق واسع، إلا أنها قد لا تتماشى دائمًا مع المتطلبات الأمنية المحددة، مما يستلزم مراجعة أمنية شاملة قبل اعتمادها.

Example: | مثال:

A government agency planning to use COTS software for document management conducts a detailed security assessment to ensure compliance with internal security policies and regulations.

تقوم وكالة حكومية تخطط لاستخدام البرمجيات الجاهزة لإدارة الوثائق بإجراء تقييم أمني مفصل لضمان الامتثال للسياسات واللوائح الأمنية الداخلية.

4.3. Open Source | البرمجيات مفتوحة المصدر

Open-source software provides access to its source code, which users can modify and distribute. While it offers flexibility and transparency, it requires a rigorous security evaluation to identify and mitigate potential vulnerabilities.

تتيح البرمجيات مفتوحة المصدر الوصول إلى الشفرة المصدرية التي يمكن للمستخدمين تعديلها وتوزيعها. على الرغم من أنها توفر المرونة والشفافية، إلا أنها تتطلب تقييمًا أمنيًا صارمًا

لتحديد ومعالجة الثغرات الأمنية المحتملة.

Example: | مثال:

A tech company decides to integrate an open-source library into its new application. The security team conducts a code review and tests for known vulnerabilities to ensure the library is secure.

تقرر شركة تقنية دمج مكتبة مفتوحة المصدر في تطبيقها الجديد. يقوم فريق الأمان بمراجعة الشفرة واختبار الثغرات المعروفة للتأكد من أمان المكتبة.

4.4. Third-Party | الطرف الثالث

Third-party software, developed by external vendors, is often integrated into existing systems. Security assessments are essential to ensure that the software does not introduce vulnerabilities or compliance issues.

غالبًا ما يتم دمج البرمجيات التي تم تطويرها من قبل بائعين خارجيين في الأنظمة الموجودة. تعتبر التقييمات الأمنية ضرورية لضمان أن البرمجيات لا تقدم ثغرات أمنية أو مشاكل امتثال.

Example: | مثال:

A retail company using a third-party customer relationship management (CRM) system conducts a security audit to ensure it complies with data protection regulations.

تقوم شركة تجزئة تستخدم نظام إدارة علاقات العملاء الخاص بالطرف الثالث بإجراء تدقيق أمني لضمان الامتثال للوائح حماية البيانات.

4.5. Managed Services (e.g., Enterprise Applications) | الخدمات المدارة (مثل التطبيقات المؤسسية)

Managed services, such as enterprise applications, involve outsourcing IT functions to a third party. While this can increase efficiency, it also requires close monitoring to ensure that security standards are maintained.

تشمل الخدمات المدارة مثل التطبيقات المؤسسية الاستعانة بمصادر خارجية لوظائف تكنولوجيا المعلومات إلى طرف ثالث. على الرغم من أن ذلك يمكن أن يزيد من الكفاءة، إلا أنه يتطلب مراقبة دقيقة لضمان الحفاظ على معايير الأمان.

Example: | مثال:

A large enterprise outsources its ERP system to a managed service provider, ensuring that the provider adheres to strict access controls and encryption standards.

تقوم مؤسسة كبيرة بالاستعانة بمزود خدمة مُدار لنظام الخاص بها لضمان أن يلتزم المزود بضوابط الوصول الصارمة ومعايير التشفير.

4.6. Cloud Services | الخدمات السحابية

Cloud services, including SaaS, IaaS, and PaaS, offer scalable and flexible solutions but introduce unique security challenges. Security assessments must focus on data protection, access controls, and compliance with relevant standards and regulations.

حلولًا قابلة للتوسع ومرنة ولكنها تقدم PaaSو IaaSو SaaS تقدم الخدمات السحابية بما في ذلك تحديات أمنية فريدة. يجب أن تركز التقييمات الأمنية على حماية البيانات، وضوابط الوصول، والامتثال للمعايير واللوائح ذات الصلة.

4.6.1. Software as a Service (SaaS) | البرمجيات كخدمة

SaaS delivers software over the internet, eliminating the need for local installation. Security considerations include ensuring that the service provider implements strong data protection measures and complies with applicable regulations.

تقدم البرمجيات كخدمة البرمجيات عبر الإنترنت مما يلغي الحاجة إلى التثبيت المحلي. تشمل الاعتبارات الأمنية ضمان أن يقوم مزود الخدمة بتنفيذ تدابير قوية لحماية البيانات والامتثال للوائح المعمول بها.

Example: | مثال:

A small business adopts a SaaS-based HR management system and ensures that the provider uses encryption for sensitive employee data and complies with GDPR.

تتبنى شركة صغيرة نظام إدارة الموارد البشرية القائم على البرمجيات كخدمة وتضمن أن يستخدم المزود التشفير لبيانات الموظفين الحساسة

4.6.2. Infrastructure as a Service (IaaS) | البنية التحتية كخدمة

IaaS provides virtualized computing resources online. Security measures include configuring the infrastructure securely and ensuring that the service provider offers robust security controls like firewalls and intrusion detection systems.

توفر البنية التحتية كخدمة موارد حوسبة افتراضية عبر الإنترنت. تشمل التدابير الأمنية تكوين البنية التحتية بشكل آمن وضمان أن يقدم مزود الخدمة ضوابط أمان قوية مثل الجدران النارية وأنظمة الكشف عن التسلل.

Example: | مثال:

A tech startup uses an IaaS platform to host its application. The startup configures the infrastructure with strong access controls and network segmentation to protect against unauthorized access.

تستخدم شركة ناشئة في مجال التكنولوجيا منصة البنية التحتية كخدمة لاستضافة تطبيقها. تقوم الشركة الناشئة بتكوين البنية التحتية باستخدام ضوابط وصول قوية وتقسيم الشبكة لحماية ضد الوصول غير المصرح به.

4.6.3. Platform as a Service (PaaS) | المنصة كخدمة

PaaS provides a platform for developing, deploying, and managing applications without worrying about the underlying infrastructure. Security assessments should focus on the platform’s ability to support secure development practices and integrate with existing security controls.

توفر المنصة كخدمة منصة لتطوير ونشر وإدارة التطبيقات دون القلق بشأن البنية التحتية الأساسية يجب أن تركز التقييمات الأمنية على قدرة المنصة على دعم ممارسات التطوير الآمن والتكامل مع ضوابط الأمان الحالية.

Example: | مثال:

A financial services firm uses a PaaS environment to develop a new mobile banking app, ensuring the platform supports secure coding practices and integrates with the firm's security infrastructure.

تستخدم شركة خدمات مالية بيئة المنصة كخدمة لتطوير تطبيق مصرفي جديد للهاتف المحمول وتضمن أن تدعم المنصة ممارسات الترميز الآمن وتتكامل مع البنية التحتية الأمنية للشركة.

Use Case: Comprehensive Assessment of a Cloud-Based CRM Solution | دراسة حالة: التقييم الشامل لحل إدارة علاقات العملاء القائم على السحابة

Scenario: A medium-sized retail company decides to adopt a cloud-based CRM solution to manage customer interactions, sales, and marketing campaigns. The company's security team is tasked with assessing the security impact of this new software acquisition.

Steps Taken:

A medium-sized retail company decides to adopt a cloud-based CRM solution to manage customer interactions, sales, and marketing campaigns. The company's security team is tasked with assessing the security impact of this new software acquisition.

Steps Taken:

1. **Vendor Assessment:** The team evaluates the CRM vendor's security posture, examining their compliance with industry standards like GDPR and ISO 27001. They also review the vendor’s history of security incidents and their response strategies.

تقييم البائع: يقوم الفريق بتقييم وضع الأمان لمزود النظام من خلال فحص امتثالهم للمعايير الصناعية كما يقومون بمراجعة تاريخ الحوادث الأمنية الخاصة بالبائع واستراتيجيات الاستجابة لديهم.

2. **SLA Negotiation:** The company negotiates a Service Level Agreement (SLA) that includes stringent data protection clauses, incident response times, and penalties for non-compliance. The SLA ensures that the CRM provider adheres to the company’s security requirements.

التفاوض على اتفاقية مستوى الخدمة تتفاوض الشركة على اتفاقية مستوى الخدمة التي تتضمن بنودًا صارمة لحماية البيانات وأوقات استجابة للحوادث وعقوبات لعدم الامتثال. تضمن اتفاقية مستوى الخدمة أن يلتزم المزود بمتطلبات الأمان الخاصة بالشركة.

3. **Security Evaluation of the SaaS Model:** Since the CRM is delivered as a SaaS, the team ensures that the service provider uses strong encryption for data at rest and in transit. They also confirm that access controls and multi-factor authentication are in place.

