مركز عمليات الأمن 450 مترجم إلي اللغة العربية

الكتاب الأول:

الفريق الأزرق: الأدوات والعمليات

يوجد مرفق القاموس فى اخر الكتاب يحتوي على بعض الكلمات وترجمتها

أهلا بيك في فريق الدفاع الأزرق!

لو لسه جديد في مجال عمليات الأمن، فأهلاً وسهلاً بيك!

- إحنا مبسوطين إنك انضميت لنا!
- المؤسسات محتاجة لمساعدتك.
- الدفاع السيبراني...
  - صناعة عظيمة تشتغل فيها.
  - واحدة من أكتر الوظايف تحديًا ومطلوبة جدًا في مجال الأمن السيبراني!
- الكورس ده هيكون البداية (أو هيكمل معاك الرحلة)!

أهلا بيك في فريق الدفاع الأزرق!

مرحبًا بك في كورس **SEC450: أساسيات فريق الدفاع الأزرق: عمليات الأمن والتحليل**. لو انت جديد في مجال أمن المعلومات ومراكز عمليات الأمن(SOC) ، استعد لرحلة مليانة تحديات ومغامرات!

الدفاع السيبراني هو بلا شك واحد من أكتر الوظائف إثارة وتحدي في مجال أمن المعلومات. مع تزايد الهجمات بشكل مستمر وبقوة مدمرة، دور الدفاع السيبراني هيكون مطلوب بشدة لسنين جاية.

يمكن تكون شوفت أدوات الهجوم قبل كده وافتكرت قد إيه الأفكار اللي وراها عبقرية. لكن صدقني، مش بس ممكن تعمل حاجات مذهلة على الجانب الدفاعي، كمان فيه فرص أكتر للإبداع والتطور.

في الماضي، فرق الدفاع كانت دايمًا ورا أحدث الهجمات بسبب السرعة الكبيرة اللي بتتطور بيها أدوات الاختراق، لكن دلوقتي إحنا في وقت مثير جدًا. أدوات فريق الدفاع الأزرق بقت متقدمة جدًا، وإطارات دفاعية زي **MITRE ATT&CK** ساعدت فريق الدفاع إنه يلحق بركب التطور، وده بيحصل بشكل مستمر وبسرعة رهيبة.

فيه حاجات مثيرة كتير بتحصل في مجال الدفاع، ومن وجهة نظر الكاتب، مفيش وقت أحسن من دلوقتي علشان تنضم لفريق الدفاع الأزرق. الكورس ده معمول علشان يساعد المبتدئين في عمليات الدفاع، سواء كنت فريق لوحدك أو عضو جديد في مركز عمليات أمن .(SOC) هدفه هو يديك طريقة التفكير والمعرفة والخبرة العملية اللي تخليك ناجح في الدفاع السيبراني الحديث.

من غير ما نضيع وقت أكتر، يلا نبدأ!

عن هذا الكورس

الكورس ده معمول مخصوص لأعضاء فرق الدفاع السيبراني، واللي بيقوموا بتدريبهم، العمل معاهم، أو إدارتهم.

- هنغطي مجموعة من أساسيات فريق الدفاع الأزرق:(Blue Team)
  - **الأشخاص** :طريقة التفكير، النماذج الذهنية، تطور المهنة، وكيفية التعامل مع الإرهاق المهني.
  - **العمليات** :التحليل، نظرية التحقيق، إدارة الأولويات(Triage) ، وتدفق البيانات.
  - **التكنولوجيا** :مراقبة الشبكة والأجهزة، فهم البروتوكولات، اكتشاف الهجمات، البرمجة التلقائية والتشغيل الآلي.
  - معلومات على المستوى الاستراتيجي، التشغيلي، والتكتيكي.
- **ليه تم كتابة الكورس ده؟** لتحقيق تدريب معياري في المجال، وإحنا محتاجين مساعدتكم!

عن هذا الكورس

الكورس ده موجه لكل اللي شغالين في عمليات الدفاع السيبراني اليومية - المحللين، مديري مراكز العمليات الأمنية(SOC) ، المهندسين، وأي شخص بيساهم في منع الهجمات واكتشافها. سواء عندك مركز عمليات أمني كامل أو فريق من شخص واحد، المفاهيم والأدوات اللي هنا هتساعدك تقدم أفضل ما عندك.

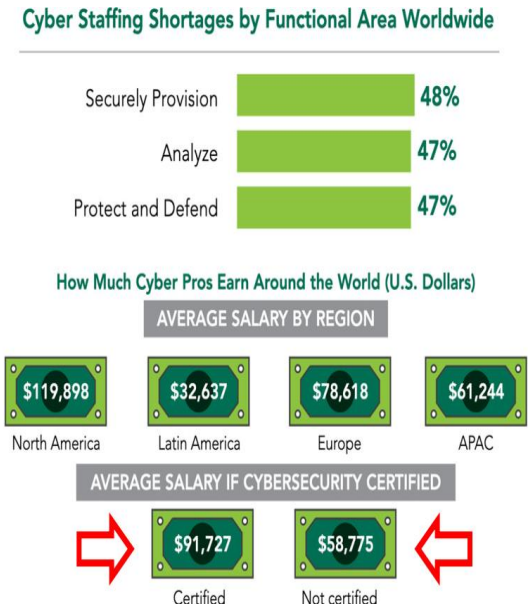
نجاح عمليات الأمن بيعتمد على 3 عوامل رئيسية :**الأشخاص، العمليات، والتكنولوجيا**، وإحنا هنغطي الثلاثة.

- **من ناحية العمليات** :هنشرح تدفقات العمل والإجراءات اللي بياخدها عضو فريق الدفاع الأزرق العادي، وهنوضح إزاي نخليها أكتر كفاءة باستخدام التشغيل الآلي وتقليل الأعمال اليدوية على قد ما نقدر.
- **من ناحية التكنولوجيا** :هنناقش الأدوات الأساسية ومصادر البيانات اللي بتكون عند أغلب فرق عمليات الأمن، وهنعلمك إزاي تستخدمها بأفضل طريقة.
- **العنصر البشري** :هو ده اللي إحنا هنا عشانه، مش كده؟ من خلال الكتب الستة دي، هنغطي مجموعة كبيرة من المواضيع مع شروحات معمقة وأنشطة عملية علشان تسهل التعلم بأسرع طريقة ممكنة.

ليه تم إنشاء الكورس ده؟ لأن مدافعين الأمن السيبراني، أو اللي بنسميهم عادةً "فرق الدفاع الأزرق"، محتاجين بشدة توجيه ومساعدة لتحديد الأولويات وإزاي يستفيدوا بأقصى شكل من اللي عندهم! أدواتنا وعملياتنا بتتطور بسرعة، وتكنولوجيتنا ممتازة لو اتستخدمت بالشكل الصحيح، لكن عندنا نقص كبير في الأشخاص اللي جاهزين للدخول في دور عمليات الأمن.

علشان كده، تركيز الكورس هيكون على تطوير مهاراتك، علشان تكون جاهز فورًا لفهم التحليل التقني واتخاذ الإجراءات الصحيحة لما يجي المهاجمين يطرقوا على أبوابك الافتراضية!

حالة الصناعة



النقاط الرئيسية من دراسة **ISC2 Workforce** العالمية لعام 2021:

- يوجد **4.19مليون** موظف في مجال الأمن السيبراني على مستوى العالم.
- تم توظيف **700ألف** متخصص في أمن المعلومات في عام 2020 فقط.
- لكننا ما زلنا نواجه نقصًا يقدر بـ **2.72مليون** عامل!
- أعلى نسب النقص كانت في الوظائف المتعلقة بالتأمين، التحليل، والحماية والدفاع.
- نقص العاملين والرواتب العالية المتاحة يجعل التوظيف والاحتفاظ بالمواهب تحديًا كبيرًا!

حالة الصناعة

ما حجم الفجوة في القوى العاملة في مجال الأمن السيبراني؟

وفقًا لدراسة القوى العاملة العالمية لعام 2021 التي أجرتها **ISC2**، بالرغم من إضافة **700,000 شخص** جديد للقوى العاملة، فإن الطلب ما زال يتفوق على العرض. ما زلنا نواجه نقصًا يقدر بحوالي **2.72مليون وظيفة** في مجال الأمن السيبراني!

من منظور عمليات الأمن السيبراني، الدراسة لاحظت أن النقص في الموظفين هو الأعلى في الأدوار المرتبطة بالتأمين، التحليل، والحماية/الدفاع (وهي الوظائف التي تخص معظم المشاركين في هذا الكورس).

هذا الاحتياج الكبير للعاملين، مع توفر رواتب مرتفعة، يعني أن السوق حاليًا في صالح الموظفين! الشريحة أعلاه تعرض نتائج استطلاع ISC2 بخصوص متوسط الرواتب العالمية لوظائف أمن المعلومات، بالإضافة إلى الزيادة الواضحة في متوسط الرواتب لمن يحصلون على شهادات معتمدة في الأمن السيبراني.

كل هذا يعني أن الخيارات الوظيفية لا تزال وفيرة بالنسبة للموظفين. ولكن على الجانب الآخر، قد يواجه المدراء تحديات أكبر، حيث أن كثرة الوظائف المتاحة قد تجعل من الصعب الاحتفاظ بأعضاء فرقهم.

على أي حال، المستقبل يبدو مشرقًا لوظائف عمليات الأمن السيبراني!

[1] 2021 Cybersecurity Workforce Study:
https://www.isc2.org/Research/Workforce-Stud

صعوبة العمل في مراكز عمليات الأمن(SOC)

المشكلة أن العمل في مراكز عمليات الأمن (SOC) يمكن أن يكون شاقًا:

حاجز دخول مرتفع: يتطلب مهارات متقدمة ومعرفة تقنية واسعة.

العمل التكراري: يعتمد غالبًا على التذاكر والتنبيهات، مما يجعله مملًا.

الهيكل الهرمي: قد يحد من الرؤية والنطاق المتاح للموظفين.

التدفق العملي المفرط: يقلل من حرية التصرف والإبداع.

الضغط المفرط: يتطلب الكثير من النقر والملء المتكرر للمعلومات.

معدل دوران عالٍ: مما يؤدي إلى بيئة "باب دوار" حيث يأتي زملاء جدد ويرحلون باستمرار.

سنناقش كيف يمكن إصلاح هذا الوضع

هدفنا هو جعل عمليات الأمن ممتعة وجذابة!

صعوبة العمل في مراكز عمليات الأمن(SOC)

من الجوانب المؤسفة في العمل داخل مراكز عمليات الأمن أن طبيعة الوظيفة قد تصبح في بعض الحالات تكرارية ومقيدة. هناك من وصف العمل في SOC بأنه مكان رائع يعزز التعلم والتفاعل المستمر، بينما هناك من يصفه بأنه "باب دوار" حيث "لا أحد يعرف ماذا يفعل"، وهذا أمر محبط!

البيئة والإجراءات التي تُستخدم داخل فريق الأمن تؤثر بشكل كبير على فعالية الفريق، تفاعل الموظفين، ومعدل الاحتفاظ بالموظفين. بغض النظر عن الوضع الحالي لمركز عملياتك، هناك دائمًا طرق لتحسينه، وسنناقش هذه الطرق خلال الكورس!

هدف ثانٍ لهذا الكورس، بجانب التدريب الفني، هو استكشاف وسائل للقضاء على المصاعب غير الضرورية المرتبطة أحيانًا بالعمل فيSOC ، مثل:

- إدخال البيانات بشكل متكرر.
- المقاييس السيئة وغير المفيدة.
- تدفقات العمل المفرطة في التقييد.
- كميات كبيرة من التنبيهات الإيجابية الخاطئة.

هذه المشكلات يمكن التحكم بها، ويجب على أي فريق يعاني منها أن يتصدى لها بشكل قوي قبل أن تؤثر على البيئة ومعنويات الفريق. سنناقش هذه القضايا بشكل معمق في القسم الخامس.

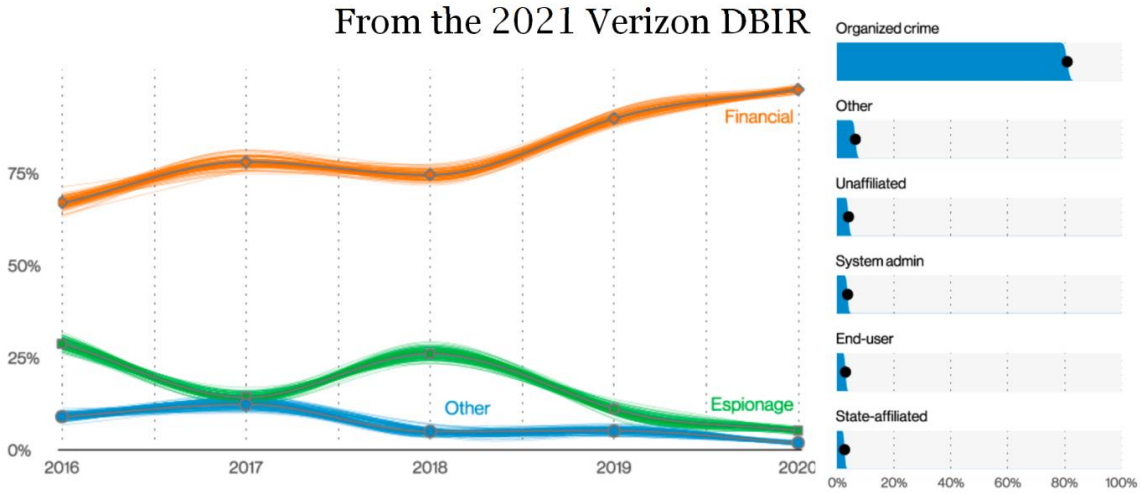
الهدف هو تحسين صورة وظائف الفريق الأزرق.(Blue Team)

على الرغم من أن هذه الوظائف قد اكتسبت سمعة سيئة في الماضي بسبب الأدوات غير الناضجة، فإن تلك الأيام أصبحت جزءًا من الماضي. التكنولوجيا المتطورة والأتمتة موجودة الآن، ويجب عليك استخدامها!

نريد أن يكون مركز العمليات مكانًا يرغب الجميع في العمل فيه على المدى الطويل، وليس مجرد محطة انتقالية أو عائق قبل التوجه لشيء آخر.

ما إذا كان هذا هو الوضع في مؤسستك أم لا، يعتمد بشكل كبير على كيفية تفاعل الأفراد، العمليات، والتكنولوجيا داخلها. سنبذل قصارى جهدنا لمساعدتك في تحسين أي موقف غير مثالي متاح. العمل في SOC سيكون دائمًا تحديًا، لكنه يجب أن يكون من النوع الممتع، وليس كفاحًا يوميًا!

لماذا نتعرض للهجمات؟



لماذا نتعرض للهجمات؟

لماذا تحدث كل هذه الهجمات السيبرانية في المقام الأول؟ تعد هذه المناقشة بالغة الأهمية لأنها تشكل الأساس الذي سنبني عليه استراتيجيتنا الأمنية بالكامل. لإنفاق ميزانيتك بطريقة منطقية ومدروسة، عليك أن تفكر في الهجمات الأكثر احتمالًا ودوافع المهاجمين – يُعرف هذا بمصطلح "معلومات التهديد" (Threat Intelligence)، وهو يساعدنا على اتخاذ أول خطوة صحيحة في الاتجاه المناسب.