تقييم الأمان لنموذج : نظرًا لأن نظام يتم تسليمه كخدمة ، فإن الفريق يضمن أن يستخدم مزود الخدمة تشفيرًا قويًا للبيانات في حالة السكون والانتقال. كما يؤكدون وجود ضوابط الوصول

والمصادقة متعددة العوامل.

4. **Integration with Existing Systems:** The security team assesses how the CRM system will integrate with the company's existing infrastructure, ensuring that it does not introduce vulnerabilities. They implement additional controls, such as secure APIs and data loss prevention (DLP) solutions.

التكامل مع الأنظمة الحالية: يقيم فريق الأمان كيفية تكامل النظام مع البنية التحتية الحالية للشركة لضمان أنه لا يقدم ثغرات أمنية. يقومون بتنفيذ ضوابط إضافية مثل واجهات برمجة التطبيقات الآمنة وحلول منع فقدان البيانات (DLP).

5. **Continuous Monitoring:** The company establishes a continuous monitoring strategy to regularly assess the CRM system's security, including periodic audits, vulnerability scanning, and compliance checks.

المراقبة المستمرة: تضع الشركة استراتيجية مراقبة مستمرة لتقييم أمان نظام بانتظام، بما في ذلك عمليات التدقيق الدورية وفحص الثغرات الأمنية والتحقق من الامتثال.

Outcome: The retail company successfully integrates the cloud-based CRM solution, enhancing its customer relationship management while maintaining a strong security posture. The thorough assessment and ongoing monitoring help prevent potential security breaches and ensure compliance with industry regulations.

النتيجة: تقوم شركة التجزئة بدمج نظام إدارة علاقات العملاء القائم على السحابة بنجاح، مما يعزز إدارة علاقات العملاء الخاصة بها مع الحفاظ على وضع أمني قوي. يساعد التقييم الشامل والمراقبة المستمرة على منع الخروقات الأمنية المحتملة وضمان الامتثال للأنظمة الصناعية.

Multiple-Choice Questions

1. **Which of the following is NOT typically included in a vendor security assessment?**

- A. Reviewing past security incidents
- B. Assessing compliance with industry standards
- C. Evaluating the vendor's marketing strategies
- D. Reviewing the vendor's security policies

2. **When negotiating a Service Level Agreement (SLA) for acquired software, which aspect is most critical?**

- A. Vendor's market share
- B. Data protection clauses
- C. Software user interface
- D. Pricing structure

3. **What is a primary security concern when using Commercial Off-The-Shelf (COTS) software?**

- A. Customizability
- B. Cost
- C. Security alignment with organization’s needs
- D. User interface design

4. **Which type of software requires rigorous security evaluation due to its transparency and flexibility?**

- A. COTS
- B. Open-source
- C. Third-party
- D. Managed services

5. **What is a key security measure when using Infrastructure as a Service (IaaS)?**

- A. High availability
- B. Configuring the infrastructure securely
- C. User experience design
- D. Marketing potential

Answers with Explanations

1. **C. Evaluating the vendor's marketing strategies** Vendor security assessments focus on evaluating security practices, incident history, and compliance, not marketing strategies.

لا تركز التقييمات الأمنية للبائعين على استراتيجيات التسويق بل على تقييم ممارسات الأمان وتاريخ الحوادث والامتثال.

2. **B. Data protection clauses** SLAs must include strong data protection clauses to ensure the security of the acquired software.

يجب أن تتضمن اتفاقيات مستوى الخدمة بنودًا قوية لحماية البيانات لضمان أمان البرمجيات المكتسبة.

3. **C. Security alignment with organization’s needs** COTS software may not always align with specific security requirements, which necessitates a security review.

قد لا تتماشى البرمجيات الجاهزة دائمًا مع المتطلبات الأمنية المحددة مما يستلزم مراجعة أمنية.

4. **B. Open-source** Open-source software, while flexible, requires thorough security evaluations to mitigate potential vulnerabilities.

تتطلب البرمجيات مفتوحة المصدر على الرغم من مرونتها تقييمات أمنية شاملة للتخفيف من الثغرات المحتملة.

5. **B. Configuring the infrastructure securely** Securely configuring IaaS infrastructure is essential to protect against unauthorized access and other security risks.

يعد تكوين البنية التحتية للبنية التحتية كخدمة بشكل آمن أمرًا ضروريًا للحماية من الوصول غير المصرح به والمخاطر الأمنية الأخرى.

---

5. Databases Security - أمن قواعد البيانات

5.1. Access Control in Databases - التحكم في الوصول في قواعد البيانات

5.1.1. Role-Based Access Control (RBAC) - التحكم في الوصول بناءً على الدور

Definition: Role-Based Access Control (RBAC) is a method of regulating access to a database based on the roles of individual users within an organization.

التحكم في الوصول بناءً على الدور هو طريقة لتنظيم الوصول إلى قاعدة البيانات بناءً على أدوار المستخدمين داخل المنظمة

Examples:

- A database administrator has full access, while a data entry clerk has limited access to specific tables.

لدى مسؤول قاعدة البيانات وصول كامل، بينما لدى كاتب إدخال البيانات وصول محدود إلى جداول معينة

5.1.2. Mandatory Access Control (MAC) - التحكم في الوصول الإلزامي

Definition: Mandatory Access Control (MAC) is a strict access control method where the operating system or database management system enforces access rules based on predefined security policies.

التحكم في الوصول الإلزامي هو طريقة صارمة للتحكم في الوصول حيث يفرض نظام التشغيل أو نظام إدارة قواعد البيانات قواعد الوصول بناءً على سياسات أمنية محددة مسبقًا

Examples:

- Military databases where access is determined by security clearance levels.

قواعد البيانات العسكرية حيث يتم تحديد الوصول بواسطة مستويات التصريح الأمني

5.1.3. Discretionary Access Control (DAC) - التحكم في الوصول التقديري

Definition: Discretionary Access Control (DAC) allows the owner of the database or specific data to control who has access to it.

التحكم في الوصول التقديري يسمح لمالك قاعدة البيانات أو البيانات المحددة بالتحكم في من لديه حق الوصول إليها

Examples:

- A database owner granting specific users permission to access or modify certain data.

مالك قاعدة البيانات يمنح المستخدمين المحددين إذنًا للوصول إلى بيانات معينة أو تعديلها

5.2. Data Encryption - تشفير البيانات

5.2.1. Transparent Data Encryption (TDE) - التشفير الشفاف للبيانات

Definition: Transparent Data Encryption (TDE) is a method used to encrypt database files at the storage level without requiring changes to applications.

التشفير الشفاف للبيانات هو طريقة تستخدم لتشفير ملفات قاعدة البيانات على مستوى التخزين دون الحاجة إلى إجراء تغييرات على التطبيقات

Examples:

- Encrypting a database's storage files to prevent unauthorized access to data if the physical files are compromised.

تشفير ملفات تخزين قاعدة البيانات لمنع الوصول غير المصرح به إلى البيانات في حالة اختراق الملفات الفعلية

5.2.2. Field-Level Encryption - تشفير مستوى الحقل

Definition: Field-Level Encryption encrypts specific fields within a database, allowing for more granular control over data security.

تشفير مستوى الحقل يقوم بتشفير حقول معينة داخل قاعدة البيانات، مما يتيح تحكمًا أكثر دقة في أمان البيانات

Examples:

- Encrypting the "credit card number" field within a database table.

تشفير حقل "رقم بطاقة الائتمان" داخل جدول قاعدة البيانات

5.2.3. Column-Level Encryption - تشفير مستوى العمود

Definition: Column-Level Encryption encrypts entire columns of data in a database, which can be useful for securing sensitive information.

تشفير مستوى العمود يقوم بتشفير أعمدة كاملة من البيانات في قاعدة البيانات، والذي يمكن أن يكون مفيدًا لتأمين المعلومات الحساسة

Examples:

- Encrypting the "Social Security Number" column in a table to protect this sensitive information.

تشفير عمود "رقم الضمان الاجتماعي" في جدول لحماية هذه المعلومات الحساسة

5.3. Database Activity Monitoring (DAM) - مراقبة نشاط قاعدة البيانات

5.3.1. Real-Time Monitoring - المراقبة في الوقت الحقيقي

Definition: Real-time monitoring involves continuously observing database activities to detect and respond to unauthorized actions immediately.

المراقبة في الوقت الحقيقي تتضمن مراقبة أنشطة قاعدة البيانات باستمرار لاكتشاف الأنشطة غير المصرح بها والرد عليها فورًا

Examples:

- Detecting a SQL injection attack as it occurs and blocking it in real time.

اكتشاف هجوم الحقن أثناء حدوثه وحظره في الوقت الحقيقي

5.3.2. Audit Logs - سجلات التدقيق

Definition: Audit logs record all database activities, providing a historical record that can be reviewed for security and compliance purposes.

سجلات التدقيق تسجل جميع أنشطة قاعدة البيانات، مما يوفر سجلًا تاريخيًا يمكن مراجعته لأغراض الأمان والامتثال

Examples:

- Reviewing audit logs to trace the source of a data breach.

مراجعة سجلات التدقيق لتتبع مصدر اختراق البيانات

5.3.3. Behavioral Analytics - تحليلات السلوك

Definition: Behavioral analytics involves analyzing patterns of database usage to detect anomalies that may indicate security threats.

تحليلات السلوك تتضمن تحليل أنماط استخدام قاعدة البيانات لاكتشاف الشذوذات التي قد تشير إلى تهديدات أمنية

Examples:

- Identifying unusual access patterns that suggest an insider threat.

تحديد أنماط وصول غير عادية تشير إلى تهديد داخلي

5.4. Database Components - مكونات قاعدة البيانات

5.4.1. Hardware - الأجهزة

Definition: Hardware refers to the physical devices that support the operation of the database, including servers, storage devices, and network equipment.

تشير الأجهزة إلى الأجهزة المادية التي تدعم تشغيل قاعدة البيانات، بما في ذلك الخوادم وأجهزة التخزين ومعدات الشبكة

Examples:

- Servers that host the database and storage arrays where the data is stored.

الخوادم التي تستضيف قاعدة البيانات ومصفوفات التخزين التي يتم تخزين البيانات فيها

5.4.2. Software - البرامج

- **A. Database (قواعد البيانات):**

Definition: The database is the organized collection of data that is managed and accessed by a database management system (DBMS).

قاعدة البيانات هي مجموعة منظمة من البيانات يتم إدارتها والوصول إليها بواسطة نظام إدارة قواعد البيانات

Examples: Oracle, MySQL, Microsoft SQL Server.

- **B. Tables (الجداول):**

Definition: Tables organize data into rows and columns, with each row representing a record and each column representing an aspect of the data.

الجداول تنظم البيانات في صفوف وأعمدة، حيث يمثل كل صف سجلًا ويمثل كل عمود جانبًا من البيانات

Examples: A table called "Customers" with columns for CustomerID, Name, and Address.

جدول يسمى "العملاء" يحتوي على أعمدة للمعرف، الاسم، والعنوان

- **C. Rows = Tuples / Records (الصفوف = التسميات / السجلات):**

Definition: Rows in a database table represent individual records, with each row containing data for a specific instance of an entity.

الصفوف في جدول قاعدة البيانات تمثل السجلات الفردية، مع احتواء كل صف على بيانات

لحالة محددة من الكيان

Examples: A single customer's details within the "Customers" table.

"تفاصيل عميل واحد داخل جدول "العملاء

- **D. Columns = Attributes (الأعمدة = السمات):**

Definition: Columns in a database table represent the attributes of the data stored in each row, such as "Name" or "Email Address."

الأعمدة في جدول قاعدة البيانات تمثل سمات البيانات المخزنة في كل صف، مثل "الاسم" أو "عنوان البريد الإلكتروني""

Examples: The "Name" column in the "Customers" table.

"عمود "الاسم" في جدول "العملاء

- **E. Fields (الحقول):**

Definition: Fields are the individual data points at the intersection of a row and a column.

الحقول هي النقاط البيانية الفردية عند تقاطع الصف والعمود

Examples: The field containing the name "John Doe" in the "Name" column of the "Customers" table.

"الحقل الذي يحتوي على الاسم "جون دو" في عمود "الاسم" بجدول "العملاء

- **F. Primary & Foreign Keys (المفاتيح الأساسية والمفاتيح الخارجية):**

-Primary Key (المفتاح الأساسي):

Definition: A unique identifier for each record in a table, ensuring that no two rows have the same value in the primary key column.

معرف فريد لكل سجل في الجدول، يضمن عدم تكرار القيم في عمود المفتاح الأساسي

Examples: The "CustomerID" field serving as the primary key in the "Customers" table.

"حقل "معرف العميل" الذي يعمل كمفتاح أساسي في جدول "العملاء

-Foreign Key (المفتاح الخارجي):

Definition: A field in one table that uniquely identifies a row of another table, establishing a relationship between the two tables.

حقل في جدول واحد يحدد بشكل فريد صفًا في جدول آخر، ويقيم علاقة بين الجدولين

Examples: The "OrderID" field in the "Orders" table that references the "CustomerID" in the "Customers" table.

"حقل "معرف الطلب" في جدول "الطلبات" الذي يشير إلى "معرف العميل" في جدول "العملاء

5.4.3. Language (SQL) - اللغة (SQL)

Definition: Structured Query Language (SQL) is the standard language for interacting with relational databases, allowing for querying, updating, and managing the data.

لغة الاستعلامات الهيكلية هي اللغة القياسية للتفاعل مع قواعد البيانات العلائقية، مما يتيح استعلام، تحديث، وإدارة البيانات

Examples:

- Using SQL to retrieve all records from the "Customers" table.

"لاسترداد جميع السجلات من جدول "العملاء

5.4.4. Users - المستخدمين

Definition: Users refer to the individuals or processes that interact with the database, each potentially having different levels of access.

المستخدمين يشيرون إلى الأفراد أو العمليات التي تتفاعل مع قاعدة البيانات، وكل منهم قد

يكون له مستويات مختلفة من الوصول

Examples:

- Database administrators, data analysts, application users.

مسؤولي قاعدة البيانات، محللي البيانات، مستخدمي التطبيقات

5.4.5. Data - البيانات

Definition: Data is the information stored within the database, organized into tables, and accessed or manipulated through queries.

البيانات هي المعلومات المخزنة داخل قاعدة البيانات، التي يتم تنظيمها في جداول ويتم الوصول إليها أو تعديلها من خلال الاستعلامات

Examples:

- Customer names, order histories, product details.

أسماء العملاء، تاريخ الطلبات، تفاصيل المنتجات

5.5. Maintaining Integrity of Data - الحفاظ على سلامة البيانات

5.5.1. Concurrency - التزامن

Definition: Concurrency in databases ensures that multiple users can access and modify the data simultaneously without causing inconsistencies.

التزامن في قواعد البيانات يضمن أن يتمكن العديد من المستخدمين من الوصول إلى البيانات وتعديلها في نفس الوقت دون التسبب في تناقضات

Examples:

- Multiple employees updating customer records at the same time without data conflicts.

قيام عدة موظفين بتحديث سجلات العملاء في نفس الوقت دون حدوث تضارب في البيانات

5.5.2. Locks - الأقفال

Definition: Locks are mechanisms that prevent simultaneous access to data by multiple users to ensure consistency and integrity.

الأقفال هي آليات تمنع الوصول المتزامن إلى البيانات من قبل عدة مستخدمين لضمان التناسق والسلامة

Examples:

- A row-level lock that allows one transaction to update a record while preventing others from accessing it.

قفل على مستوى الصف يسمح لمعاملة واحدة بتحديث سجل بينما يمنع الآخرين من الوصول إليه

5.5.3. ACID - ACID

- **A. Atomicity (الذرية):**

Definition: Atomicity ensures that a transaction is completed fully or not at all, preventing partial updates.

الذرية تضمن أن يتم إكمال المعاملة بالكامل أو لا يتم تنفيذها على الإطلاق، مما يمنع التحديثات الجزئية

Examples: A money transfer that either moves the entire amount or cancels the transaction.

تحويل الأموال الذي إما ينقل المبلغ بالكامل أو يلغي المعاملة

- **B. Consistency (التناسق):**

Definition: Consistency ensures that a database remains in a valid state before and after a transaction.

التناسق يضمن أن تبقى قاعدة البيانات في حالة صالحة قبل وبعد المعاملة

Examples: Ensuring that account balances are accurate before and after a withdrawal.

التأكد من دقة أرصدة الحسابات قبل وبعد السحب

- **C. Isolation (العزل):**

Definition: Isolation ensures that transactions are processed independently without interference from other transactions.

العزل يضمن معالجة المعاملات بشكل مستقل دون تداخل من المعاملات الأخرى

Examples: A transaction that updates a record does not affect another transaction that is reading the same record.

معاملة تقوم بتحديث سجل لا تؤثر على معاملة أخرى تقرأ نفس السجل

- **D. Durability (الدوام):**

Definition: Durability ensures that once a transaction is committed, the changes are permanent, even in the event of a system failure.

الدوام يضمن أنه بمجرد تنفيذ المعاملة، تصبح التغييرات دائمة حتى في حالة فشل النظام

Examples: A successfully completed order remains recorded in the database even if the system crashes immediately afterward.

طلب مكتمل بنجاح يبقى مسجلاً في قاعدة البيانات حتى إذا تعطل النظام بعد ذلك مباشرة

5.6. SQL Injection - الحقن

Definition: SQL injection is a type of attack where malicious SQL code is inserted into a query to manipulate or access data in a way that was not intended.