يقدم لنا تقرير تحقيقات خروقات البيانات لعام 2021 من Verizon، وهو أحد أكثر التقارير شمولًا التي تُنشر سنويًا، فكرة عن الهجمات الأكثر شيوعًا ودوافعها. يوضح الرسم البياني أعلاه الأنواع والدوافع الأكثر شيوعًا للمهاجمين عبر مختلف الصناعات. كما يوفر التقرير بيانات متخصصة حسب الصناعة، وهو أمر يجب عليك مراجعته فيما يتعلق بمجالك.

ما الذي يوضحه هذا التقرير؟

الغالبية العظمى من الهجمات (المعروفة لدى Verizon) مدفوعة ماليًا.

تأتي في المرتبة الثانية بفارق كبير الهجمات المتعلقة بـ"التجسس" (Espionage)، وهي تشمل العديد من الهجمات المتطورة والمرتبطة بالتهديدات المستمرة المتقدمة (APT) والهجمات التي تستغل ثغرات يوم الصفر (Zero-Day) والتي تُذكر كثيرًا في الأخبار.

أما بقية الهجمات فهي مدفوعة بمشاعر انتقامية، أو بدافع التسلية، أو تقع تحت تصنيفات "أخرى".

كيف نستخدم هذه المعلومات؟

فكر في أولوياتك الحالية:

هل تخطط للدفاع ضد التهديدات المستمرة المتقدمة التي تسعى لسرقة الملكية الفكرية؟

أم أنك تستعد لمواجهة مجموعات الجريمة المنظمة التي تهدف إلى تنفيذ هجمات الفدية؟

هل تتماشى استراتيجيتك مع ملف التهديدات لصناعتك؟ معرفة هذه التهديدات والاستعداد لها تُعتبر هدفًا مبدئيًا ممتازًا لوضع دفاعات متوافقة مع التهديدات المحتملة.

سنأخذ هذه الفكرة ونواصل تطويرها وتكرارها طوال هذا الكورس لبناء دفاعات أكثر قوة وفعالية.

[1] Verizon 2021 DBIR:
https://www.verizon.com/business/resources/reports/dbir/

كم من الوقت يستغرق اكتشاف الاختراق؟

Detection speed getting better.... or is it?

GLOBAL MEDIAN DWELL TIME, 2011-2020

Compromise Notifications	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
All	416	243	229	205	146	99	101	78	56	24
External Notification	—	—	—	—	320	107	186	184	141	73
Internal Detection	—	—	—	—	56	80	57.5	50.5	30	12

وفقًا لتقرير **Mandiant M-Trends 2021**، الذي يغطي جميع الاختراقات التي استجابت لها Mandiantخلال عام 2020، يبدو أن سرعة الاكتشاف تتحسن، لكن هل هذا التحسن حقيقي؟

الحقائق من التقرير:

- بلغ متوسط الوقت العالمي لاكتشاف الاختراقات 24 يومًا، منخفضًا من 56 يومًا في العام السابق.
- الاختراقات التي تم اكتشافها داخليًا استغرقت **12يومًا فقط**، بينما بلغ المتوسط **73يومًا** للحالات التي تم الإبلاغ عنها بواسطة مصادر خارجية.

لكن هناك مشكلة!

- يشير التقرير إلى أن هذه الأرقام المنخفضة قد تكون مضللة، وذلك بسبب نوعية الهجمات التي أصبحت تُنفذ.
- على سبيل المثال، الهجمات باستخدام **برمجيات الفدية(Ransomware)** ، التي تكشف عن نفسها فور تنفيذها، ساهمت في خفض هذا المعدل. وبالتالي، فإن هذا "التحسن" في الأرقام ليس إنجازًا حقيقيًا لفريق الدفاع، بل نتيجة طبيعة هذه الهجمات.

السؤال الأهم:

ما هو الزمن المثالي لاكتشاف الاختراق؟ كيف يمكننا تحديد ذلك؟

- إحدى الطرق للإجابة هي النظر في مدى سرعة تحرك المهاجمين، ومحاولة مجاراتهم أو التفوق عليهم.
- على سبيل المثال، تُظهر بعض التقارير أن برمجيات الفدية يمكن أن تنتشر على مستوى المؤسسة وتكون نشطة في غضون **ساعات قليلة** فقط، خصوصًا عند استغلال ثغرات أمنية حاسمة غير مُعالجة.

الواقع الحالي:

- حتى متوسط 28 يومًا (أو 12 يومًا للاكتشاف الداخلي) **لا يزال بطيئًا للغاية** بالنسبة للطبيعة السريعة للهجمات السيبرانية اليوم.

ماذا علينا أن نفعل؟

سنناقش لاحقًا مفهوم **دورة OODA** (الملاحظة، التوجيه، القرار، التنفيذ) وأهميته في تسريع استجابة الدفاعات الأمنية، لضمان أن يكون فريق الدفاع دائمًا أسرع من المهاجمين. سنعمل على استراتيجيات وأدوات تمكننا من تقليص زمن الاكتشاف بشكل كبير، لأن الوقت لا يزال جوهريًا في المعركة ضد التهديدات السيبرانية.

[1] Ryuk in 5 hours: The DIFR Report: https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/

[2] IcedID to XingLocker Ransomware in 24 hours: https://thedfirreport.com/2021/10/18/icedid-to-xinglockerransomware-in-24-hours/

[3] Mandiant M-Trends 2021: https://vision.fireeye.com/editions/11/11-m-trends.html

العلاج: تحسين عمليات الأمن السيبراني

عمليات الأمن السيبراني:

"حماية سرية وسلامة وتوافر أنظمة المعلومات في المؤسسة من خلال التصميم والتكوين الاستباقي، المراقبة المستمرة لحالة الأنظمة، اكتشاف الإجراءات غير المقصودة أو الحالات غير المرغوب فيها، وتقليل الأضرار الناتجة عن التأثيرات غير المرغوب فيها".

تحليل: تحسين عمليات الأمن السيبراني

الخطوة الأولى نحو تبني عقلية أمنية دفاعية تبدأ بفهم **ما هي عمليات الأمن السيبراني؟** هذا التعريف الذي يستخدمه **كريس كراولي**، كبير المدربين في SANS وخبير عمليات الأمن، يشمل جوهر مهمة العمليات الأمنية.

تركز عمليات الأمن السيبراني على:

- **ضمان أداء الأنظمة كما هو متوقع :**ويتم ذلك من خلال التصميم الجيد والمراقبة المستمرة.
- **التعامل مع المشكلات عند حدوثها :**عند وقوع اختراق أو مشكلة ما، تكون مهمة عمليات الأمن هي **تقليل الأضرار** إلى الحد الأدنى.

لاحظ أن الهدف ليس إزالة الأضرار تمامًا.

هذا الاعتراف يعكس حقيقة أن **لا يوجد شبكة غير قابلة للاختراق**، وأن الهجمات ستحدث لا محالة.

السؤال هنا هو:

- هل فريقك والتقنيات التي تستخدمها مهيئة بشكل صحيح لتقليل الأضرار إلى أدنى مستوى ممكن؟

الغاية:

عمليات الأمن السيبراني ليست مجرد مجموعة من الأدوات أو الإجراءات؛ إنها نهج شامل لضمان أن المؤسسة ليست فقط قادرة على منع التهديدات، ولكن أيضًا على الاستجابة بفعالية عندما تقع تلك التهديدات.

ما هو مركز عمليات الأمن السيبراني؟

- **Cyber**: يتعلق بأنظمة المعلومات.
- **Security**: ضمان الاستخدام المشروع فقط.
- **Operations**: الأداء المستمر.
- **Center**: محور أو نقطة تجمع للأنشطة.

الفريق الأزرق (Blue Team) للمؤسسة:

- قد يكون فريق أمن يتكون من شخص واحد أو مجموعة منظمة.
- يتضمن العديد من الاختصارات المحتملة.SOC, ISOC, SIRT, CSIRT, DART :
- الأهداف تشمل:
  - المراقبة/الصيد الإلكتروني.
  - الاستجابة للحوادث.
  - استخبارات التهديدات.
  - التحليلات الجنائية الرقمية.
- أي شخص أو فريق مسؤول عن "عمليات الأمن."

ما هو مركز عمليات الأمن السيبراني؟

إذا كانت **عمليات الأمن** تعني حماية بياناتك ومراقبتها وتقليل الأضرار الناتجة عن الهجمات، فإن مركز العمليات الأمنية (SOC) هو محور هذه الأنشطة.
يمثل المركز (سواء كان افتراضيًا أو فعليًا) تجمعًا للأشخاص والعمليات والتقنيات التي تعمل على تحقيق هذه الأهداف.
غالبًا ما يُطلق على هذا الفريق **الفريق الأزرق(Blue Team)** ، أو مركز العمليات الأمنية(SOC) ، أو أسماء أخرى ضمن اختصارات متعددة.
في هذه الدورة، سيتم استخدام المصطلحين "الفريق الأزرق" و"مركز العمليات الأمنية" بشكل متبادل.
ملاحظات مهمة:

- ليس كل مؤسسة لديها مركز عمليات أمنية كامل بالمعنى التقليدي.
- بالنسبة لهذا الكتاب وهذه الدورة، فإن وجود فريق دفاع متكامل ليس هو النقطة الرئيسية.
- عند الإشارة إلى "مركز العمليات الأمنية" في هذا النص، تخيل أننا نتحدث عن الجهة المسؤولة عن:
  - مراقبة التهديدات واكتشافها.
  - الاستجابة للحوادث.
  - المهام الأمنية المشابهة.

سواء كانت هذه المهام تتم بواسطة شخص واحد أو فريق كبير، فإن الأهم هو تحقيق الأداء الذي تحتاجه المؤسسة في مجال الدفاع السيبراني.
ما الذي يعنيه هذا الأداء وكيف نحققه؟
هذا هو ما ستتناوله بقية الدورة!

عقلية الدفاع الحديثة

الدفاع الحديث هو أملنا الوحيد، ويعني:

- افتراض حدوث اختراق مسبقًا.
- دفاع قائم على الاكتشاف.
- اكتشاف استباقي: فرق البحث.(Hunt Teams)
- التركيز على مرحلة ما بعد الاستغلال.
- التركيز على الاستجابة.
- استراتيجية تعتمد على تقييم المخاطر.

"الوقاية هي الهدف المثالي، لكن الاكتشاف ضرورة".

عقلية الدفاع الحديثة

كجزء من الفريق الأزرق، يجب أن نتأكد من أن الجميع يدركون مفهوم "عقلية الدفاع الحديثة" ومتطلباتها لحماية الشبكات في عصرنا الحالي. في دورة " **SANS SEC511: المراقبة المستمرة وعمليات الأمن** "التي أعدها إريك كونراد وسيث ميسينار، تم تقديم رؤية ممتازة حول أهم المفاهيم المتعلقة بهذا المجال، وهي مذكورة هنا.

الخطوات الأساسية للدفاع الحديث:

1. افتراض الاختراق:

علينا أن نعترف بأن احتمال حدوث اختراق هو أمر واقع، وأن نعد دفاعًا قويًا يشمل تقنيات الوقاية والاكتشاف لمواجهة ما قد يفلت من التدابير الأولية.

2. الاكتشاف الاستباقي:

يمكن لفرق الصيد (Hunt Teams) أو أي جهة مكلفة بالبحث في البيانات المجمعة اكتشاف الأدلة على الأنشطة التي تمكنت من تجاوز الدفاعات الأمامية وأخذ موطئ قدم داخل البيئة. يجب أن تركز هذه الفرق على مرحلة ما بعد الاستغلال، حيث يُفترض أن التهديد قد تجاوز بالفعل مرحلة الاستغلال المبدئي.

3. الاستجابة السريعة:

الاكتشاف لا يكفي بدون القدرة على الاستجابة بسرعة. بمجرد اكتشاف أي تهديد، يجب أن يكون لدينا العمليات والتقنيات المهيأة للاستجابة الفورية لتقليل الأضرار ومنع تفاقم الوضع. كلما تم التعامل مع الخرق مبكرًا، قلّت تكلفة الإصلاح والتنظيف.

4. دفاع مستند إلى المخاطر:

معظم الفرق لا تمتلك الوقت أو الميزانية لحماية كل شيء بشكل مثالي. لذلك، من الضروري فهم ما يسعى إليه المهاجمون داخل المؤسسة وكيف يمكنهم الوصول إليه. وضع تقنيات الوقاية والاكتشاف أمام الخوادم التي تحتوي على البيانات الأكثر أهمية والأشخاص الذين لديهم صلاحيات الوصول إليها هو استثمار عقلاني لتعظيم قيمة أدوات الأمن لديك. **في النهاية**، الهدف هو بناء دفاع متماسك وفعال يعتمد على فهم واضح للمخاطر والتهديدات، ويوازن بين الوقاية والاكتشاف والاستجابة لتحقيق أقصى درجات الحماية.

[1] SEC511: https://www.sans.org/cyber-security-courses/continuous-monitoring-security-operations/

تلخيص مهمتنا

"تقليل احتمالية التأثير المادي على مؤسستي نتيجة حدث إلكتروني".

—**ريك هوارد،** المدير التنفيذي للأمن والمحلل الرئيسي في CyberWire

تلخيص مهمتنا

تحتوي هذه الفقرة على واحدة من التعريفات المفضلة لدى المؤلف للأمن السيبراني، حيث تختصر المهمة في عبارة بسيطة وقابلة للتذكر. كل ما تقوم به كمدافع سيبراني يجب أن يتماشى مع هذا الهدف الرئيسي الشامل:

"تقليل احتمالية التأثير المادي على مؤسستي نتيجة حدث إلكتروني".

من المستحسن بشدة قراءة المقال المشار إليه في الاسفل حيث يشرح ريك هوارد بالتفصيل كيف صاغ هذا التعريف بعناية. فهم هذا التعريف يُعد عنصرًا أساسيًا يجب أن يستوعبه كل مدافع.

تفصيل التعريف:

- **"تقليل الاحتمالية" -** لأننا لن نكون مثاليين.
- **"للتأثير المادي" -** لأن هذا هو الأكثر أهمية؛ جميع التأثيرات سيئة، ولكن التأثيرات المادية الكبيرة هي ما يجب أن نركز عليه.
- **"على مؤسستي بسبب حدث إلكتروني" -** تحديد نطاق عملنا على مؤسستنا وأحداث الأمن السيبراني فقط، لأننا لسنا مسؤولين عن منع جميع أنواع التأثيرات المادية.

ما هو دورك في هذه المهمة؟

مهمتك، في نهاية المطاف، هي تقليل آثار الاختراق على مؤسستك إلى الحد الأدنى الممكن. لتحقيق ذلك، يجب أن تكون مستعدًا لتحديد علامات الاختراق بسرعة وإيقاف تطور الحادث.

يمكنك القيام بذلك من خلال:

- شبكة مُراقبة بشكل جيد.
- مجموعة من نقاط النهاية (endpoints) المجهزة بأدوات الكشف.
- القدرة على إصدار التنبيهات وفرز القضايا المحتملة بدقة وسرعة.

التحديات:

- هذه المهمة ليست سهلة.
- تتطلب التعلم المستمر ورغبة قوية في ملاحقة المهاجمين.
- تتغير تقنيات الهجوم والاستغلال يوميًا.
- ستتعامل دائمًا مع معرفة غير مكتملة حول الموقف الحالي.

كيفية الاستعداد:

- تعلم كيفية فهم البروتوكولات المستخدمة على الشبكة.
- تعلم قراءة وتحليل ملفات السجلات (logs) بفعالية.
- تعلم إجراء تحليل عالي الجودة.
- فهم كيفية تدفق البيانات بالطريقة الصحيحة (وغير الصحيحة).

هذا هو الهدف الأساسي الذي نسعى لتحقيقه في هذه الدورة، وهو إعدادك للقيام بهذه المهمة بفعالية وكفاءة.

[1] "Cybersecurity first principles", thecyberwire.com: https://thecyberwire.com/stories/36065117662b4e6ebf0d350163283fc6/cybersecurity-first-principles

أهداف دورةSEC450

تهدف هذه الدورة إلى تعليم:

- الأدوات :أنظمة إدارة معلومات الأحداث الأمنية(SIEM) ، منصات استخبارات التهديدات، أنظمة إدارة الحوادث، والمزيد.
- البيانات :سجلات الشبكة، الأجهزة الطرفية، وتطبيقات البرمجيات.
- التصنيف الأولي :القدرة على تحديد القضايا الأكثر أهمية بسرعة ودقة.
- التحليل :كيفية إجراء تحقيقات ذات جودة عالية.
- الأتمتة :متى وماذا يتم أتمتته لجعل حياتك أسهل.
- العقلية :نماذج التفكير لتحقيق النجاح في الدفاع السيبراني الحديث.
- التحسين المستمر :كيفية تحديد وتنفيذ التحسينات.
- تمهيد الطريق للنجاح كعضو في الفريق الأزرق!

أهداف دورة SEC450

يحقق الفريق الأزرق أفضل أداء عندما يمتلك رؤية واقعية لما هو ممكن ويكون لديه علاقة عمل جيدة مع المؤسسة. على الرغم من أن معظم محتوى هذه الدورة سيركز على البيانات والعمليات وسير العمل داخل مركز العمليات الأمنية(SOC) ، فمن المهم ألا تغفل عن الصورة الكبرى لكيفية تكامل هذا الفريق مع المنظمة ككل.

تذكر أنه من منظور العمل، يمكن تلخيص دورك في عبارة مشابهة:

"تأكد من أن المشكلة الأمنية السيبرانية ليست هي العائق الذي يمنع الأعمال التجارية من الحدوث / الحكومة من العمل، إلخ. وفي الوقت نفسه، حاول تقليل جميع التكاليف المتعلقة بالأمن السيبراني قدر الإمكان!"

لكن التحدي الحقيقي يكمن في ترجمة هذا الهدف العام إلى العمليات والأدوات والبيانات ذات المستوى التفصيلي، وهو ما يعقد الأمور.

ستركز هذه الدورة بشكل كبير على التفاصيل الفنية، وأنواع الهجمات، ووسائل الدفاع، والعناصر داخل مركز العمليات الأمنية لتحقيق هدف إنشاء فريق أزرق قوي وفعال قادر على حماية مؤسستك بنجاح!

البداية بأساس قوي

في هذا الجزء:

1. المكونات الأساسية لعمليات الأمن.
2. تعريف وفهم مهمة مركز العمليات الأمنية.(SOC)
3. ضمان توافق مركز العمليات الأمنية مع أهداف المنظمة ومستوى تقبلها للمخاطر.
4. الهيكل التنظيمي لعمليات الأمن.
5. الوظائف الأساسية لعمليات الأمن.
6. وثائق مرجعية مفيدة للممارسين.
7. قياس فعالية مركز العمليات الأمنية وتوضيحها.

البداية بأساس قوي

في هذا الجزء، سنتناول بعض المكونات الأساسية لعمليات الأمن والنماذج المختلفة المستخدمة لفهم العناصر البشرية والعمليات والتكنولوجيا المعنية.

الهدف هو مساعدتك على فهم كيفية بناء أساس قوي (أو تقييم الأساس الحالي لديك) وضمان استمرار مركز العمليات الأمنية (SOC) في التوافق مع أهداف مؤسستك.

مكونات عمليات الأمن

- **الأفراد** :يقومون بالتحليل والتحقيق وتصميم وتنفيذ العمليات.
- **العمليات** :تسلسل محدد للأحداث يتم تنفيذه لتحقيق هدف معين.
- **التكنولوجيا** :الأجهزة والبرمجيات المستخدمة لتنفيذ المهمة.

مكونات عمليات الأمن

أحد الطرق الشائعة للنظر إلى مركز العمليات الأمنية (SOC) هو من خلال العناصر الأساسية المطلوبة. يحتاج الفريق الأزرق (Blue Team) الفعّال إلى ثلاثة مكونات رئيسية :**الأفراد، العمليات، والتكنولوجيا**.

1. **الأفراد:** يعتبر الأفراد العنصر الأهم والأساسي. بدون فريق متعاون ومتحمس للتواصل والعمل، لا يمكن لأي فريق أزرق أن ينجح. الأفراد هم **القلب والروح** لعمليات الفريق الأزرق، واختيارهم المناسب يمكن أن يكون العامل الحاسم لنجاح أو فشل الفريق. لا يمكن لأي عملية أو تقنية أن تعوض فريقًا مختل الوظائف أو غير مدرب أو غير راضٍ.
2. **العمليات**: تحدد العمليات ما الذي سيقوم به الأفراد وكيفية تنفيذهم له. يتطلب تعريف العمليات تحديد المهام المهمة وتصميم الحلول المثلى لإتمامها.
3. **التكنولوجيا**: تعتبر التكنولوجيا الأداة التي تمكّن من تنفيذ العمليات بكفاءة ودقة. تتيح التكنولوجيا مراقبة كميات هائلة من البيانات وتعمل كقوة مضاعفة لأداء أعضاء الفريق. إذا كنت تدير الدفاع السيبراني بشكل صحيح، **فالتكنولوجيا ليست بديلًا عن الأفراد**، بل وسيلة لتحسين أدائهم. إذا كان بالإمكان استبدال محلليك بالتكنولوجيا، فهذا يعني أنهم كانوا يقومون بمهام متكررة كان من الأفضل أتمتتها منذ البداية، وليس بالعمل التحليلي الذي ينبغي أن يكون عليه دورهم.

هذه المكونات الثلاثة تشكل **"الركائز الثلاث "**لعمليات الأمن. بدون أحدها، لن يتمكن الفريق من تحقيق النجاح.

فهم مهمتك - أربعة أسئلة أساسية

الدفاع السيبراني صعب - من أين نبدأ؟

- لنشتق بعض الأهداف والمتطلبات. إليك مجموعة رائعة من الأسئلة التي تساعدك على توضيح مهمتك وفهم ملامح النجاح:
  1. ما الذي نحاول حمايته؟
  2. ما هي التهديدات؟
  3. كيف يمكننا اكتشافها؟
  4. كيف سنستجيب لها؟

فهم مهمتك - أربعة أسئلة أساسية

تصنيف الأشخاص، العمليات، والتكنولوجيا يمثل مجرد عناصر أساسية، لكن عند دمجها معًا، ما الذي نحاول تحقيقه؟ الإجابة البسيطة هي :**الدفاع عن مؤسسة ما!**

لتحديد كيفية استخدام الأشخاص والعمليات والتكنولوجيا لبناء هذا الدفاع، يمكننا الاعتماد على الأسئلة الأربعة التي طرحت في كتاب ."**Crafting the Infosec Playbook**"هذه الأسئلة صيغت بطريقة تساعد أي فريق على صياغة مهمته وتوضيح ملامح النجاح.

- إذا كنت بصدد بناء فريقك من الصفر، تُعد هذه الأسئلة نقطة انطلاق ممتازة لتحديد مهمة مركز العمليات الأمنية (SOC) وحتى كيفية قياس النجاح.
- وإذا كنت تعمل بالفعل ضمن مركز عمليات أمنية قائم، فكّر في كيفية إجابتك على هذه الأسئلة، وما إذا كانت الإجابات تتماشى مع ما يقوم به فريقك فعليًا يوميًا.

الأسئلة الأربعة:

1. ما الذي نحاول حمايته؟
2. ما هي التهديدات؟
3. كيف يمكننا اكتشافها؟
4. كيف سنستجيب لها؟

كلما كانت إجاباتك على هذه الأسئلة أكثر دقة وتفصيلًا، زادت فرص نجاحك. نعم، قد تعرف أنك بحاجة إلى "حماية بيانات شركتك من التهديدات المتقدمة"(APTs) ، ولكن ما هي هذه التهديدات بالتحديد؟ كيف ستهاجمك؟ ما أنواع البيانات المستهدفة؟ أين تُخزن هذه البيانات؟ ومن يمتلك صلاحية الوصول إليها؟

الفكرة واضحة :كلما كانت معلوماتك أكثر تفصيلًا، زادت فرصك في النجاح.

ننصحك بشدة بمراجعة هذه الأسئلة بشكل دوري، لأن الإجابات ستتغير مع تطور التهديدات، فريقك، والمؤسسة التي تعمل بها.

[1] Crafting the Infosec Playbook:
https://www.oreilly.com/library/view/crafting-the-infosec/9781491913598/

مواءمة مركز العمليات الأمنية (SOC) مع المنظمة

ميثاق مركز العمليات الأمنية

ميثاق، معتمد من الإدارة، يتضمن:

- الجمهور المستهدف بالخدمة.
- الخدمات المقدمة.
- نطاق العمل.
- بيان المهمة والأهداف العامة.
- الهيكل التنظيمي ومفهوم العمليات.

لجنة التوجيه

- تحدد المخاطر التي تهم العمل.
- توائم قدرات وأداء مركز العمليات الأمنية مع احتياجات العمل.

مواءمة مركز العمليات الأمنية (SOC) مع المنظمة

بعد التفكير في الإجابات على الأسئلة الأربعة الأساسية، يجب أن تنظر في كيفية تقاطع هذه الإجابات مع متطلباتك وميزانيتك وقدرات فريقك واحتياجات المنظمة. هذه المعلومات مجتمعة تساعدك في صياغة أو مراجعة **ميثاق مركز العمليات الأمنية** الخاص بك.

ميثاق مركز العمليات الأمنية هو الوثيقة التوجيهية التي تحدد معايير عمل فريق العمليات الأمنية. هذه الوثيقة تُضفي الشرعية وتمنح الفريق الأزرق السلطة اللازمة لتنفيذ الأنشطة المطلوبة لحماية البيئة الأمنية. كما أنها تحدد بشكل عام نطاق عمل الفريق، واجباته، الخدمات المقدمة، الجمهور المستفيد، وبيان المهمة الرئيسي الذي تمت الموافقة عليه من قبل الإدارة.

الميثاق يُعد بمثابة الأساس الذي يضمن أن الجميع (سواء داخل الفريق أو خارجه) على علم بما هو متوقع من هذا الفريق.

ميثاق الفريق الأمني يجب اعتباره وثيقة ديناميكية.

بسبب التغير السريع في التكنولوجيا والمنظمات، قد يحتاج الميثاق إلى التحديث أيضًا. يمكن أن تكون **لجنة التوجيه** الحل لهذه المشكلة.

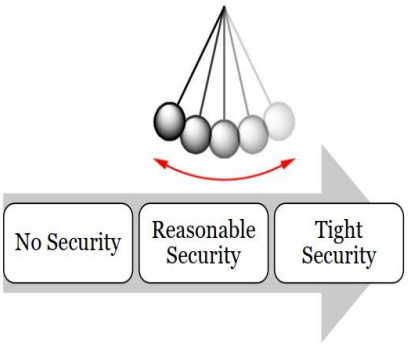
لجنة توجيه مركز العمليات الأمنية (SOC Steering Committee) هي اجتماع دوري مع أصحاب المصلحة الأساسيين لمركز العمليات الأمنية. تضمن هذه اللجنة:

- استمرار توافق مركز العمليات الأمنية مع توقعات العمل.
- الحفاظ على خطوط اتصال مفتوحة.
- تلبية مركز العمليات الأمنية لمتطلبات العمل واحتياجاته.
- تركيز الموارد على المخاطر المناسبة.

تعد لجنة التوجيه الطريقة التي يتواصل بها الفريق الأزرق مباشرة مع الجمهور المستفيد لضمان تقديم الخدمات المطلوبة والمنتظرة، بدلًا من تقديم دفاعات مبنية على افتراضات الفريق فقط.

هاتان الركيزتان (الميثاق ولجنة التوجيه) توفران التوجيه الأساسي والمستمر لما يجب أن يقوم به مركز العمليات الأمنية، من يحميه، وكيف يتم ذلك.

تحديد شهية المؤسسة للمخاطر



- تذكّر النظر إلى الصورة الأكبر:
  - المؤسسات لا تُوجد بهدف أن تكون آمنة فقط.
- أين تأتي الأمن السيبراني في قائمة الأولويات؟
  - الجهات الحكومية/العسكرية :الأهمية القصوى.
  - الشركات الناشئة الجديدة :أهمية منخفضة.
  - اسأل ما إذا كانت مؤسستك لديها "بيان شهية المخاطر."
- الفريق الأمني الناضج يفهم شهية المخاطر:
  - يعمل ضمن هذا الإطار (مع إمكانية محاولة التأثير عليه).
  - يتغير مع تغيّر الإدارة وأولويات الشركة.

تحديد شهية المؤسسة للمخاطر

لجنة التوجيه يجب أن توضح بجلاء مفهوم شهية المؤسسة للمخاطر. يجب على جميع أعضاء مركز العمليات الأمنية (SOC) فهم المخاطر الكبرى التي ترى المؤسسة أنها تواجهها، وكيف ينعكس ذلك على نهجها في تنفيذ مهمتها.

تختلف أولويات الأمن السيبراني بشكل كبير بين المؤسسات بناءً على طبيعتها:

- **المؤسسات الحكومية والدفاع الوطني** غالبًا ما تكون لديها شهية منخفضة جدًا للمخاطر، ومستعدة لتطبيق ضوابط أمنية أكثر تطفلاً لتقليل احتمالية حدوث خروقات.
- **الشركات الناشئة الجديدة** قد ترى الأمن كوظيفة يجب تنفيذها بأقل مستوى ممكن لضمان العمل بسرعة قصوى.

دور الفريق الأمني هو أخذ هذه المعلومات بعين الاعتبار والعمل وفقًا لها، أو إعلام الإدارة عندما يكون تقدير المخاطر غير دقيق لتتم مراجعة القرارات وإجراء التعديلات المناسبة.

يجب أن تكون على دراية بأن شهية المخاطر ستتغير بمرور الوقت مع نضوج المؤسسة أو تغيير القيادة. فهم التفكير الحالي للإدارة حول المخاطر يُعدّ من الأمور المهمة التي يجب على الفريق الأزرق القيام بها.

بعض المؤسسات لديها وثيقة رسمية تُسمى **"بيان شهية المخاطر".** قراءة هذه الوثيقة (إذا كانت موجودة) تُسهم في فهم رؤية الإدارة العليا بوضوح.

الالتزام بمستوى تحمل المخاطر

- "ما هو أسوأ ما قد يحدث؟"
- ما نوع العمل الذي تقوم به مؤسستك؟
- ما مدى أهمية نجاح فريق الأمن؟
  - أهمية عالية: التحكم في التطبيقات، أنظمة الكشف والاستجابة المتقدمة(EDR/XDR) ، تصميم شبكات عدم الثقة(Zero Trust) ، سياسات بريد إلكتروني صارمة، إلخ.
  - أقل أهمية: أدوات أساسية وقدرات مراقبة بيانات محدودة.
- هدفك: إيجاد طرق لتعزيز مستوى الأمان إلى أقصى حد ممكن دون إعاقة سير العمل.
- تطبيق جميع خيارات "الأمان غير المرئي" المناسبة.
- اتخاذ قرارات ذكية فيما يخص عناصر الأمان المزعجة أو "المرئية."