حقن SQL هو نوع من الهجمات حيث يتم إدخال كود SQL ضار في استعلام للتحكم في البيانات أو الوصول إليها بطريقة غير مقصودة

Examples:

- An attacker entering "' OR '1'='1" into a login form to bypass authentication.

المهاجم يقوم بإدخال الكود في نموذج تسجيل الدخول لتجاوز المصادقة

Use Case

Scenario: A financial institution uses a database to store sensitive customer information, including account details and transaction histories. The institution must ensure that this data is secure, consistently available, and accessible only to authorized personnel.

تستخدم مؤسسة مالية قاعدة بيانات لتخزين معلومات العملاء الحساسة، بما في ذلك تفاصيل الحسابات وتواريخ المعاملات. يجب على المؤسسة ضمان أن تكون هذه البيانات آمنة، متاحة باستمرار، ومقتصرة على الموظفين المصرح لهم فقط

Implementation:

1. **Access Control:** The database implements Role-Based Access Control (RBAC) to ensure that only authorized personnel can access or modify customer data. For example, customer service representatives can view account balances but cannot change them, while database administrators have broader access.

التحكم في الوصول: تقوم قاعدة البيانات بتطبيق التحكم في الوصول بناءً على الدور لضمان أن يتمكن الموظفون المصرح لهم فقط من الوصول إلى بيانات العملاء أو تعديلها. على سبيل المثال، يمكن لممثلي خدمة العملاء عرض أرصدة الحسابات ولكن لا يمكنهم تغييرها، بينما يتمتع مسؤولو قاعدة البيانات بوصول أوسع.

2. **Data Encryption:** Transparent Data Encryption (TDE) is applied to protect the data at rest, ensuring that even if the physical storage media are compromised, the data remains encrypted and inaccessible.

تشفير البيانات: يتم تطبيق التشفير الشفاف للبيانات لحماية البيانات أثناء تخزينها، مما يضمن أنه حتى في حالة اختراق وسائط التخزين الفعلية، تظل البيانات مشفرة وغير قابلة للوصول.

3. **Database Activity Monitoring (DAM):** Real-time monitoring and audit logs are employed to track all access and modification activities, allowing the institution to detect and respond to unauthorized actions promptly.

مراقبة نشاط قاعدة البيانات: يتم استخدام المراقبة في الوقت الحقيقي وسجلات التدقيق لتتبع جميع أنشطة الوصول والتعديل، مما يسمح للمؤسسة باكتشاف الرد على الأنشطة غير المصرح بها بسرعة.

4. **SQL Injection Prevention:** The database implements prepared statements and input validation to protect against SQL injection attacks, ensuring that user input

cannot be used to manipulate queries.

منع الحقن تقوم قاعدة البيانات بتطبيق الاستعلامات المعدة والتحقق من المدخلات لحمايتها من هجمات حقن ، مما يضمن أن المدخلات لا يمكن استخدامها للتلاعب بالاستعلامات.

Multiple Choice Questions

1. Which access control method assigns permissions based on job functions within an organization?

- A) Discretionary Access Control (DAC)
- B) Role-Based Access Control (RBAC)
- C) Mandatory Access Control (MAC)
- D) Attribute-Based Access Control (ABAC)

2. What is the primary purpose of Transparent Data Encryption (TDE)?

- A) Encrypting specific columns within a database
- B) Encrypting data during transmission over a network
- C) Encrypting the storage files of a database
- D) Encrypting backup files

3. Which ACID property ensures that a transaction is either fully completed or not executed at all?

- A) Atomicity
- B) Consistency
- C) Isolation

- D) Durability

4. What is the purpose of SQL Injection?

- A) To enhance the performance of SQL queries
- B) To insert valid data into a database
- C) To exploit a vulnerability in the software to manipulate the database
- D) To secure data in a database

5. Which of the following is an example of a security feature in SQL?

- A) Concurrency Control
- B) SQL Injection
- C) Role-Based Access Control (RBAC)
- D) Field-Level Encryption

Answers and Explanations:

1. **B) Role-Based Access Control (RBAC)** Role-Based Access Control (RBAC) assigns permissions based on the roles individuals have within an organization, aligning access rights with job functions.

2. **C) Encrypting the storage files of a database** Transparent Data Encryption (TDE) is used to encrypt the database's storage files, ensuring that the data is protected even if the physical files are accessed.

3. **A) Atomicity** Atomicity ensures that all parts of a transaction are completed successfully, or none of them are, preserving the database's integrity.

4. **C) To exploit a vulnerability in the software to manipulate the database** SQL Injection is used to manipulate a database by inserting malicious SQL code, often to access unauthorized data or perform unauthorized operations.

5. **D) Field-Level Encryption** Field-Level Encryption is a security feature that allows individual fields within a database to be encrypted, providing more granular control over data security.

---

6. Define and Apply Secure Coding Guidelines and Standards - تعريف وتطبيق إرشادات ومعايير الترميز الآمن

6.1. Security Weaknesses and Vulnerabilities at the Source-Code Level - نقاط الضعف الأمنية والثغرات على مستوى الشيفرة المصدرية

6.1.1. Buffer Overflows - تجاوزات المخزن المؤقت

Definition: A buffer overflow occurs when more data is written to a buffer than it can hold, potentially overwriting adjacent memory and causing unexpected behavior or vulnerabilities.

تجاوزات المخزن المؤقت تحدث عندما يتم كتابة بيانات أكثر من السعة التي يمكن أن يستوعبها المخزن المؤقت، مما قد يؤدي إلى الكتابة فوق الذاكرة المجاورة ويسبب سلوكًا غير متوقع أو ثغرات

Examples:

- An attacker sending excessively large input to a vulnerable application to overwrite memory and execute arbitrary code.

مهاجم يقوم بإرسال مدخلات كبيرة جدًا إلى تطبيق ضعيف لكتابة فوق الذاكرة وتنفيذ تعليمات برمجية عشوائية

6.1.2. SQL Injection - حقن

Definition: SQL injection involves inserting malicious SQL statements into an application's input fields, allowing attackers to manipulate the database and gain unauthorized access.

الحقن يتضمن إدخال أوامر ضارة في حقول إدخال التطبيق، مما يسمح للمهاجمين بالتلاعب بقاعدة البيانات والحصول على وصول غير مصرح به

Examples:

- An attacker inputting SQL code in a login form to bypass authentication and access sensitive data.

مهاجم يقوم بإدخال كود في نموذج تسجيل الدخول لتجاوز المصادقة والوصول إلى البيانات الحساسة

6.1.3. XSS / CSRF

Definition:

- **XSS (Cross-Site Scripting):** XSS involves injecting malicious scripts into web pages viewed by other users, potentially leading to theft of session cookies or other sensitive information.

البرمجة النصية عبر المواقع: يتضمن إدخال نصوص ضارة في صفحات الويب التي يشاهدها المستخدمون الآخرون، مما قد يؤدي إلى سرقة ملفات تعريف الارتباط أو معلومات حساسة أخرى

- **CSRF (Cross-Site Request Forgery):** CSRF tricks users into performing unwanted actions on a web application where they are authenticated, potentially compromising their data.

تزوير الطلب عبر المواقع: يخدع المستخدمين لأداء إجراءات غير مرغوب فيها على تطبيق ويب حيث يكونون مصدقين، مما قد يعرض بياناتهم للخطر

Examples:

- XSS: Injecting a script into a comment field that steals cookies from other users.

إدخال نص برمجي في حقل تعليق يسرق ملفات تعريف الارتباط من المستخدمين الآخرين

- CSRF: Sending a request to change the email address of a user without their knowledge.

إرسال طلب لتغيير عنوان البريد الإلكتروني لمستخدم دون علمه

6.1.4. Covert Channels - القنوات السرية

Definition: Covert channels use unintended methods or means to communicate or exfiltrate information in a way that bypasses security controls.

القنوات السرية تستخدم طرقًا أو وسائل غير مقصودة للتواصل أو استخراج المعلومات بطريقة تتجاوز الضوابط الأمنية

Examples:

- Embedding hidden messages in non-traditional data fields or using timing-based channels to leak information.

إدراج رسائل مخفية في حقول بيانات غير تقليدية أو استخدام قنوات تعتمد على التوقيت لتسريب المعلومات

6.1.5. Backdoors - الأبواب الخلفية

Definition: Backdoors are hidden methods of bypassing normal authentication or security measures, allowing unauthorized access to a system or application.

الأبواب الخلفية هي طرق خفية لتجاوز المصادقة أو التدابير الأمنية العادية، مما يسمح بالوصول غير المصرح به إلى النظام أو التطبيق

Examples:

- A developer unintentionally leaving a hard-coded password in the code or an attacker adding a backdoor to gain access.

مطور يترك عن غير قصد كلمة مرور مشفرة في الشيفرة البرمجية أو مهاجم يضيف بابًا خلفيًا للحصول على الوصول

6.1.6. Trapdoor - الفخاخ البرمجية

Definition: Trapdoor refers to a secret entry point in software that allows someone to bypass normal authentication or access controls, often used for malicious

purposes.

الفخاخ البرمجية تشير إلى نقطة دخول سرية في البرمجيات تتيح لشخص ما تجاوز المصادقة أو ضوابط الوصول العادية، وغالبًا ما تستخدم لأغراض خبيثة

Examples:

- A developer intentionally adding a trapdoor to a system for future exploitation.

مطور يضيف عمدًا فخًا برمجيًا إلى النظام لاستغلاله في المستقبل

6.1.7. Logic Bomb - قنبلة منطقية

Definition: A logic bomb is malicious code programmed to trigger under specific conditions, often causing damage or disruption.

القنبلة المنطقية هي شيفرة خبيثة مبرمجة للتنشيط تحت ظروف معينة، مما يتسبب غالبًا في الضرر أو الاضطراب

Examples:

- Code that deletes files or corrupts data if a certain date is reached or a condition is met.

شيفرة تقوم بحذف الملفات أو إتلاف البيانات إذا تم الوصول إلى تاريخ معين أو تم استيفاء شرط معين

6.1.8. Memory Reuse - إعادة استخدام الذاكرة

Definition: Memory reuse involves using memory locations that have been previously allocated, which can lead to security issues if sensitive data is not properly cleared.

إعادة استخدام الذاكرة تتضمن استخدام مواقع الذاكرة التي تم تخصيصها مسبقًا، مما يمكن أن يؤدي إلى مشكلات أمان إذا لم يتم مسح البيانات الحساسة بشكل صحيح

Examples:

- Accessing memory locations that contain old data, potentially exposing sensitive information.

الوصول إلى مواقع الذاكرة التي تحتوي على بيانات قديمة، مما قد يعرض معلومات حساسة

6.1.9. TOCTOU - Time-of-check to time-of-use

Definition: Time-of-check to time-of-use (TOCTOU) vulnerabilities occur when there is a window of time between checking a condition and using the result, allowing an attacker to exploit changes made in that window.

ثغرات وقت التحقق إلى وقت الاستخدام تحدث عندما يكون هناك نافذة زمنية بين التحقق من شرط واستخدام النتيجة، مما يسمح للمهاجم باستغلال التغييرات التي تمت خلال تلك النافذة

Examples:

- Checking if a file is writable, then during the time before writing, an attacker replaces it with a different file.

التحقق مما إذا كان الملف قابلًا للكتابة، ثم خلال الوقت قبل الكتابة، يقوم المهاجم باستبداله بملف مختلف

6.2. Security of Application Programming Interfaces (API) - أمان واجهات برمجة التطبيقات

6.2.1. REST

Definition: Representational State Transfer (REST) is an architectural style for designing networked applications, which relies on stateless communication and uses standard HTTP methods.

نقل الحالة التمثيلية هو نمط معماري لتصميم التطبيقات الشبكية، والذي يعتمد على الاتصال بدون حالة ويستخدم الطرق القياسية

Examples:

- Using RESTful APIs to fetch data from a server and display it on a web application.

لجلب البيانات من الخادم وعرضها على تطبيق ويب

6.2.2. SOAP

Definition: Simple Object Access Protocol (SOAP) is a protocol for exchanging

structured information in web services using XML, known for its strict standards and built-in error handling.

بروتوكول الوصول البسيط للكائنات هو بروتوكول لتبادل المعلومات المنظمة في خدمات الويب باستخدام ، المعروف بمعاييره الصارمة وآلية معالجة الأخطاء المدمجة

Examples:

- Using SOAP APIs to handle transactions and ensure message integrity in enterprise applications.

لمعالجة المعاملات وضمان تكامل الرسائل في تطبيقات المؤسسات

6.3. Secure Coding Practices - ممارسات الترميز الآمن

6.3.1. Input Validation - التحقق من المدخلات

- **A. Sanitizing Inputs - تطهير المدخلات**

Definition: Sanitizing inputs involves cleaning user-provided data to remove any harmful characters or patterns that could be used in an attack.

تطهير المدخلات يتضمن تنظيف البيانات المقدمة من قبل المستخدم لإزالة أي أحرف أو أنماط ضارة قد تُستخدم في الهجوم

Examples: Removing HTML tags from user inputs to prevent XSS attacks.

إزالة العلامات مدخلات المستخدمين لمنع الهجمات

- **B. Type Checking - التحقق من النوع**

Definition: Type checking ensures that input data matches the expected data type, preventing type-related vulnerabilities.

التحقق من النوع يضمن تطابق بيانات المدخلات مع النوع المتوقع، مما يمنع الثغرات المتعلقة بالنوع

Examples: Ensuring that a numeric input field only accepts numbers and rejects non-numeric characters.

التأكد من أن حقل الإدخال الرقمي يقبل الأرقام فقط ويرفض الأحرف غير الرقمية

6.3.2. Authentication and Authorization - المصادقة والتفويض

- **A. Authentication - المصادقة**

Definition: Authentication is the process of verifying the identity of a user or system, typically through credentials such as usernames and passwords.

المصادقة هي عملية التحقق من هوية مستخدم أو نظام، عادةً من خلال بيانات الاعتماد مثل أسماء المستخدمين وكلمات المرور

Examples: Using multi-factor authentication (MFA) to enhance security by requiring additional verification methods.

استخدام المصادقة متعددة العوامل لتعزيز الأمان من خلال طلب طرق تحقق إضافية

- **B. Authorization - التفويض**

Definition: Authorization determines what an authenticated user or system is allowed to do, controlling access to resources and operations.

التفويض يحدد ما يُسمح للمستخدم أو النظام المصادق عليه القيام به، مما يتحكم في الوصول إلى الموارد والعمليات

Examples: Assigning user roles and permissions to control access to different features or data within an application.

تعيين أدوار وصلاحيات المستخدمين للتحكم في الوصول إلى ميزات أو بيانات مختلفة داخل تطبيق

6.3.3. Error Handling - معالجة الأخطاء

- **A. Generic Error Messages - رسائل الأخطاء العامة**

Definition: Generic error messages provide minimal information about the nature of an error, reducing the risk of exposing sensitive system details.

رسائل الأخطاء العامة تقدم معلومات قليلة حول طبيعة الخطأ، مما يقلل من خطر الكشف عن تفاصيل النظام الحساسة

Examples: Displaying a simple "An error occurred" message rather than detailed system errors.

عرض رسالة "حدث خطأ" بسيطة بدلاً من الأخطاء التفصيلية للنظام

- **B. Logging Errors - تسجيل الأخطاء**

Definition: Logging errors involves recording error information for analysis and troubleshooting, aiding in identifying and addressing issues.

تسجيل الأخطاء يتضمن تسجيل معلومات الخطأ للتحليل واستكشاف الأخطاء وإصلاحها، مما يساعد في تحديد ومعالجة المشكلات

Examples: Storing detailed error logs in a secure location to track and investigate application issues.

تخزين سجلات الأخطاء التفصيلية في موقع آمن لتتبع واستكشاف مشكلات التطبيق

6.4. Software-Defined Security - الأمان المعرف بالبرمجيات

Definition: Software-defined security (SDS) refers to security mechanisms that are managed and controlled through software, enabling dynamic, policy-based security management.

الأمان المعرف بالبرمجيات يشير إلى آليات الأمان التي يتم إدارتها والتحكم فيها من خلال البرمجيات، مما يتيح إدارة الأمان الديناميكية القائمة على السياسات

Examples:

- Implementing virtual firewalls and security policies that can be adjusted through centralized management platforms.

تنفيذ جدران الحماية الافتراضية وسياسات الأمان التي يمكن تعديلها من خلال منصات الإدارة المركزية

Use Case

Scenario: A software development company is implementing secure coding practices to protect their applications from vulnerabilities. They need to ensure that their codebase is resilient against common attacks and follows industry standards for security.

شركة تطوير برمجيات تقوم بتنفيذ ممارسات الترميز الآمن لحماية تطبيقاتها من الثغرات. يحتاجون إلى ضمان أن تكون قاعدة الشيفرة الخاصة بهم مقاومة للهجمات الشائعة وتتبع معايير الصناعة للأمان

Implementation:

1. **Buffer Overflow Protection:** The development team implements secure coding practices to avoid buffer overflows by using safe functions and performing proper input validation.

حماية من تجاوزات المخزن المؤقت: يقوم فريق التطوير بتطبيق ممارسات الترميز الآمن لتجنب تجاوزات المخزن المؤقت من خلال استخدام دوال آمنة وإجراء التحقق المناسب من المدخلات.

2. **API Security:** The team ensures that APIs are protected by using secure protocols (such as HTTPS for REST) and implementing proper authentication and authorization mechanisms.