الالتزام بمستوى تحمل المخاطر

هل شركتك غير مستعدة إطلاقاً لتحمل أي اختراق وستتخذ تدابير قصوى لحماية نفسها مهما كلف الأمر؟ أم أنها تفضل اتخاذ نهج متوازن يضمن إنجاز الأعمال بسرعة؟

فكر في الأسئلة السابقة. على الرغم من أن هذه المعلومات يُفترض أن تُعطى من الإدارة العليا، إلا أن الإجابة قد تكون واضحة أحياناً. توقف للحظة وفكر في أسوأ ما يمكن أن يحدث لمؤسستك: هل هو اختراق للبيانات أو تعطيل للبنية التحتية الحرجة التي تديرها؟ فكر في مدى احتمال حدوث هذه الأمور وما الذي قد يتطلبه ذلك من حيث الوصول، ثم فكر في التدابير التي وضعتها شركتك لمنع هذا السيناريو. يتمثل أحد أهداف اللجنة التوجيهية في مساعدة الشركة على إيجاد الإجابات وتحديد المبلغ والوقت الذي ترغب في استثماره لمنع هذه الأحداث من الحدوث. بعد ذلك، سيقوم مركز عمليات الأمن (SOC) بترجمة هذه التوجيهات إلى ضوابط يجب تنفيذها.

الشركات ذات التحمل المنخفض للاختراق ستجد نفسها غالباً تخضع لضوابط صارمة، مثل التحكم في التطبيقات، والشبكات بأسلوب "عدم الثقة"، والأنظمة المعزولة أو التي لا تتصل بالإنترنت-air) (gapped، وإجراءات صارمة للتحكم في الوصول للإنترنت والبريد الإلكتروني. أما الشركات ذات التحمل الأعلى للمخاطر فقد تكتفي بضوابط أساسية – مثل برامج مكافحة الفيروسات المدمجة في أنظمة التشغيل، والتسجيلات الافتراضية التي يوفرها الموردون، ومرشحات البريد الإلكتروني الأساسية للكشف عن الرسائل غير المرغوب فيها.

كعضو في فريق الدفاع(Blue Team) ، تتمثل مهمتك في ضمان توافق شهية المخاطر مع الضوابط والتقنيات المستخدمة. إذا وجدت أن الشركة بدأت تتخذ مخاطر غير ضرورية، ربما لأنها لم تفهمها تماماً أو لم تكن مدركة لها، يجب أن تشعر بالتمكين لتقديم توصيات حول أي فجوات في التغطية الأمنية. سنتطرق لاحقاً في الدورة إلى كيفية القيام بذلك بشكل لبق لتجنب المشاكل. نحن نحاول الوصول إلى منطقة التوازن حيث يتم تلبية شهية المخاطر المدروسة بشكل جيد، بما يضمن أمان الشركة ويسمح بإتمام العمل بسلاسة دون عوائق إلا عند الضرورة.

توافق شهية المخاطر مع الواقع

تخيل أنك تعمل في شركة لتصنيع اللقاحات:

- هناك حاسوب من نوع خاص (بُني بواسطة بائع) يدير خط إنتاج حرج.
- النظام مغلق ومعتمد، ولا يُسمح بإضافة برامج أمان إضافية.
- يتطلب:
  - نقل بيانات عبر بروتوكول FTP الصادر.
  - صفحة حالة على الويب من الداخل.
  - نظام التشغيل هو Windows XP.

كيف يمكنك تأمين هذا الجهاز؟

تلميح: الإجابة ليست "عدم السماح باستخدامه" – ستُرفض هذه المقاربة بسرعة.

توافق شهية المخاطر مع الواقع

موقف قد تواجهه كمثال حيث يكون مستوى المخاطر المطلوب على خلاف مع متطلبات العمل. افترض أنك تعمل في شركة لتصنيع اللقاحات وجزء من عملية التصنيع يتطلب إعداد جهاز حاسوبي حساس يجب الموافقة على أي تغييرات عليه بسبب حساسية العملية. يعتمد النظام على Windows XPولا يمكن تعديله بإضافة برامج مثل برامج المراقبة أو الجدران النارية أو حتى الحماية من الفيروسات. علاوة على ذلك، لا يمكنك تحديث النظام لأن الشركة المصنعة للنظام قد أغلقت أبوابها وليس هناك بديل.

لتعقيد الأمور، يحتاج هذا الجهاز أيضًا إلى تسجيل البيانات وإرسالها عبر بروتوكول FTP غير الآمن، كما يستضيف صفحة حالة عبر خادم ويب قديم يحتمل أنه غير آمن. يبدو هذا تناقضاً: يجب أن يكون آمنًا، لكنك مجبر على تشغيل Windows XP على جهاز يؤدي مهمة حاسمة. فما العمل؟

قد يميل البعض إلى إخبار الشركة بأن هذه المخاطرة كبيرة جداً وأن استخدام الجهاز في أي شكل هو أمر غير عقلاني! لكنك ستُرفض إذا كانت هذه هي الخلاصة التي اقترحتها؛ إذ من المحتمل أن يكون الرد هو "بالطبع لا، هذا الجهاز مسؤول عن إنتاج بقيمة معينة للساعة، عليك إيجاد حل آخر"!

ما هي الخيارات الأخرى؟

بما أننا لا نستطيع لمس النظام الداخلي للجهاز، فإن الحلول ستكون غالباً عبر استخدام أجهزة أمان خارجية كضوابط تعويضية. يجب أن تقوم هذه الأجهزة بفحص محتوى الاتصالات الشبكية للكشف عن الفيروسات، وتقييد اتصالات النظام لتكون فقط عبر المنافذ الضرورية أو مع الأنظمة التي يحتاج إلى التواصل معها بشكل صارم. بالإضافة إلى ذلك، يمكن استخدام جدران حماية تطبيقات الويب لحماية التطبيق الذي يعمل عبر الويب.

هذه هي الأنواع المعقدة من الحالات الواقعية التي ستواجهها كعضو في فريق الدفاع Blue) (Team، ويجب عليك تقبل الوضع، ومعالجة المخاطر والمتطلبات، واقتراح حل مناسب، وكذلك تفسير البيانات التي يتم توليدها للكشف عن أي اختراق محتمل في مثل هذا الإعداد.

قبول المخاطر

يُعتبر مفهوم قبول المخاطر مادة للسخرية أحيانًا في مجال أمن المعلومات. ورغم رغبتنا الشديدة في إنشاء شبكة مثالية لا يمكن اختراقها، فمن الشائع أن تقرر المنظمة قبول مخاطر محددة. الأمن السيبراني يمثل جزءًا واحدًا من معادلة عمل معقدة، وعلى الرغم من أن الأمان قد يكون محور اهتمامك بالكامل، فإنه قد يكون مجرد عامل واحد ضمن العديد من العوامل الأخرى التي تشغل الإدارة لضمان استمرار العمل.

في النهاية، أفضل ما يمكننا فعله هو تقديم معلومات دقيقة وكاملة للإدارة لتقوم بدورها في ضمان استمرارية العمل. إذا كنت تختلف مع قرار معين وتعتقد أنه ينطوي على مخاطر كبيرة وقد يؤدي إلى مشاكل لاحقًا، فإن أفضل ما يمكنك فعله هو محاولة توضيح الأسباب بفعالية أكبر أو توثيق النصيحة التي تم تقديمها والمضي قدمًا في مهامك اليومية.

حقيقة الفريق الأزرق الأولى:

الاختراق سيحدث

السؤال هو... كيف سيؤثر عليك؟

النتيجة 1: ينجح المهاجم في الخطوات الأولى للهجوم، لكن يتم اكتشافه بسرعة ويفشل في إكمال مهمته.

النتيجة 2: لا يتم اكتشاف المهاجم، مما يجعله يتحرك بحرية ويحدث تأثيرًا كبيرًا.

ليس جميع المهاجمين سيتم منعهم من البداية.

الاعتراف بهذه الحقيقة والاستعداد لما سيحدث بعد الاختراق هو ما يميز فرق الأمن الجيدة عن السيئة.

الهدف: اكتشاف وتقليل الضرر الناتج عن الاختراق.

الحقيقة الأولى للفريق الأزرق:

من المهم أن نتذكر أنه بغض النظر عن مدى صعوبة محاولاتنا، سيحدث الاختراق بدرجة معينة. من المستحيل وضع دفاع مثالي يعمل للأبد. ومع ذلك، هذا لا يعني أن أي هجوم سيكون كارثيًا. يقع على عاتق الفريق الأزرق تحديد مدى تقدم الهجوم والضرر الذي قد يحدثه. الفريق الأزرق يؤثر على هذه الأمور من خلال توعية الأعمال بالمخاطر الحقيقية في مجال الأمن السيبراني ودفع السياسات والتكوينات الجيدة في جميع أنحاء البيئة. هذا يساعد على منع العديد من الهجمات من البداية، ولكنه لن يمنعها جميعًا.

كما يجب أن نعرف كيفية الرد، وأن يكون لدينا التدريب والأدوات اللازمة للاستجابة بسرعة عندما تسوء الأمور.

تركز هذه الدورة على مساعدتك في إيقاف الهجمات ذات التأثير الأعلى – تلك الهجمات المستهدفة التي تهدف إلى ابتزاز أموالك أو تدمير بياناتك أو تسريب معلوماتك الحساسة. هذه الهجمات متعددة المراحل ولا يمكن أن تحدث مرة واحدة باستخدام استغلال واحد فقط. التعرض للتصيد الاحتيالي أو تثبيت برمجيات خبيثة على جهاز كمبيوتر محمول لشخص ما ليس نهاية القصة. لكن ما سيحدث إذا لم يُلاحظ هذا الهجوم، واستغل المهاجم هذا الوصول على مدى أشهر لسرقة الملكية الفكرية أو المعلومات الشخصية الحساسة، ونشر هذا الاختراق علنًا، سيصبح ذلك مكلفًا ومدمرًا للغاية!

لذلك، الهدف النهائي للفريق الأزرق هو منع تحقيق الهجوم كاملاً، وإذا كان بإمكاننا منع الهجوم من الأساس، فهذا أفضل!

حقيقة الفريق الأزرق الثانية:

شركتك لا توجد فقط لتكون آمنة

يقوم الفريق بوظيفة "الحد من الخسائر:"

- نقلل من مخاطر الأمن السيبراني إلى مستوى مقبول.
- يجب إيجاد توازن بين الأمن والإنتاجية.
- لا أحد يريد أو يستطيع شراء "الأمان الكامل"، فالتكلفة ستكون باهظة.
- التوازن يتم تحديده بواسطة مؤسستك وإدارتها.
- قد يكون ذلك محبطًا، لكنه لا يعني أننا لا نستطيع محاولة التأثير على القرارات.
- يجب على الفريق الأزرق إبلاغ متخذي القرارات المرتبطة بالمخاطر.
- المعلومات الجيدة تتطلب فهمًا عميقًا لمجالك.

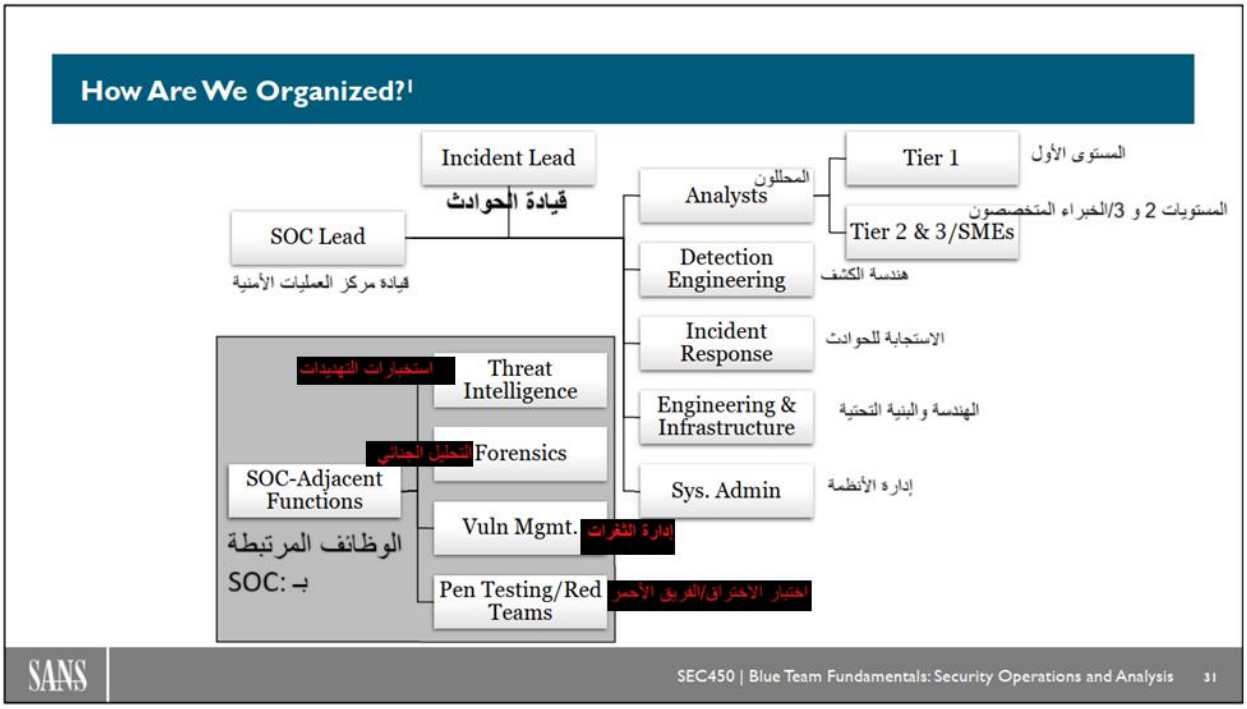
حقيقة الفريق الأزرق الثانية:

بالنظر إلى النقطة السابقة، قد يكون من المغري الرغبة في إغلاق كل شيء وتشديد الحماية إلى أقصى حد. ومع ذلك، من المهم الحفاظ على منظور شامل. نعم، يمكن للفريق الأزرق أن يحدد جميع نقاط الضعف ويطالب بتشديد الحماية على الجميع؛ ولكن يجب أن نتذكر أن الشركة لا توجد فقط لتحقيق الأمان. فالشركات تهدف إلى خلق قيمة بطرق متعددة، ويمكن النظر إلى الأمن السيبراني في النهاية كوظيفة للحد من الخسائر، تشبه الحراس في متجر يحرسون البضائع من السرقة. قد يفرض صاحب المتجر إجراءات تفتيش صارمة مثلTSA ، لكن سيؤدي ذلك غالبًا إلى خروج المتجر من السوق رغم تحقيق نسبة 0% في الخسائر الناتجة عن السرقة.

العلاقة مع ما سبق هي أن "الشركات تستمر في العمل فقط إذا أدارت المخاطر بشكل فعال وصحيح." لذلك، لا يمكننا العيش بدون أمن مطلقًا! يجب إيجاد توازن بين الأمان وحرية العمل دون عرقلة سير الأعمال. قد يكون هذا محبطًا أحيانًا، لكن كل شركة لها رؤيتها الخاصة حول ما تعتبره مخاطر رئيسية (سيبرانية وغيرها) وكيفية الموازنة بين الأمان والإنتاجية. الهدف النهائي للفريق الأزرق هو مساعدة الشركة على فهم المخاطر الحقيقية التي تواجهها ومساعدتها على تأمين الأمور قدر الإمكان، مع تقليل التأثير على الإنتاجية إلى أدنى حد ممكن.

هنا يتجلى فن تصميم نظام آمن. في بعض الأحيان، يجب تقديم تنازلات وتصميم حلول ذكية تسمح للموظفين والشبكات بالعمل دون إبطاء وتيرة الإنتاج أو التقليل من قيمة الشركة.