يتأكد الفريق من أنها محمية من خلال استخدام بروتوكولات آمنة وتنفيذ آليات المصادقة والتفويض المناسبة.

3. **Secure Error Handling:** Generic error messages are used to prevent the leakage of sensitive information, and detailed error logging is implemented for internal analysis.

معالجة الأخطاء الآمنة: يتم استخدام رسائل الأخطاء العامة لمنع تسرب المعلومات الحساسة، ويتم تنفيذ تسجيل الأخطاء التفصيلية للتحليل الداخلي.

4. **Memory Management:** The team applies best practices for memory management, including proper clearing of memory and avoiding reuse of sensitive data.

إدارة الذاكرة: يقوم الفريق بتطبيق أفضل الممارسات لإدارة الذاكرة، بما في ذلك مسح الذاكرة بشكل صحيح وتجنب إعادة استخدام البيانات الحساسة.

5. **Software-Defined Security:** Virtual security appliances and policy-based

management are used to adapt security measures to evolving threats dynamically.

الأمان المعرف بالبرمجيات: يتم استخدام الأجهزة الأمنية الافتراضية وإدارة السياسات للتكيف مع التدابير الأمنية لتلبية التهديدات المتطورة بشكل ديناميكي.

Multiple-Choice Questions

1. What is a common method to prevent buffer overflow vulnerabilities?

A. Using unbounded string functions

B. Validating input sizes

C. Ignoring memory management

D. Employing weak input validation

2. Which of the following is an example of a method to protect APIs?

A. Using unencrypted HTTP

B. Implementing proper authentication and authorization

C. Ignoring input validation

D. Allowing open access to APIs

3. What is a secure practice for handling errors in an application?

A. Displaying detailed error messages to users

B. Logging errors in a secure location

C. Ignoring error messages

D. Using generic error messages and not logging errors

4. Which type of attack can be prevented by using parameterized queries?

A. Cross-Site Scripting (XSS)

B. SQL Injection

C. Buffer Overflow

D. Denial of Service (DoS)

5. What is a benefit of using software-defined security (SDS)?

A. Static security measures

B. Dynamic, policy-based management

C. Reduced security flexibility

D. Manual configuration of security settings

Answers and Explanation

1. Answer: B. Validating input sizes

Explanation: Validating input sizes ensures that the data written to a buffer does not exceed its capacity, thus preventing buffer overflows.التحقق من أحجام المدخلات يضمن أن البيانات المكتوبة إلى المخزن المؤقت لا تتجاوز سعتها، مما يمنع تجاوزات المخزن المؤقت.

2. Answer: B. Implementing proper authentication and authorization

Explanation: Implementing proper authentication and authorization ensures that only authorized users can access the API and perform allowed actions.تنفيذ المصادقة والتفويض المناسبين يضمن أن المستخدمين المصرح لهم فقط يمكنهم الوصول وأداء الإجراءات المسموح بها

3. Answer: B. Logging errors in a secure location

Explanation: Logging errors in a secure location helps in tracking and analyzing

issues while preventing sensitive information from being exposed to users.

تسجيل الأخطاء في موقع آمن يساعد في تتبع وتحليل المشكلات بينما يمنع الكشف عن المعلومات الحساسة للمستخدمين.

4. Answer: B. SQL Injection

Explanation: Parameterized queries prevent SQL injection by ensuring that user input is treated as data rather than executable code.

الاستعلامات المهيأة تمنع الحقن من خلال ضمان أن يتم التعامل مع مدخلات المستخدم كبيانات بدلاً من الشيفرة القابلة للتنفيذ.

5. Answer: B. Dynamic, policy-based management

Explanation: Software-defined security enables dynamic adjustments of security measures based on evolving threats and policies, enhancing adaptability and responsiveness.الأمان المعرف بالبرمجيات يتيح التعديلات الديناميكية لتدابير الأمان بناءً على التهديدات والسياسات المتطورة، مما يعزز التكيف والاستجابة.

---

7. Application Security Controls - ضوابط أمان التطبيقات

Definition: Application security controls refer to measures implemented within applications to protect them from threats and vulnerabilities, ensuring that the software performs securely and as intended.

ضوابط أمان التطبيقات تشير إلى التدابير التي يتم تنفيذها داخل التطبيقات لحمايتها من التهديدات والثغرات، وضمان أن البرنامج يعمل بأمان وكما هو مقصود.

Purpose: The purpose of application security controls is to safeguard applications from various types of attacks, protect sensitive data, ensure compliance with security policies, and enhance overall system reliability.

الغرض من ضوابط أمان التطبيقات هو حماية التطبيقات من أنواع مختلفة من الهجمات، وحماية البيانات الحساسة، وضمان الامتثال لسياسات الأمان، وتعزيز موثوقية النظام بشكل

عام.

7.1. Input Validation - التحقق من المدخلات

Definition: Input validation is the process of verifying that input data meets certain criteria before processing it. This helps prevent malicious data from entering the system and causing security issues.

التحقق من المدخلات هو عملية التحقق من أن بيانات المدخلات تلبي معايير معينة قبل معالجتها. يساعد ذلك في منع البيانات الخبيثة من الدخول إلى النظام والتسبب في مشكلات أمنية.

Purpose: The purpose of input validation is to ensure that only valid data is accepted by the application, preventing security vulnerabilities such as SQL injection, XSS, and buffer overflows.

الغاية من التحقق من المدخلات هي ضمان قبول البيانات الصالحة فقط من قبل التطبيق، مما يمنع الثغرات الأمنية

7.1.1. Whitelist Validation - التحقق من القوائم البيضاء

Definition: Whitelist validation involves defining a list of acceptable input values or formats. Inputs that match the criteria are allowed, while others are rejected.

التحقق من القوائم البيضاء ينطوي على تحديد قائمة بالقيم أو التنسيقات المقبولة للمدخلات. يتم السماح بالمدخلات التي تتطابق مع المعايير، بينما يتم رفض الآخرين.

Examples:

- Allowing only predefined options in a dropdown menu.

السماح فقط بالخيارات المحددة مسبقًا في قائمة منسدلة.

7.1.2. Length Checks - التحقق من الطول

Definition: Length checks ensure that input data does not exceed the maximum allowed length, preventing buffer overflow vulnerabilities and ensuring consistent data processing.

التحقق من الطول يضمن أن بيانات المدخلات لا تتجاوز الطول الأقصى المسموح به، مما يمنع ثغرات تجاوز المخزن المؤقت ويضمن معالجة البيانات بشكل متسق.

Examples:

- Limiting a username to a maximum of 20 characters.

تحديد اسم المستخدم بحد أقصى قدره 20 حرفًا.

7.1.3. Format Validation - التحقق من التنسيق

Definition: Format validation involves checking that input data conforms to a specific format or pattern, such as email addresses or phone numbers.

التحقق من التنسيق يتضمن التحقق من أن بيانات المدخلات تتوافق مع تنسيق أو نمط محدد، مثل عناوين البريد الإلكتروني أو أرقام الهواتف.

Examples:

- Verifying that an email address contains "@" and a domain name.

التحقق من أن عنوان البريد الإلكتروني يحتوي على "@" واسم النطاق.

Use Case

Scenario: An e-commerce website implements input validation to prevent security vulnerabilities. They use whitelist validation to ensure only allowed product categories are submitted, perform length checks to avoid buffer overflow issues, and validate email format to ensure proper user registration.

موقع التجارة الإلكترونية ينفذ التحقق من المدخلات لمنع الثغرات الأمنية. يستخدمون التحقق من القوائم البيضاء لضمان تقديم فئات المنتجات المسموح بها فقط، ويقومون بإجراء التحقق من الطول لتجنب مشاكل تجاوز المخزن المؤقت، ويتحققون من تنسيق البريد الإلكتروني لضمان تسجيل المستخدمين بشكل صحيح.

Implementation:

1. **Whitelist Validation:** Only specific product categories are accepted through the form.

التحقق من القوائم البيضاء: يتم قبول فئات المنتجات المحددة فقط من خلال النموذج.

2. **Length Checks:** Usernames are limited to 20 characters to avoid overflow issues.

التحقق من الطول: يتم تحديد أسماء المستخدمين بحد أقصى 20 حرفًا لتجنب مشاكل تجاوز المخزن المؤقت.

3. **Format Validation:** Email addresses are validated to ensure they follow a correct pattern.

التحقق من التنسيق: يتم التحقق من عناوين البريد الإلكتروني للتأكد من أنها تتبع نمطًا صحيحًا.

7.2. Authentication and Authorization - المصادقة والتفويض

Definition: Authentication and authorization are processes used to verify the identity of users and determine their access rights to resources and functionalities within an application.

المصادقة والتفويض هما عمليات تُستخدم للتحقق من هوية المستخدمين وتحديد حقوق وصولهم إلى الموارد والوظائف داخل التطبيق.

Purpose: The purpose of authentication is to confirm that users are who they claim to be, while authorization ensures that authenticated users have the appropriate permissions to access or perform actions on resources.

الغرض من المصادقة هو التأكد من أن المستخدمين هم من يدعون أنهم، بينما التفويض يضمن أن المستخدمين المصادق عليهم لديهم الأذونات المناسبة للوصول إلى الموارد أو تنفيذ إجراءات عليها.

7.2.1. Multi-Factor Authentication (MFA) - المصادقة متعددة العوامل

Definition: Multi-Factor Authentication (MFA) requires users to provide two or more verification factors to gain access, adding an additional layer of security.

المصادقة متعددة العوامل تتطلب من المستخدمين تقديم عاملين أو أكثر من عوامل التحقق للوصول، مما يضيف طبقة إضافية من الأمان.

Examples:

- Combining a password with a one-time code sent to a mobile device.

دمج كلمة مرور مع رمز لمرة واحدة يتم إرساله إلى جهاز محمول.

7.2.2. Role-Based Authorization - التفويض القائم على الدور

Definition: Role-based authorization assigns permissions based on user roles, ensuring that individuals only have access to resources necessary for their role.

التفويض القائم على الدور يخصص الأذونات بناءً على أدوار المستخدمين، مما يضمن أن الأفراد لديهم فقط الوصول إلى الموارد الضرورية لدورهم.

Examples:

- Granting administrative access to system administrators while limiting regular users to basic functionalities.

منح الوصول الإداري لمشرفي النظام بينما يقتصر المستخدمون العاديون على الوظائف الأساسية.

7.2.3. Single Sign-On (SSO) - تسجيل الدخول الأحادي

Definition: Single Sign-On (SSO) allows users to authenticate once and gain access to multiple applications or systems without re-entering credentials.

تسجيل الدخول الأحادي يتيح للمستخدمين المصادقة مرة واحدة والوصول إلى تطبيقات أو أنظمة متعددة دون إعادة إدخال بيانات الاعتماد.

Examples:

- Logging into an email account and automatically being logged into associated productivity tools.

تسجيل الدخول إلى حساب البريد الإلكتروني والدخول تلقائيًا إلى أدوات الإنتاجية المرتبطة.

Use Case

Scenario: A financial services company implements authentication and authorization controls to enhance security. They use MFA for login, role-based authorization to

restrict access based on job functions, and SSO to streamline user access to various systems.

شركة خدمات مالية تنفذ ضوابط المصادقة والتفويض لتعزيز الأمان. يستخدمون المصادقة متعددة العوامل لتسجيل الدخول، والتفويض القائم على الدور لتقييد الوصول بناءً على وظائف العمل، وتسجيل الدخول الأحادي لتبسيط وصول المستخدمين إلى أنظمة متعددة.

Implementation:

1. **Multi-Factor Authentication (MFA):** Users must provide a password and a verification code to log in.

المصادقة متعددة العوامل يجب على المستخدمين تقديم كلمة مرور ورمز تحقق لتسجيل الدخول.

2. **Role-Based Authorization:** Access is granted based on user roles, with admins having broader access.

التفويض القائم على الدور: يتم منح الوصول بناءً على أدوار المستخدمين، مع منح المشرفين وصولًا أوسع.

3. **Single Sign-On (SSO):** Users can access multiple applications with a single login session.

تسجيل الدخول الأحادي يمكن للمستخدمين الوصول إلى تطبيقات متعددة بجلسة تسجيل دخول واحدة.

7.3. Secure Session Management - إدارة الجلسات الآمنة

Definition: Secure session management involves controlling and protecting user sessions to ensure that session information is secure and not exposed to unauthorized parties.

إدارة الجلسات الآمنة تتضمن التحكم وحماية جلسات المستخدم لضمان أن معلومات الجلسة آمنة وغير مكشوفة لأطراف غير مصرح بها.

Purpose: The purpose of secure session management is to prevent session hijacking, fixation, and other session-related attacks by ensuring proper handling and protection of session data.

الغاية من إدارة الجلسات الآمنة هي منع اختطاف الجلسات والتثبيت والهجمات الأخرى

المتعلقة بالجلسات من خلال ضمان التعامل السليم وحماية بيانات الجلسة.

7.3.1. Session ID Randomization - عشوائية معرّف الجلسة

Definition: Session ID randomization involves generating unpredictable session identifiers to prevent attackers from guessing or predicting session IDs.

عشوائية معرّف الجلسة تتضمن توليد معرّفات جلسة غير قابلة للتوقع لمنع المهاجمين من تخمين أو التنبؤ بمعرّفات الجلسة.

Examples:

- Using cryptographically secure random number generators for session IDs.

استخدام مولدات أرقام عشوائية آمنة من الناحية التشفيرية لمعرّفات الجلسة.

7.3.2. Session Expiry - انتهاء الجلسة

Definition: Session expiry refers to the automatic termination of a session after a period of inactivity or a predefined duration.

انتهاء الجلسة يشير إلى إنهاء الجلسة تلقائيًا بعد فترة من عدم النشاط أو مدة محددة مسبقًا.

Examples:

- Logging out users automatically after 15 minutes of inactivity.

تسجيل خروج المستخدمين تلقائيًا بعد 15 دقيقة من عدم النشاط.

7.3.3. Secure Cookies - ملفات تعريف الارتباط الآمنة

Definition: Secure cookies are cookies that are transmitted over secure channels (e.g., HTTPS) and have attributes set to ensure they are not accessible via client-side scripts.

ملفات تعريف الارتباط الآمنة هي ملفات تعريف الارتباط التي يتم نقلها عبر قنوات آمنة وتحتوي على سمات لضمان عدم الوصول إليها عبر السكربتات من جانب العميل .

Examples:

- Setting the "Secure" and "HttpOnly" flags on cookies to enhance their security.

تعيين العلامات على ملفات تعريف الارتباط لتعزيز أمانها.

Use Case

Scenario: A web application implements secure session management to protect user sessions. They use session ID randomization to prevent session guessing, set sessions to expire after inactivity, and ensure cookies are transmitted securely with appropriate attributes.

تطبيق ويب ينفذ إدارة الجلسات الآمنة لحماية جلسات المستخدمين. يستخدمون عشوائية معرّف الجلسة لمنع تخمين الجلسات، ويحددون انتهاء الجلسات بعد عدم النشاط، ويضمنون أن يتم نقل ملفات تعريف الارتباط بأمان مع السمات المناسبة.

Implementation:

1. **Session ID Randomization:** Generates session IDs using secure random number generators.

عشوائية معرّف الجلسة: توليد معرّفات الجلسة باستخدام مولدات أرقام عشوائية آمنة.

2. **Session Expiry:** Sessions automatically expire after 30 minutes of inactivity.

انتهاء الجلسة: تنتهي الجلسات تلقائيًا بعد 30 دقيقة من عدم النشاط.

3. **Secure Cookies:** Cookies are marked as "Secure" and "HttpOnly" to prevent unauthorized access.

ملفات تعريف الارتباط الآمنة: يتم وضع علامة على ملفات تعريف الارتباط لمنع الوصول غير المصرح به.

7.4. Error Handling and Logging - معالجة الأخطاء والتسجيل

Definition: Error handling and logging involve managing and recording errors that occur within an application. Proper handling and logging are crucial for troubleshooting, maintaining application security, and ensuring compliance.

معالجة الأخطاء والتسجيل تتضمن إدارة وتسجيل الأخطاء التي تحدث داخل التطبيق. المعالجة والتسجيل المناسبان أمران حاسمان لاستكشاف الأخطاء وإصلاحها، والحفاظ على أمان التطبيق،

وضمان الامتثال.

Purpose: The purpose of error handling and logging is to identify, analyze, and address issues effectively while maintaining the security and integrity of the application.

الغرض من معالجة الأخطاء والتسجيل هو تحديد وتحليل ومعالجة المشكلات بفعالية مع الحفاظ على أمان وسلامة التطبيق.

7.4.1. Generic Error Messages - رسائل الأخطاء العامة

Definition: Generic error messages provide minimal information to users, avoiding the disclosure of sensitive details about the system's inner workings.

رسائل الأخطاء العامة تقدم معلومات قليلة للمستخدمين، مما يتجنب الكشف عن تفاصيل حساسة حول طريقة عمل النظام الداخلية.

Examples:

- Displaying a simple "An error occurred" message rather than detailed system errors.

عرض رسالة "حدث خطأ" بسيطة بدلاً من الأخطاء التفصيلية للنظام.

7.4.2. Detailed Logging - التسجيل التفصيلي

Definition: Detailed logging involves recording comprehensive information about errors, including the context and specifics of the issues, for effective troubleshooting.