كيف يتم تنظيمنا؟



التنظيم الداخلي

يوضح الرسم البياني أعلاه الهيكل التنظيمي الوظيفي الشائع لفريق عمليات الأمن في المؤسسات الكبيرة. هذا الهيكل يبرز أن إدارة مركز عمليات الأمن تتطلب الكثير من العمل الفني المتكامل. بالإضافة إلى المحللين الذين يقومون بفرز التنبيهات، يتطلب تشغيل مثل هذه الإمكانيات التقنية دعم أشخاص متخصصين في مجالات مثل هندسة الكشف، ومطاردة التهديدات، والهندسة، وإدارة الأنظمة، وغيرها. هناك أيضًا ما يعرف بالوظائف المرتبطة بـSOC ؛ في بعض الفرق، تعتبر هذه المجموعات جزءًا من مركز العمليات الأمنية، وفي فرق أخرى تكون مستقلة.

كثير من المهتمين يتساءلون عن أفضل مكان لهذه المجموعات، وما إذا كان يجب أن تكون تحت إدارة SOC أم لا. يرى الكاتب أنه لا يوجد نموذج واحد يناسب جميع الحالات، فكل منظمة تختلف من حيث طبيعتها ومهامها وهيكلها. بدلاً من اتباع هيكل معين، ينبغي التفكير فيما يمكن أن يقدمه فريق يعمل بشكل جيد في كل وظيفة من هذه الوظائف وكيف يمكن قياس ذلك.

إذا كانت الفرق تحقق الأهداف المطلوبة، فمن المحتمل أن يكون الهيكل التنظيمي الحالي مناسبًا. ولكن إذا كان هناك نقص في التواصل أو مشاكل تتطلب دمج الفرق تحت مدير مشترك، فقد يكون من المناسب إعادة النظر في الهيكل التنظيمي.

مراكز العمليات الأمنية (SOC) الطبقية

بالنسبة لأدوار المحللين، يتم تنظيم العديد من الفرق وفق هيكل طبقي حيث يمثل المحللون في المستوى الأول دورًا مبتدئًا. مع اكتساب الأفراد خبرة، يمكن ترقيتهم إلى مستوى أعلى. غالباً ما يتضمن دور المستوى الأول عمليات محددة بوضوح تساعد القادمين الجدد على فهم قواعد SOC والبيانات المتاحة، لكن قد يُفرض عليهم بعض القيود، مثل الأدوات المتاحة لهم أو البيانات التي يمكنهم الوصول إليها.

هناك مزايا وعيوب للهيكل الطبقي. من الإيجابيات أن تحديد المسؤوليات يساعد في التركيز على التعلم ويضمن سير العمل بشكل متكرر، مما يجعل الجميع على علم بمهامهم بدقة. أما الجانب السلبي، فهو أن القيود قد تسبب إحباطًا للمحللين، وخاصة إذا لم يُسمح لهم باستخدام أدوات متقدمة.

مع تقدم المحللين إلى المستويات 2 و 3، يتم منحهم المزيد من الحرية والمهام الأكثر تعقيدًا، مثل تحليل البرامج الضارة وهندسة الذاكرة العكسية. هذا التقدم يوفر حافزًا قويًا ويعتبر وسيلة فعالة لإدارة SOC عندما يتم تطبيقه بالشكل الصحيح.

مراكز العمليات الأمنية (SOCs) بدون هيكل طبقي

يشعر العديد من المحللين بالإحباط من مراكز العمليات الأمنية ذات الهيكل الطبقي، حيث يعانون من المهام المتكررة أو عدم الحصول على الفرصة للقيام بمهام أكثر تعقيدًا. لهذا، قد يكون نموذج العمل غير الطبقي خيارًا أفضل لبعض الفرق. في مراكز SOC غير الطبقية، يتم منح المحللين حرية أكبر للتعلم واستكشاف جميع البيانات والأدوات المتاحة بدون قيود مفروضة. وقد أظهرت الدراسات أن المحللين في هذا النموذج يشعرون برضا أكبر عن وظائفهم، مما يساعد على تحسين الاحتفاظ بالموظفين على المدى الطويل ويتيح للـ SOC بناء المواهب اللازمة للمهام المعقدة.

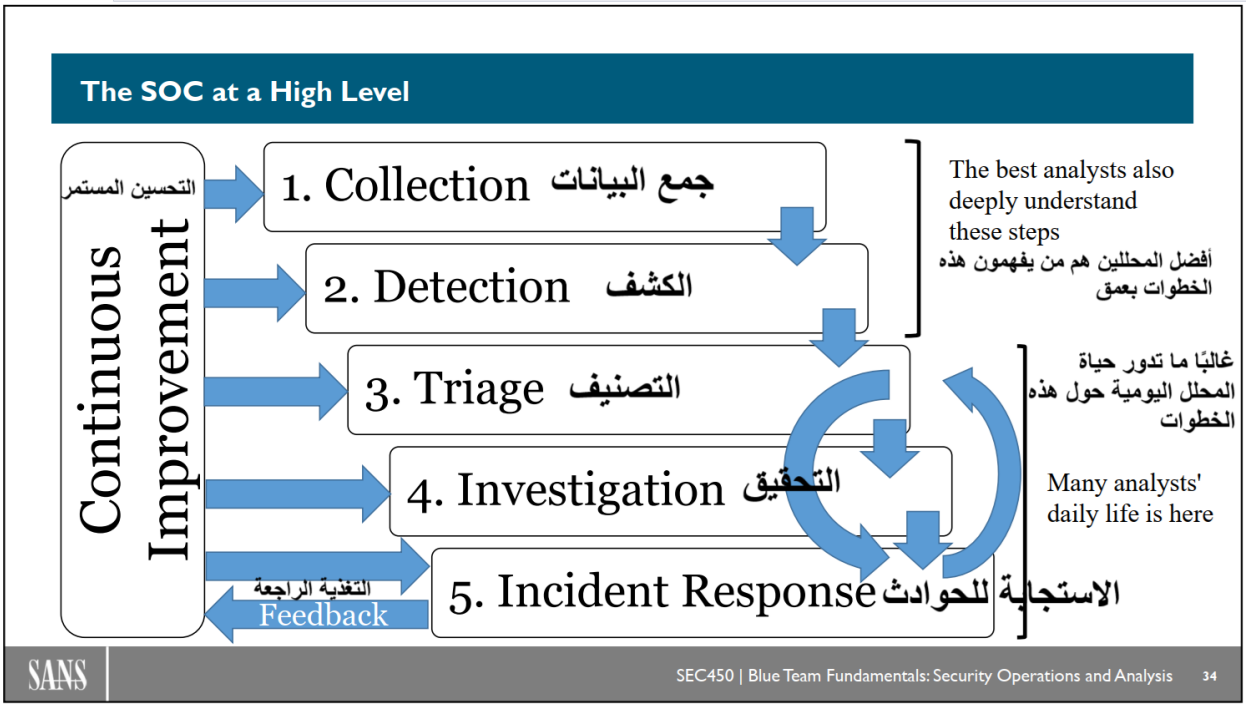
خصائص SOC غير الطبقي:

- **التعاون المشترك :**يعمل الجميع معًا لإنجاز المهام، مما يتطلب إدارة دقيقة للتنبيهات.
- **الوصول الكامل للأدوات والبيانات :**حتى المحللين الجدد يمكنهم استخدام جميع الأدوات المتاحة، ولكن يجب عليهم معرفة حدود قدراتهم.
- **التعلم السريع :**يتمتع المحللون بحرية أكبر في التعلم واكتساب المهارات، مع أهمية كبيرة للعمل الجماعي.
- **التقدم الوظيفي من خلال الألقاب :**يُستخدم نظام الألقاب مثل المحلل الأول والمحلل الرئيسي للتقدم المهني بدلًا من الترقيات الرسمية في الهيكل الطبقي.

في المقابل، يقدم نموذج SOC الطبقي مسارًا وظيفيًا واضحًا وأدوارًا محددة وتدفقًا منظمًا للمهام. على الرغم من أن ذلك قد يوفر كفاءة عالية في عمليات التحويل والمعالجة، إلا أنه قد يحد من قدرة المحللين على الاستكشاف والتعلم، وقد يؤدي إلى مشكلات في الاحتفاظ بالموظفين بسبب التكرار في المهام وبطء التقدم.

كلا النموذجين لهما مميزاتهما وعيوبهما، ويعتمد القرار بشأن النموذج الأنسب على متطلبات الفريق وأهدافه.

مركز العمليات الأمنية (SOC) من منظور شامل



نظرة عامة علىSOC

بعد مناقشة هيكل الفريق والأهداف، سنلقي نظرة زمنية على كيفية عمل العمليات الأمنية بتفصيل أكبر عبر مجموعة من الخطوات الأساسية، التي يمكن تقسيمها على النحو التالي: جمع البيانات، الكشف، التصنيف، التحقيق،)وفي بعض الأحيان الاستجابة للحوادث إذا كانت هذه المسؤولية تقع على عاتق.(SOC

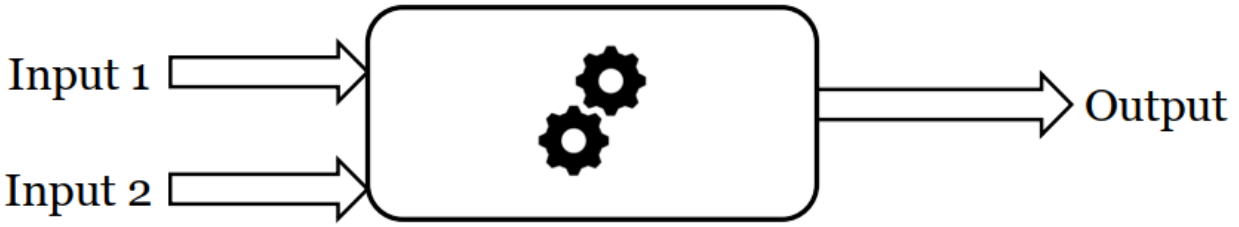
- **جمع البيانات :**تعتمد هذه المرحلة على تلقي البيانات ذات الصلة بالأمن والتي تساعد في فهم ما يحدث داخل البيئة.
- **الكشف :**من بين جميع البيانات التي تم جمعها، يجب تمييز العناصر المريبة في مرحلة الكشف. يعتمد نجاح هذه المرحلة على الأدوات المتاحة، ومعلومات التهديدات، ومعرفة تكتيكات وأساليب المهاجمين، وغيرها. تتحول العناصر التي تفي بعتبة معينة من الشك إلى تنبيهات يتم وضعها في قائمة التصنيف للمتابعة.
- **التصنيف :**غالبًا ما تكون هناك عناصر متعددة تحتاج إلى المتابعة في الوقت نفسه، لذا من المهم تصنيف العناصر الأكثر خطورة أو أهمية. من الناحية المثالية، تساعد الأدوات على تسليط الضوء على العناصر الأهم. يعتمد نجاح هذه المرحلة على عدة عوامل، مثل معرفة مراحل الهجوم وأساليب الهجوم، وتقييم المخاطر، وإثراء البيانات، والخبرة بالبيئة.
- **التحليل :**بعد اختيار العنصر الأكثر خطورة، يجب الخوض في التفاصيل والتحقيق فيه لمعرفة ما إذا كان يمثل تهديدًا حقيقيًا، ومن ثم تحويله للاستجابة للحوادث إذا لزم الأمر. يجب أن يكون المحللون مدربين على إجراء التحقيق بدقة، وتجنب الانحياز المعرفي وأخطاء التحليل. يشمل هذا التحقيق التحقق من كون التنبيه إيجابيًا زائفًا أم لا، وأيضًا التحقيق في "ما حدث" في حالة الحوادث الحقيقية. يتطلب أداء هذه المرحلة تدريبًا مكثفًا ويزداد تحسنًا مع الخبرة، وسنركز على هذه الخطوة بشكل خاص في هذا البرنامج التدريبي.
- **الاستجابة للحوادث :**بعد إتمام التحقيق، يجب اتخاذ جميع الخطوات اللازمة لاحتواء المشكلة، والقضاء على المهاجم، واستعادة البيئة إلى وضعها الطبيعي. يجب أيضًا توثيق نتائج الحادث

والبحث عن التحسينات الممكنة لتحقيق أداء أفضل في المرة القادمة. هذا يقودنا إلى العملية الشاملة التي يجب أن تحدث في جميع المراحل: التحسين المستمر المدعوم بنتائج التحقيقات.

كل خطوة من هذه الخطوات تلعب دورًا حيويًا في تحقيق كفاءة عمليات الأمن. وجود ضعف في أي منها يؤدي إلى مشاكل أخرى في المراحل التالية من العملية، لذا من المهم التقييم والتحسين المستمر لكل خطوة.

وأخيرًا، فيما يتعلق بحياة المحلل اليومية، خاصة المحللين الجدد، نجد أن معظم وقتهم يكون في الخطوات 3 إلى 5. تعلم كيفية اختيار التنبيهات وتصنيفها يتطلب فهم دورات تطور الهجمات وتكتيكات الهجوم، وهذا موضوع واسع بحد ذاته. التحليل أيضًا موضوع واسع ويشمل تدريب المحلل على إجراء التحقيق بشكل منهجي ودقيق. الهدف من هذا البرنامج التدريبي هو شرح هذه العمليات وتقديم الأدوات اللازمة لفهم كل خطوة وتحليلها بفعالية.

تفكيك عمليات وتقنيات مركز العمليات الأمنية(SOC)



لفهم وظائفSOC ، سنقوم بتبسيطها:

- تجريد الأدوات/الوظائف إلى "صندوق" بسيط يحتوي على مدخلات ومخرجات.
- التفكيك إلى مدخلات، مخرجات، وعمليات داخلية يوضح كيف يرتبط كل عنصر بالآخر.