التسجيل التفصيلي يتضمن تسجيل معلومات شاملة عن الأخطاء، بما في ذلك السياق وتفاصيل المشكلات، لاستكشاف الأخطاء وإصلاحها بشكل فعال.

Examples:

- Logging error codes, stack traces, and user actions leading up to the error.

تسجيل رموز الأخطاء، وأثر التتبع، وإجراءات المستخدمين التي أدت إلى الخطأ.

7.4.3. Audit Trails - سجلات التدقيق

Definition: Audit trails are records of all actions and changes within an application, providing a chronological history for security audits and compliance.

سجلات التدقيق هي سجلات لجميع الإجراءات والتغييرات داخل التطبيق، مما يوفر تاريخًا زمنيًا للتدقيق الأمني والامتثال.

Examples:

- Maintaining logs of user login attempts, data modifications, and system changes.

الحفاظ على سجلات محاولات تسجيل دخول المستخدمين، وتعديلات البيانات، وتغييرات النظام.

Use Case

Scenario: An online banking application integrates error handling and logging mechanisms to monitor and address issues. They use generic error messages for users, detailed logs for troubleshooting, and audit trails for security reviews.

تطبيق بنكي عبر الإنترنت يدمج آليات معالجة الأخطاء والتسجيل لمراقبة ومعالجة المشكلات. يستخدمون رسائل أخطاء عامة للمستخدمين، وسجلات تفصيلية لاستكشاف الأخطاء وإصلاحها، وسجلات تدقيق للمراجعات الأمنية.

Implementation:

1. **Generic Error Messages:** Users receive a generic "An error occurred" message during issues.

رسائل الأخطاء العامة: يتلقى المستخدمون رسالة "حدث خطأ" عامة خلال المشكلات.

2. **Detailed Logging:** All errors are logged with detailed context, including user actions and system status.

التسجيل التفصيلي: يتم تسجيل جميع الأخطاء بسياق تفصيلي، بما في ذلك إجراءات المستخدمين وحالة النظام.

3. **Audit Trails:** Comprehensive audit trails are maintained for all significant actions and changes.

سجلات التدقيق: يتم الحفاظ على سجلات تدقيق شاملة لجميع الإجراءات والتغييرات المهمة.

Multiple-Choice Questions

1. What is the primary purpose of input validation in application security?

A. To format data for display

B. To ensure data is properly processed

C. To reject invalid or malicious data

D. To encrypt sensitive data

2. How does Multi-Factor Authentication (MFA) enhance security?

A. By using only passwords for login

B. By requiring additional verification factors

C. By eliminating the need for passwords

D. By allowing single sign-on (SSO)

3. What is a common practice to secure session cookies?

A. Setting cookies to be accessible via JavaScript

B. Using the "Secure" and "HttpOnly" flags

C. Allowing cookies to be sent over HTTP

D. Storing cookies in local storage

4. What should be included in detailed logging for effective troubleshooting?

A. Only error messages

B. User actions and error context

C. System uptime records

D. External API call logs

5. What is the main advantage of using role-based authorization?

A. It simplifies user interface design

B. It provides a single login for multiple systems

C. It ensures users only access resources they need

D. It generates random session IDs

Answers and Explanation

1. Answer: C. To reject invalid or malicious data

Explanation: Input validation ensures that only valid and safe data is accepted by the application, preventing potential security threats.

التحقق من المدخلات يضمن قبول البيانات الصالحة والآمنة فقط من قبل التطبيق، مما يمنع التهديدات الأمنية المحتملة.

2. Answer: B. By requiring additional verification factors

Explanation: MFA enhances security by requiring users to provide multiple forms of verification, making unauthorized access more difficult. تعمل على تعزيز الأمان من خلال طلب عدة أشكال من التحقق من المستخدمين، مما يجعل الوصول غير المصرح به أكثر صعوبة.

3. Answer: B. Using the "Secure" and "HttpOnly" flags

Explanation: Setting cookies with the "Secure" and "HttpOnly" flags helps prevent unauthorized access and enhances security by ensuring cookies are only transmitted over secure channels and are not accessible via client-side scripts.

تعيين ملفات تعريف الارتباط يساعد في منع الوصول غير المصرح به ويعزز الأمان من خلال ضمان إرسال ملفات تعريف الارتباط عبر قنوات آمنة فقط وعدم الوصول إليها عبر السكربتات من جانب العميل.

4. Answer: B. User actions and error context

Explanation: Detailed logging should include user actions and the context of the errors to effectively diagnose and resolve issues.

يجب أن يتضمن التسجيل التفصيلي إجراءات المستخدمين وسياق الأخطاء لتشخيص المشكلات وحلها بشكل فعال.

5. Answer: C. It ensures users only access resources they need

Explanation: Role-based authorization ensures that users have access only to the resources necessary for their roles, enhancing security and minimizing potential risks.

يضمن التفويض القائم على الدور أن يحصل المستخدمون على الوصول فقط إلى الموارد اللازمة لأدوارهم، مما يعزز الأمان ويقلل من المخاطر المحتملة.

Conclusion

This module highlighted the importance of integrating security throughout the Software Development Life Cycle (SDLC) to protect against vulnerabilities and threats. تسلط هذه الوحدة الضوء على أهمية دمج الأمان طوال دورة حياة تطوير البرمجيات لحماية البرمجيات من الثغرات والتهديدات

By identifying and applying appropriate security controls, assessing software security effectiveness, and evaluating the security impact of acquired software, organizations can significantly reduce risks. من خلال تحديد وتطبيق ضوابط الأمان المناسبة وتقييم فعالية أمان البرمجيات وتقييم تأثير الأمان للبرمجيات المكتسبة يمكن للمنظمات تقليل المخاطر بشكل كبير

Additionally, adhering to secure coding guidelines and implementing robust application security controls are essential practices for ensuring that software remains secure, resilient, and compliant with industry standards. بالإضافة إلى ذلك فإن الالتزام بإرشادات البرمجة الآمنة وتنفيذ ضوابط أمان التطبيقات القوية هي ممارسات أساسية

لضمان بقاء البرمجيات آمنة ومرنة ومتوافقة مع معايير الصناعة

Resources

1- Official (ISC)² CISSP Study Guide

2- CISSP (ISC)² Official Practice Tests

3- CISSP All-in-One Exam Guide by Shon Harris

4- Cybrary – CISSP Training by Kelly Handerhan

https://www.cybrary.it/course/cissp

5- Oreilly – CISSP Training by Sari Greene

https://www.oreilly.com/library/view/cissp-4th-edition/9780135328613/?_gl=1*jwhz1z*_ga*MTgyMDY2NDI5LjE3MTczNzAwMDI.*_ga_092EL089CH*MTcxNzM3MDAwMi4xLjEuMTcxNzM3MDEwNi41OC4wLjA.

6- CISSP bundles by Thor Pedersen

https://thorteaches.com/cissp/

7- CISSP MindMaps YouTube Playlist from Destination Certification

https://www.youtube.com/playlist?list=PLZKdGEfEyJhLd-pJhAD7dNbJyUgpqI4pu

---

تم بحمد الله انهاء الشرح المختصر للمادة العلمية لشهادة مهندس أمن نظم معلومات معتمد

#CISSP Certified information systems security professional

أسئل الله العظيم ان يكون هذا العمل خالص لوجهه، وادعوا كل من أستفد من المادة العلمية الدعاء ل أمي وأبى بالرحمة

والسلام عليكم ورحمة الله وبركاته

Mohamed Hesham Abdelmotaleb 2h

جزاك الله خير و جعله في ميزان حسناتك يا بشمهندس عماد

Like · Reply | 1 Reaction

HARDI Othman 2h
Programmer

ماشاء الله وعلم ينتفع به

Like · Reply | 1 Reaction

Omar Alalwi 9h
Technical Lead | Team Lead | Software Engineer | Senior Full Stack Developer (Laravel & Vue.js) | Database Analyst |...

ماشاء الله , كتب الله اجرك وزادك علماً ..
ان شاء الله نقتدي بك ونرتب لمحتوى عربي في مجالنا

Like · Reply | 1 Reaction

OUSAMA AL TAHA 19h
Cyber Security Engineer at NASCO

وفقك الله تعالى

Like · Reply | 1 Reaction

Gassim M. Abbas, MBA, PMP®, CISA, ITIL®, MCSA 21h
IT Project Management | IT Auditing | IT Service Management

جزاك الله خيرا..

Like · Reply | 1 Reaction

See more comments

More articles by this author

Module 7: Security Operations / إدارة عمليات...
Aug 5, 2024

Module 6: Security Assessment and Testing...
Jul 28, 2024

CISSP Module 5: Identi and Access Manageme
Jul 8, 2024

See all

Explore topics

- Sales
- Marketing
- Business Administration
- HR Management
- Content Management
- Engineering
- Soft Skills
- See All