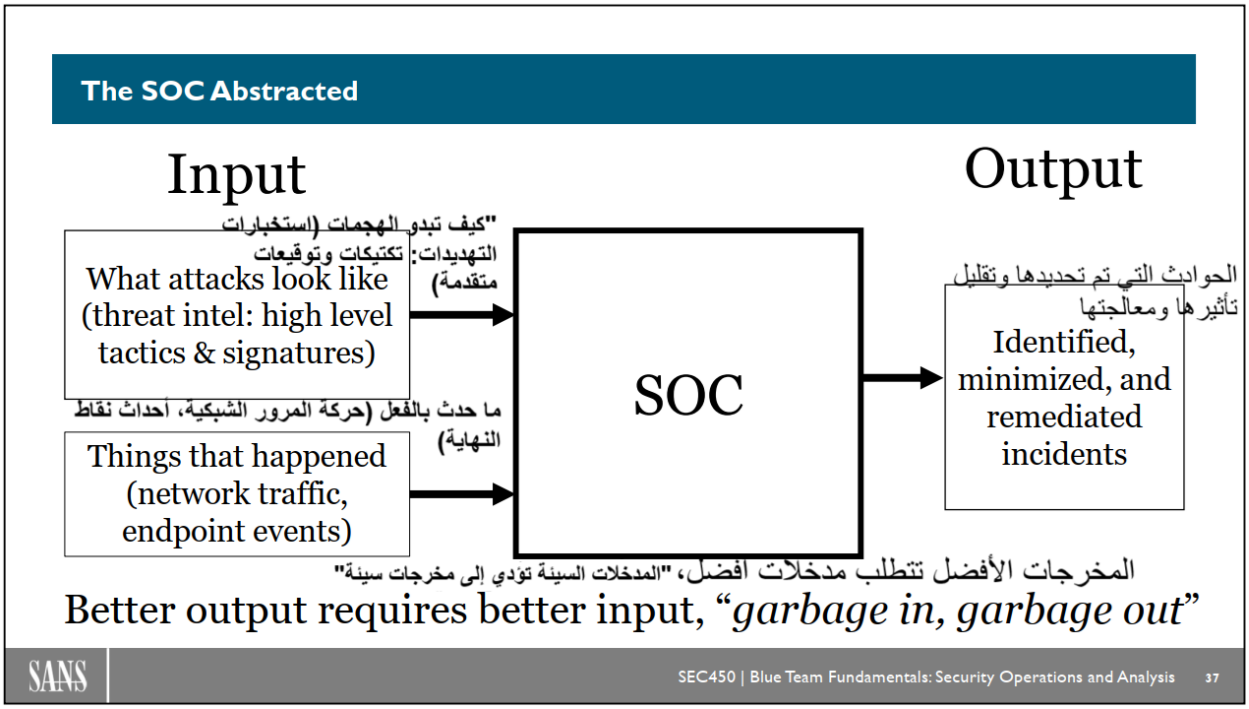
تفكيك عمليات وتقنيات SOC

أحد التحديات التي تواجه المحللين الجدد في مركز العمليات الأمنية (SOC) هو فهم كيفية تدفق البيانات التي يتعين عليهم التعامل معها بين جميع الأدوات في المركز. ورغم أن SOC يتكون من تداخل معقد لأدوات وعمليات متعددة، فإنه يمكن فهم عمله إذا بدأنا ببساطة ونمينا فهمنا تدريجيًا. لتحقيق ذلك، سنقوم في هذا البرنامج التدريبي بتفكيك وتبسيط الأنظمة المعقدة إلى مجموعة من المدخلات، والعمليات الداخلية، والمخرجات.

يتيح لنا هذا الأسلوب فهم نوع المدخلات التي يستقبلها كل نظام، والعمليات الداخلية التي تعمل على هذه المدخلات، وما يُتوقع من النظام إنتاجه كمخرجات. على سبيل المثال، دعونا نأخذ نظام كشف التسلل .(IDS) ورغم كونه جهازًا معقدًا، يمكننا تبسيط ما يفعله لفهم سريع. في جوهره، يستقبل IDS كمدخل حركة مرور الشبكة المحالة إليه ومجموعة من التواقيع لمحتويات معينة في حركة المرور. يعمل داخليًا على مطابقة حركة المرور مع التواقيع الموجودة في قائمة المدخلات، ويخرج تنبيهات يتم توجيهها في النهاية إلى قائمة التنبيهات في .SOC لا نحتاج لمعرفة تفاصيل كيفية عمل IDS لفهم دوره، بل يكفينا معرفة أن المخرجات هي نتاج المدخلات، التي تتمثل في حركة المرور التي يمكنه رؤيتها وعدد ونوع التواقيع الفعالة. الأمر بسيط، أليس كذلك؟

بمجرد فهم كل وظيفة على حدة بهذه الطريقة، يصبح من الأسهل إعادة دمجها ورؤية الصورة الكبيرة لكيفية عمل جميع هذه العناصر معًا. من خلال هذه الطريقة، سنعمل على فهم كيفية استخدام SOC لكل أداة من الأدوات المتاحة بالشكل الأمثل.

تجريد مركز العمليات الأمنية(SOC)



تجريد مركز العمليات الأمنية

رغم أن بناء الفهم من الأسفل وفهم جميع الأجزاء يعد مفيدًا، يمكننا أيضًا التعلم من الأعلى للأسفل عبر تجريد جميع التفاصيل لجعل المهمة واضحة. ماذا لو قمنا بتجريد SOC بالكامل؟ على مستوى عالٍ للغاية، ما هي المدخلات والمخرجات الأساسية لـSOC ؟ كما هو موضح بالشريحة أعلاه، يمكننا تبسيط الأمر بالقول إن SOC هو نظام يستقبل كمدخلات ما يحدث في البيئة وما يبدو عليه الهجوم، ليُنتج كخرج الحوادث التي تم تحديدها، تقليلها، ومعالجتها.

كما هو الحال مع أي نظام، إذا كنا نرغب في مخرجات أفضل، نحتاج إلى مدخلات أفضل (وهذا هو أصل عبارة "المدخلات السيئة تؤدي إلى مخرجات سيئة"). بالنسبة لـSOC ، يعني ذلك إما زيادة الرؤية أو تحسين المعرفة بماهية الهجوم. صندوق "SOC" هنا هو مجرد تجريد لمجموعة معقدة من التفاعلات، لكن على أبسط مستوى، هذا هو ما نقوم به وتلك هي المتغيرات الرئيسية التي تتحكم فيه. من خلال النظر إلى أدواتنا وأنظمتنا بهذه النظرة التجريدية العالية، على الرغم من أنها ليست مثالية، تساعدنا هذه الطريقة في فهم النظام وتحديد الأدوات التي يمكننا استخدامها عندما لا يعمل كما نرغب.

وظائف العمليات والتقنيات في مركز عمليات الأمن(SOC)

تنظيم مهام فريق الأمن:

- الأنشطة الأساسية لمركزSOC
  - **جمع البيانات** :معرفة ما يحدث على الشبكة والأجهزة
  - **الكشف** :تحديد العناصر المثيرة للاهتمام من البيانات التي تم جمعها
  - **الفرز والتحقيق** :تأكيد القضايا المكتشفة وتحديد أولوياتها
  - **الاستجابة للحوادث** :التعامل مع الهجمات والحد من تأثيرها
- القدرات التخصصية والإضافية
  - **معلومات التهديدات** :جمع معلومات لتحسين كشف الهجمات
  - **التحقيق الجنائي** :دعم الاستجابة للحوادث من خلال البحث المتعمق والهندسة العكسية
  - **التقييم الذاتي** :جرد الأصول، مراقبة التكوينات، تقييم الثغرات، فريق الاختراق، وغيرها

وظائف العمليات والتقنيات في مركزSOC

لنقم بتفصيل الوظائف العليا لمركز SOC إلى عناصر تعتبر غالبًا "وظائف أساسية" مقارنة بالمجالات التخصصية. تميل المهام الأساسية لمركز SOC إلى أن تكون ضمن مسؤولية محللي SOC أو من يعملون على مقربة منهم. قد تقوم الفرق الصغيرة بجميع هذه المهام ضمن نفس المجموعة، بينما تتطلب المجالات التخصصية عادة مهارات مختلفة إلى حد كبير؛ لذا فإن الأدوار التخصصية تُسند عادةً لأفراد محددين. تمتلك المنظمات الكبيرة فرقًا مخصصة للبحث الجنائي، واستخبارات التهديدات، واختبار الاختراق، بينما قد تلجأ المنظمات الصغيرة إلى الاستعانة بمصادر خارجية لهذه القدرات لزيادة الكفاءة في التكاليف.

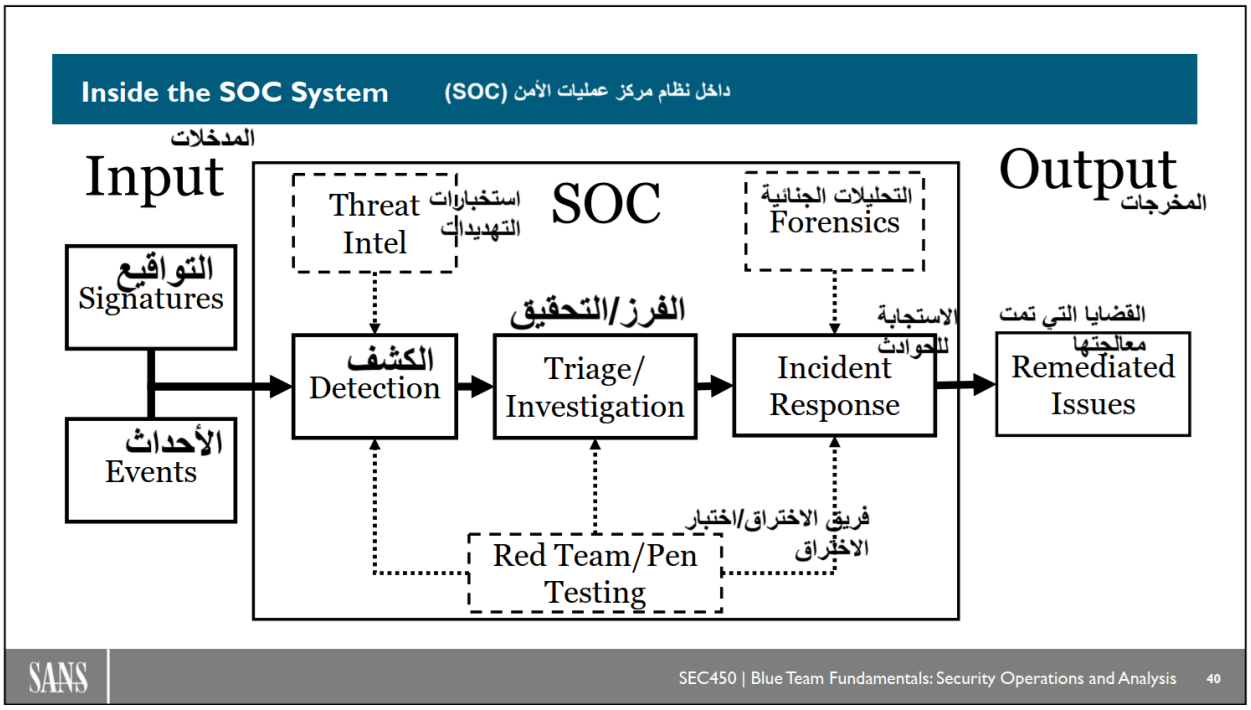
وظائف SOC الأساسية:

- **جمع البيانات** :يشمل التقنيات والعمليات التي تمكّننا من فهم ما يحدث على الشبكة والنقاط الطرفية. كما سنتناول لاحقًا، يمكن تقسيم هذه العملية إلى مراقبة الشبكة ومراقبة النقاط الطرفية/التطبيقات.
- **الكشف** :هدف وظيفة الكشف هو مراقبة البيانات المجموعة من الشبكة والنقاط الطرفية وتحديد أي علامات على اختراق محتمل بدقة. يمكن اعتبار هذه الوظيفة جزءًا من ما تقوم به أنظمة الكشف عن الاختراقات (IDS) على الشبكة والأجهزة، وبرامج مكافحة الفيروسات، وتحليلاتSIEM ، وأي أدوات أخرى تراقب الأحداث اليومية وتصدر تنبيهات عند اكتشاف اختراق محتمل.
- **الفرز والتحقيق** :يتم في هذه الوظيفة ترتيب وتحليل التنبيهات التي تم تحديدها لتحديد الأولويات والتحقق من مدى صحتها. في معظم مراكزSOC ، سيتم تحديد العديد من الأحداث المحتملة للبرمجيات الخبيثة، ويكون الدور الرئيسي لمحلل SOC هو التمييز بين الأحداث الحرجة والتحقق مما إذا كان هناك هجوم فعلي.
- **الاستجابة للحوادث** :مجال الاستجابة للحوادث مسؤول عن الاستجابة للمشاكل التي تم التحقق منها وضمان تقليل تأثير المشكلة. في مراكز SOC الصغيرة، يكون ذلك ضمن نطاق عمل المحللين، أما في المراكز الأكبر، فقد يكون هناك مجموعة منفصلة تعرف باسم فريق الاستجابة للحوادث CIRT) أو .(CSIRT بغض النظر عن هيكل المنظمة، تُعتبر الاستجابة للحوادث جزءًا أساسيًا من مهام فريق الأمن (البلو تيم).

القدرات التخصصية والإضافية:

- **استخبارات التهديدات** :مهمة فريق استخبارات التهديدات هي جمع معلومات مفصلة عن مجموعات الهجوم المهتمة بالمنظمة، وذلك لمساعدة فريق الأمن على الحصول على ميزة تكتيكية واستراتيجية ضد المهاجمين. إذا تمكنا من توقع أهداف وخطوات وبنية المهاجمين مقدمًا، سيكون من الصعب عليهم تحقيق أهدافهم.
- **التحقيق الجنائي** :وظيفة متخصصة تهدف إلى تحديد ما حدث بدقة خلال الاختراق. يمكن أن يشمل ذلك التحقيقات التقليدية على الأقراص الصلبة، أو ما هو أكثر تخصصًا مثل تحليل الذاكرة، الهندسة العكسية للبرمجيات الخبيثة، أو حتى عمليات.eDiscovery
- **التقييم الذاتي** :يُعد هذا المصطلح مظلة لمجموعة من الوظائف التي قد لا تكون بشكل مباشر ضمن .SOC تشمل هذه المجموعة وظائف مثل مراقبة التكوينات، تقييم الثغرات، اختبار الاختراق، فريق الاختراق، وجرد الأصول. تشترك جميع هذه الأنشطة في مساعدة فريق الأمن في أداء عملهم بفعالية، سواء بمراقبة القضايا المحتملة (إدارة الثغرات) أو اختبار استجابة الفريق الأمني للتهديدات المحاكية (اختبار الاختراق وفريق الاختراق). بغض النظر عن مكانها في هيكل المنظمة، تُعد جزءًا حيويًا من منظومة الأمان.

داخل النظام



لنأخذ الآن المناطق الوظيفية ونربطها بمخطط المدخلات/المخرجات عالي المستوى لمركز عمليات الأمن (SOC) لنبدأ بتطوير صورة أكثر تفصيلًا. عند النظر إلى هذا المخطط، تُظهر المربعات العريضة المكونات الأساسية لمركز SOC – وهي جمع البيانات، الكشف، الفرز، التحقيق، والاستجابة للحوادث. أما المربعات المتقطعة فهي تمثل الوظائف التي تساهم في تعزيز قدرات الوظائف الأساسية وتساعدنا على تحسين النتائج. على سبيل المثال، يعتبر فريق الاختراق (Red Team)قدرة تساعد في اختبار وظائف الكشف والاستجابة لدينا من خلال محاكاة نشاطات وتكتيكات هجومية واقعية. وتساعدنا التحليلات الجنائية في فهم الحوادث بعمق أكبر من خلال تحديد ما حدث على الأجهزة المتأثرة، وتحديد قدرات البرمجيات الخبيثة، أو معرفة البيانات التي قد تم سرقتها. كما تُسهم استخبارات التهديدات في تحسين قدراتنا على الكشف من خلال تقديم توقعات حول تصرفات الخصوم على مستوى استراتيجي وتكتيكي.

خلال هذه الدورة، سنقوم بفحص هذه المكونات الوظيفية الفردية والأدوات التي تساعد في تنفيذها، مع التركيز على مدخلاتها ومخرجاتها وما تتضمنه كل منها. الهدف هو التأكد من أنك لا تفهم فقط كيفية عمل كل نظام فردي، بل أيضًا كيفية تفاعلها مع بعضها لتكوين الصورة الكاملة كما تراها هنا.

معلومات هامة لمركز عمليات الأمن(SOC)

- **رسم تخطيطي للشبكة :**نسخة مبسطة لسهولة الرجوع إليها.
- **نقاط الرؤية :**تتضمن أجهزة "Taps" و "Span Ports"والتقاط الحزم الكاملة.(PCAP)
- **رسم تدفق البيانات :**يوضح كيفية وصول حركة المرور إلى الإنترنت.
- **رسم تدفق السجلات :**يوضح من أين تأتي السجلات وإلى أين تذهب.
- **خطة الاستجابة للحوادث :**تحدد ما يجب القيام به عند حدوث مشاكل.
- **خطة الاتصال :**تحدد من يجب إبلاغه ومتى.
- قائمة بالأصول الحيوية ونقاط الاتصال.
- خطط التعافي من الكوارث واستمرارية الأعمال.
- أي سياسات أو معايير أو إجراءات أو إرشادات أخرى ذات صلة.

معلومات هامة لمركز عمليات الأمن(SOC)

لأداء المهام الأساسية لمركز عمليات الأمن بكفاءة، يجب أن تتوفر بعض المعلومات الأساسية والبيانات المهمة لديه. أحد العناصر المهمة هو نظرة شاملة حول كيفية تدفق البيانات عبر الشبكة وأماكن تواجد نقاط الرؤية الخاصة بالمركز. في بعض الحوادث، يجب الإجابة عن سؤال مثل "هل كنا قادرين على رؤية تلك الحركة؟"؛ وبدون فهم دقيق لتدفق البيانات داخل الشبكة وأماكن مراقبتها، يصبح من الصعب الإجابة عن هذا السؤال، مما يؤدي إلى إرباك وتأخير في اتخاذ الإجراءات. من المثالي أن تتضمن هذه المعلومات تدفق حركة الإنترنت وحركة الشبكة الداخلية، وكذلك الأماكن التي يستطيع مركز العمليات فيها رؤية سجلات التدفق، والتقاط الحزم الكاملة، أو السجلات التي تشير إلى أي نشاط مشبوه.

لا نريد أن يقوم المحلل بالبحث عن سجلات غير موجودة، ثم يستنتج بشكل خاطئ أن الاختراق لم يحدث بسبب عدم وجود سجلات تدل عليه. فهم الأماكن التي تتم فيها التغطية بالمراقبة، وأماكن عدم توفرها يساعد على تجنب هذا الخطأ.

بالإضافة إلى هذه المعلومات، فإن وجود خطة استجابة للحوادث توضح الخطوات التي يجب اتخاذها في حالة وقوع حادث كبير يسهم في ضمان سلاسة العمل أثناء الكوارث. كما يجب وجود خطة اتصال لتجنب إضاعة الوقت في البحث عن الأشخاص الواجب الاتصال بهم وكيفية الوصول إليهم. وقائمة بالأصول الحيوية ضرورية للغاية حتى لا يكون هناك شك حول أهمية البيانات على أي خادم (وسنتناول تصنيف البيانات في وقت لاحق من الدورة). يصعب الدفاع عن بياناتك الأكثر أهمية أو حتى التعرف على أنها معرضة للخطر إذا كنت لا تعرف مكانها أو الأنظمة التي تستند عليها.

الوثائق التي يجب أن يكون المحللون على دراية بها

السياسات: توجهات عامة على مستوى عالٍ، شاملة وإلزامية

مثال: "يجب أن يكون لدى جميع الأنظمة المتصلة بالشبكة برنامج مضاد فيروسات مثبت"

المعايير: إلزامية أيضاً، تحدد كيفية التنفيذ أو مدى التطبيق

مثال: "إعدادات التكوين لوكلاء مضاد الفيروسات يجب أن تكون..."

الإجراءات: تعليمات خطوة بخطوة لإتمام عملية معينة

مثال: "كيفية تثبيت برنامج مضاد الفيروسات والتأكد من عمله"

الإرشادات: اختيارية، تتضمن إجراءات أو خطوات موصى بها حيث لا توجد معايير أو إجراءات محددة

مثال: "أفضل الممارسات لنشر برنامج مضاد الفيروسات"

الخطوط الأساسية: قائمة بإعدادات دقيقة للغاية (مثل معايير CIS)

حالات الاستخدام/الخطط: قواعد وإجراءات محددة خاصة بمركز العمليات الأمنية للكشف عن التهديدات

الوثائق التي يجب أن يكون المحللون على دراية بها

قد يكون من المربك للمبتدئين التمييز بين أنواع الوثائق المختلفة اللازمة لتشغيل مركز عمليات الأمن. قد تبدو بعض أنواع الوثائق متشابهة للوهلة الأولى، ولكن لكل منها محتوى يمكن تمييزه عن الآخر. إليك أنواع الوثائق وأغراضها المعترف بها بشكل عام:

السياسات: تُعتبر السياسات وثائق توجيهية على مستوى عالٍ وشاملة، لا تدخل في التفاصيل الدقيقة ولكن تحدد المتطلبات العامة للتكوين. عادةً ما تجيب السياسات على سؤال "ما" الذي يجب فعله. يجب اعتبار محتويات السياسات إلزامية.

المعايير: على عكس السياسات، تقدم المعايير تفاصيل أكثر حيث تحدد "كيفية" تحقيق شيء معين أو مقدار ما يجب تطبيقه. كما يجب اعتبار الالتزام بالمعايير إلزاميًا.

الإجراءات: توضح الإجراءات التعليمات خطوة بخطوة لإتمام مهمة معينة. يمكن اعتبارها أدنى مستوى من الوثائق من حيث احتوائها على تفاصيل محددة.

الإرشادات: تعتبر الإرشادات غير إلزامية. تقدم توصيات وإجراءات مقترحة للتكوين أو أفضل الممارسات.

الخطوط الأساسية: قوائم مفصلة للغاية، مثل معايير الأمان التي توفرها مركز أمن الإنترنت (CIS) لنظم التشغيل والتطبيقات.

حالات الاستخدام/الخطط: على عكس الأنواع الأخرى من الوثائق التي قد تجدها مستخدمة في جميع أنحاء المنظمة، تُعتبر حالات الاستخدام والخرائط (Playbooks) فريدة من نوعها لمركز عمليات الأمن. تختلف تعريفاتها من مؤسسة لأخرى، ولكن بشكل عام، حالات الاستخدام هي توثيق كامل لسبب ومنطق مشروط يمكن تنفيذه على جهاز أمني معين، غالبًا ما يكون نظام إدارة معلومات الأمان والأحداث (SIEM). قد تتضمن حالات الاستخدام، على سبيل المثال، "كشف محاولات تسجيل الدخول باستخدام القوة الغاشمة" أو "محاولة مستخدم الوصول إلى موارد غير مصرح بها". أحيانًا يُستخدم هذا المصطلح بالتبادل مع "الخطط" (Playbooks) وأحيانًا لا. قد يُستخدم مصطلح الخطط ليشير إلى شيء يشبه الإجراءات، ولكن يركز على استجابة للحوادث أو صيد التهديدات حيث يتم تنفيذ "خطة" لإبراز احتمالات النشاط الخبيث.

[1] https://www.cisecurity.org/cis-benchmarks/

[2] Cisco's definition of a playbook: https://blogs.cisco.com/security/using-a-playbook-model-to-organize-yourinformation-security-monitoring-strategy

قياس نشاطك والتواصل به باستخدام مقاييس مركز العمليات الأمنية(SOC)

- سيتم تقييمك بناءً على المقاييس التي تقوم بتقديمها!
- المقاييس الجيدة:
  - مستمدة من الأعلى إلى الأسفل – ما هو المتطلب المحدد الذي يساعدك هذا المقياس في تتبعه؟
  - قابلة للتنفيذ – هل هناك حد معين إذا تجاوز أو انخفض يجب أن تتخذ إجراءً؟ ماذا ستفعل إذا تم الوصول إلى هذا الحد؟
  - محددة بشكل جيد/قابلة للتكرار – إذا طلبت من شخصين جمع هذا المقياس، هل سيحصلان على نفس الرقم؟
  - محدثة بشكل متكرر وآلي – أي قيمة تقوم بتتبعها يجب ألا تتطلب ساعات من العمل للحصول عليها، ويجب تحديثها بسرعة كافية للتمكن من التفاعل مع التغييرات.
  - اسأل نفسك: "إذا كان هذا المقياس يتحسن، هل تحسنت فعليًا حالة الأمان؟"

قياس نشاطك والتواصل به

على الرغم من أننا لا نملك الوقت في هذا الدرس لتغطية نقاش شامل حول المقاييس، يجب أن يكون المحللون على دراية بأن المقاييس الموجهة للخارج هي المعيار الذي سيقيمون بناءً عليه. لكن مجرد أن يمكن تتبع رقم معين لا يعني بالضرورة أنه مقياس جيد للتقييم! يجب أن تكون المقاييس التي تود تتبعها متوافقة مع الأهداف، قابلة للتنفيذ، محددة وقابلة للتكرار، ويفضل أن تُجمع بطريقة آلية وبوتيرة متكررة. فالمقاييس التي لا تتبع هذه الإرشادات قد تصبح غير مفيدة، أو غير دقيقة، أو عبئًا كبيرًا، وفي أسوأ الحالات، يمكن أن تعطي انطباعًا بأن المركز لا يقوم بواجباته!

للمحللين :إذا وجدت نفسك ملتزمًا أو محاسبًا على مقياس لا توافق عليه، فحينها حان وقت النقاش مع مديرك. سنتناول هذا الأمر بشكل أعمق في اليوم الخامس، ولكن بإيجاز، إذا كنت تعتقد أن مقياسًا معينًا يحفزك على اتخاذ إجراءات لا تحسن الأمان فعليًا، فعليك أن تتحدث وتوضح هذا الأمر. فغالبًا ما يتعرض المديرون لضغوط من أصحاب القرار لاستخدام مقاييس معينة دون فهم حقيقي لطبيعة عملك. يجب أن تدرك أن استخدام المقياس الخاطئ سيؤدي إلى تدهور الأمان، ومن الأفضل للجميع أن تقدم شرحًا واضحًا لسبب ذلك واقتراح بديل أفضل. وكما هو مذكور في أسفل هذه الشريحة، يجب أن تكون المقاييس مبنية على الواقع؛ إذا تحسن الرقم بينما لم تتحسن فعليًا الأوضاع على الأرض، فهذا يعني أن لديك مقياسًا غير مرتبط بالواقع وأهداف الفريق، ويجب تصحيحه قبل أن يتسبب في مشاكل أكبر.

للإدارة :يجب أن تكون هذه المناقشة فعّالة مع فريقك؛ اسألهم إذا كانوا متفقين مع المقاييس التي تجمعها، وإذا لم يكونوا كذلك، كيف يمكنهم تحسينها! للحصول على مزيد من المعلومات حول المقاييس، يُعد MGT551 من SANS - بناء وقيادة مراكز عمليات الأمن – إضافة ممتازة لهذا الدرس. في هذا المقرر، نغطي بشكل موسع طرق تطوير مقاييس مفيدة وقيمة وتمثيلية لفريقك سواء في المهام التشغيلية أو المبادرات الجديدة. مكان رائع للبدء في إنشاء مقاييس متوافقة مع الأهداف من الأعلى إلى الأسفل هو نظام **GQM**(الذي صُمم في الأصل لتطوير البرمجيات، ولكن هذا الأسلوب يمكن تطبيقه أيضًا هنا). يمكن الاطلاع على الورقة البحثية حول هذه الطريقة على الموقع .**sec450.com/gqm**

نظرة عامة على مركز عمليات الأمن(SOC)

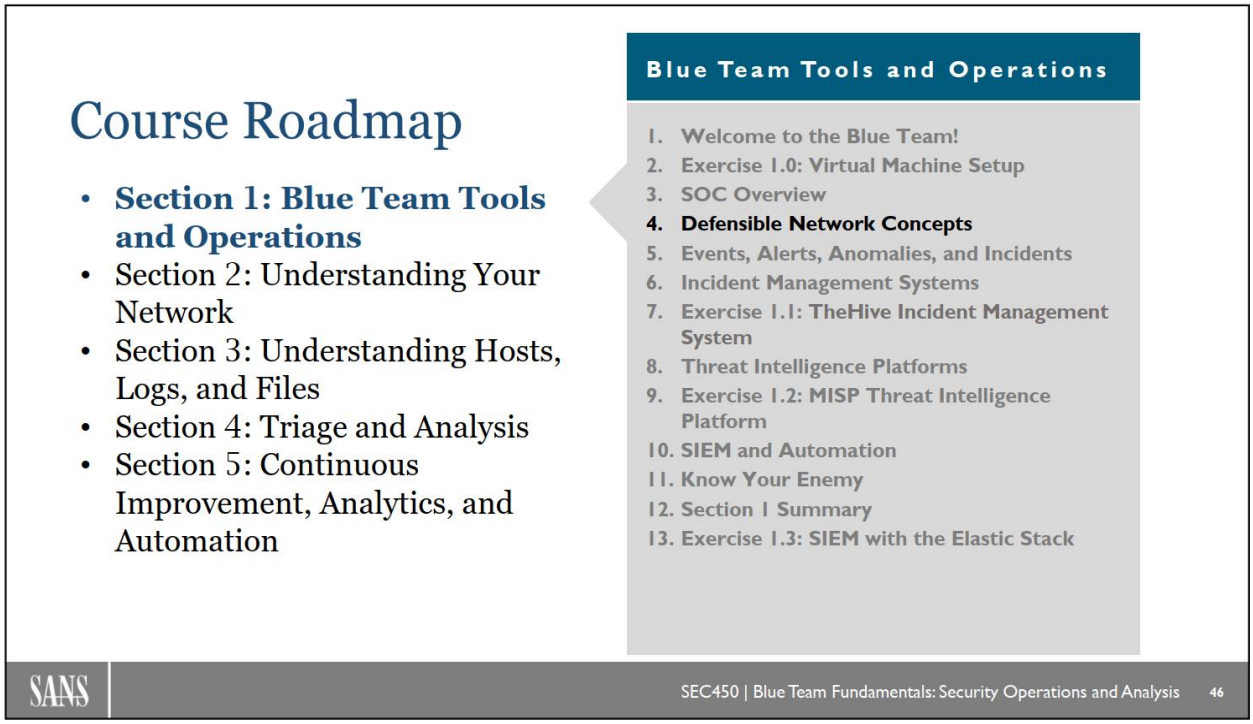
- مهمتك: تحديد وتقليل الانتهاكات
- التفويض يمنحك الصلاحية للقيام بذلك
- اللجنة التوجيهية ترشدك
  - تساعد في توجيه أنواع الضوابط التي يتم نشرها
- مركز العمليات الأمنية عبارة عن مجموعة معقدة من الأنظمة التي تساعد على تحقيق هذه المهمة
  - أشخاص، تكنولوجيا، عمليات، مدخلات ومخرجات
  - جمع المعلومات، الكشف، التقييم المبدئي، التحقيق، الاستجابة للحوادث، معلومات التهديد، التقييم الذاتي، والتحليل الجنائي
- تختلف الهيكليات التنظيمية لمراكز العمليات الأمنية – لا توجد "أفضل" طريقة تنظيمية
- يجب جمع المعلومات الهامة ومراقبتها وفهمها

نظرة عامة على مركز العمليات الأمنية(SOC)

تناولنا في هذا القسم العديد من المفاهيم العامة لفهم مركز العمليات الأمنية، بدءًا من تعريف مهمته. وأكدنا على أنه رغم أننا نعمل في مجال أمن المعلومات، يجب أن نبقى مرتبطين بالهدف الأكبر – وهو تقليل المخاطر على الأعمال، مع مراعاة أن هذا هو الهدف الأساسي. يُعد التخطيط والتنفيذ لتحقيق هذا الهدف مفتاح النجاح لفريق الدفاع(Blue Team) ، وتُعتبر المقاييس إحدى الطرق الرئيسية للتعبير عن ذلك. كما يقال: "ما يتم قياسه، يتم إنجازه." يساعد قياس أدائك ليس فقط في تحسينه، بل أيضًا في سرد القصة التي توضح كيف أن الاستثمار في فريق الدفاع يحقق عائداً ملموساً.

قد تختلف الأدوار والهيكليات التنظيمية لمراكز العمليات الأمنية بشكل كبير بين المؤسسات، لكن هذا لا يعني وجود إجابة واحدة صحيحة. الفكرة من تقديم الأدوار، ومراكز العمليات الأمنية ذات المستويات المتدرجة أو غير المتدرجة، والرسوم البيانية التنظيمية المحتملة لمركز العمليات الأمنية هي لتوضيح أن هناك العديد من التكوينات الصالحة، وكل منها يحقق توازنًا مختلفًا. يمكن تحديد كيفية تنظيم فريقك بناءً على احتياجات الشركة، وتوجيهات اللجنة التوجيهية لمركز العمليات الأمنية، ومن يعملون داخله.

قدمنا أيضًا الأنظمة الوظيفية داخل مركز العمليات الأمنية وناقشنا كيف يمكن لنظرة شاملة للنظام أن تساعدنا في تحليل كل عملية فردية والتداخلات بينها. هذا يُبسط الطبيعة المعقدة لجميع عمليات فريق الدفاع ويجعل من السهل فهمها وتحسينها. سنواصل عرض العمليات من هذا المنظور خلال الدورة، حيث نحلل المدخلات، والمخرجات، والعوامل الداخلية التي تُشغل الأنظمة التي سنستخدمها يوميًا.



خريطة الدورة التدريبية

- **القسم الأول :أدوات وعمليات فريق الدفاع(Blue Team)**
- **القسم الثاني** :فهم الشبكة الخاصة بك
- **القسم الثالث** :فهم المضيفين، السجلات، والملفات
- **القسم الرابع** :التقييم والتحليل
- **القسم الخامس** :التحسين المستمر، التحليلات، والأتمتة

أدوات وعمليات فريق الدفاع(Blue Team)

1. مرحباً بك في فريق الدفاع!
2. التمرين 1.0: إعداد الآلة الافتراضية
3. نظرة عامة على مركز العمليات الأمنية(SOC)
4. **مفاهيم الشبكة القابلة للدفاع**
5. الأحداث، التنبيهات، الشذوذ، والحوادث
6. أنظمة إدارة الحوادث
7. التمرين 1.1: نظام إدارة الحوادثTheHive
8. منصات استخبارات التهديدات
9. التمرين 1.2: منصة استخبارات التهديداتMISP
10. إدارة الأمن والمعلومات (SIEM) والأتمتة
11. اعرف عدوك
12. ملخص القسم الأول
13. التمرين 1.3: إدارة الأمن والمعلومات باستخدام Elastic Stack

مفاهيم الشبكة القابلة للدفاع

في هذا القسم:

- ما الذي يجعل الشبكة "قابلة للدفاع"؟
- أنواع مراقبة البيانات المطلوبة لتحقيق الأمن
- مراقبة الأمان المستندة إلى الشبكة
- مراقبة الأجهزة والتطبيقات
- مراقبة السحابة
- مفاهيم توحيد البيانات المراقَبة
- تنسيق أنواع البيانات المختلفة للتوحيد

مفاهيم الشبكة القابلة للدفاع

سيتناول هذا القسم بعض الأسئلة الأساسية حول كيفية مراقبة الشبكة وكيف ينبغي أن يتم ذلك. سنناقش أنواع بيانات المراقبة الخاصة بالشبكة والأجهزة والسحابة، واستراتيجيتنا العامة لجمع هذه البيانات واستخدامها. بنهاية هذا القسم، يجب أن تبدأ في تقييم أنواع البيانات المتاحة لديك، وما قد يحتاج فريقك إلى إضافته أو جمعه بطريقة أفضل أو مختلفة.

الشبكات القابلة للدفاع

وفقًا لريتشارد بيتليك، فإن الشبكة القابلة للدفاع تتميز بما يلي:

- **مراقبة** :حيث يتم جمع بيانات الشبكة والأجهزة وتوحيدها في موقع مركزي.
- **جرد** :معرفة مكونات شبكتك بالكامل.
- **تحكم** :السيطرة على دخول وخروج حركة المرور والوصول إلى الاتصالات.
- **تحديد الملكية** :معرفة من يملك الخدمات المخدومة وتخطيط تشغيل الأصول.
- **التقليل** :تقليل السطح الذي يمكن للهجوم الوصول إليه.
- **تقييم** :تحديد الثغرات واختبار الدفاعات.
- **التحديث** :معالجة التحديثات والثغرات المعروفة.
- **قياس** :قياس تقدم مركز العمليات الأمنية وفرق تكنولوجيا المعلومات في تنفيذ هذه الخطوات.

يمنحك هذا فرصة لمقاومة الاختراقات.

الشبكات القابلة للدفاع

أحد المفاهيم الهامة التي يجب الاحتفاظ بها هو إجابة السؤال "ما الذي يجعل الشبكة قابلة للدفاع؟" بمعنى آخر، ما هي المعايير التي يجب أن تلبيها الشبكة الحديثة لتكون قابلة للدفاع ضد الخصوم المعاصرين؟ بناءً على مقالة من مدونة ريتشارد بيتليك في عام 2008 (والتي ما زالت ذات صلة)، يصبح الدفاع السيبراني صعبًا بدون بيئة تلبي هذه المواصفات.

"إن بنية الشبكة القابلة للدفاع هي بنية معلوماتية تتميز بما يلي:

- **مراقبة** :تتمثل أسهل الطرق وأقلها تكلفةً لتطوير شبكة قابلة للدفاع في نشر أجهزة مراقبة أمان الشبكة التي تلتقط بيانات الجلسات كحد أدنى، وبيانات المحتوى الكاملة إن أمكن، والبيانات الإحصائية. إذا كان بإمكانك الوصول إلى مصادر بيانات أخرى، مثل سجلات الجدران النارية/الموجهات/أنظمة الحماية من التطفل/أنظمة أسماء النطاقات/الوكلاء، ابدأ في استغلالها أيضًا. ينبغي أن تكون هذه خطوة سريعة، حيث يتم جمع البيانات من قبل مجموعة صغيرة ومركزية. يجب أن تبدأ دائمًا بالمراقبة، كما قال بروس شناير ببلاغة عام 2001.
- **جرد** :يعني ذلك معرفة ما تستضيفه شبكتك. بمجرد أن تبدأ في المراقبة، يمكنك الحصول على الكثير من هذه المعلومات بشكل غير مباشر.
- **تحكم** :بعد معرفة كيفية عمل شبكتك ومكوناتها، يمكنك البدء في تنفيذ ضوابط قائمة على الشبكة، مثل تصفية الدخول والخروج، والتحكم في قبول الشبكة، وغيرها. الفكرة هنا هي التحول من شبكة مفتوحة إلى أخرى يتم فيها تفويض النشاط مسبقًا قدر الإمكان.
- **تحديد الملكية** :تحديد أصحاب الأصول ووضع السياسات والإجراءات وخطط التشغيل الخاصة بالأصول. يمكن مبادلة هذه الخطوة بالخطوة السابقة. هذا العنصر هو شرط مسبق لإجراء الاستجابة للحوادث.
- **التقليل** :العمل مع أصحاب المصلحة لتقليل السطح القابل للهجوم على أجهزتهم. يمكنك تطبيق هذه الفكرة على العملاء والخوادم والتطبيقات والوصلات الشبكية، وما إلى ذلك. من خلال تقليل السطح القابل للهجوم، يمكنك تحسين قدرتك على أداء جميع الخطوات الأخرى، لكن لا يمكنك حقًا تنفيذ التقليل حتى تعرف من يملك ماذا.
- **التقييم** :عملية تقييم الضعف لتحديد الثغرات في الأصول. يمكنك وضع هذه الخطوة قبل التقليل. قد يجادل البعض بضرورة البدء بالتقييم، لكن قد يكون من الأسهل البدء بتعطيل الخدمات غير الضرورية أولاً.

- **التحديث** :يعني الحفاظ على الأصول محدثة ومؤمنة لمقاومة الهجمات المعروفة من خلال معالجة الثغرات المعروفة. يمكن أن تتسبب التحديثات أحيانًا في تعطل التطبيقات، ولهذا تأتي هذه الخطوة في النهاية.
- **القياس** :يضيف ريتشارد في كتابه "ممارسة مراقبة أمان الشبكة" الخطوة الأخيرة "القياس". هذه الخطوة تتضمن قيام فريق الأمان وتكنولوجيا المعلومات بقياس تقدمهم في تنفيذ الخطوات السابقة، مما يخلق حلقة تغذية مرتدة لضمان إنجاز المهام".

سنركز في هذا القسم على المراقبة. فهم نظام جمع البيانات والمراقبة هو الجزء الأول لتكوين فهم شامل في مركز عمليات الأمن والبدء كأحد المحللين المتميزين! بمجرد فهم ما يتم جمعه من بيانات، وكيفية جمعها، ومن أين تأتي، ستتمكن من تحديد المصادر المطلوبة للإجابة على أي سؤال تحليلي بشكل أكثر دقة

[1] https://taosecurity.blogspot.com/2008/01/defensible-network-architecture-20.html

جانبان للمراقبة

يمكن النظر إلى المراقبة من جانبين رئيسيين:

- ليست تقسيمًا مثاليًا لأنواع البيانات، لكنها مفيدة للنقاش.

مراقبة الطرفيات والتطبيقات *** مراقبة الشبكة

جانبان للمراقبة

أحد المفاهيم الأولى في تعريف "الشبكة القابلة للدفاع" لريتشارد بيتليك هو "المراقبة"، وهذا ما نركز عليه في هذا القسم. يمكن التفكير في المراقبة من خلال مجالين رئيسيين سنتناول كلا منهما على حدة. المجال الأول هو **المراقبة المعتمدة على الشبكة** —وهي القدرة على تحديد الأنشطة المشبوهة من خلال مستشعرات الشبكة وتسجيل بروتوكولات الشبكة. أما المجال الثاني فهو **مراقبة الطرفيات والتطبيقات**، والذي يتضمن القدرة على رؤية ما يحدث على الأجهزة الطرفية نفسها، بالإضافة إلى التطبيقات التي تعمل على هذه الأجهزة) أو ربما التطبيق فقط في حالة التطبيقات المستضافة على السحابة كخدمات.(SaaS

ملاحظة سريعة: هذا مجرد طريقة للتفكير وتقديم الأنواع المختلفة من سجلات البيانات. هذا التمييز ليس تقسيمًا دقيقًا وحاسمًا. قد يبدو أن العديد من السجلات يمكن أن تندرج ضمن كلا الفئتين، خاصة عند إدخال خدمات السحابة المستضافة. على سبيل المثال، استضافة DNS السحابي، وهي تعتبر تطبيقًا يعمل على نقطة طرفية في مكان ما، لكن بالنسبة لك فهي خدمة تُقدم وتُسجل استخدام بروتوكول الشبكة في مؤسستك. إذًا، هل هذا يُعد مراقبة شبكة أم مراقبة طرفية؟ في هذه الحالة، لا يهم التحديد الدقيق بقدر ما يهم السؤال عن أهمية السجلات لأمان النظام والتأكد من جمعها. تقسيمها إلى سجلات خاصة بالشبكة وأخرى بالطرفيات هو فقط طريقة لتسهيل التأكد من الحصول على كل ما هو ضروري.

[1] https://taosecurity.blogspot.com/2008/01/defensible-network-architecture-20.html

ما الذي يمكنك رؤيته في شبكتك؟
فكر في جمع بيانات شبكتك...

- هل يمكنك رؤية إحصاءات النطاق الترددي عالي المستوى وتدفق حركة المرور؟
- هل تعرف أي المنافذ قيد الاستخدام فعليًا؟
- ما البروتوكولات التي تُستخدم فعليًا على هذه المنافذ؟
- ما التطبيقات التي يتم الوصول إليها باستخدام تلك الخدمات؟
- هل تعرف أي النطاقات يتم زيارتها ومن قبل من؟
- هل يمكنك استرجاع بيانات الحزم الكاملة من المعاملات؟
- هل يمكنك اكتشاف حركة المرور المشفرة المشبوهة؟

كيف نحصل على هذه الإجابات؟

ما الذي يمكنك رؤيته على شبكتك؟

توقف للحظة وفكر في المعلومات التي تجمعها عن حركة مرور شبكتك. إذا سألت عن حجم تدفق البيانات بين أي عنوانين IP داخلي أو خارجي، هل يمكنك الحصول على تلك المعلومات؟ ماذا عن فحص جميع المنافذ المستخدمة، أو الخدمات الفعلية والبرامج التي تستخدم تلك المنافذ؟ هل يمكنك استرجاع نسخة من حركة المرور الفعلية على الشبكة؟ هل تعرف أي النطاقات يتم زيارتها؟ هل تقوم بفك تشفير أو على الأقل بجمع بيانات المعاملات لحركة المرور المشفرة؟ هذه بعض الأمور التي سنحتاج إلى مراقبتها لتوفير دفاع فعال يعتمد على الشبكة.

مراقبة أمن الشبكة

ما هي مراقبة أمن الشبكة(NSM) ؟

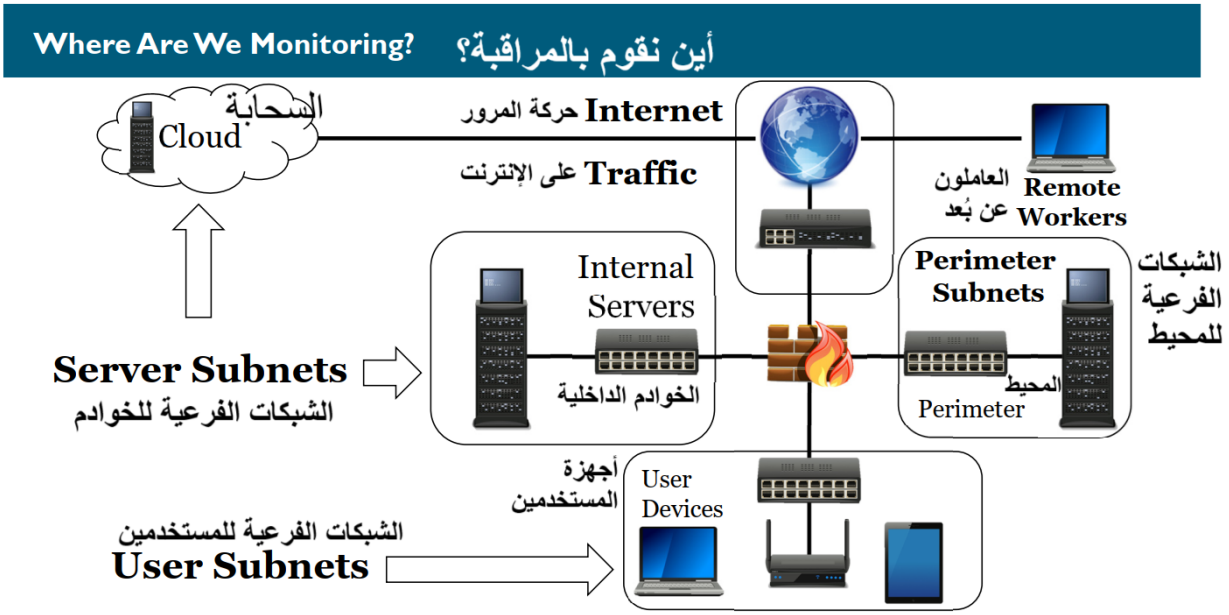
- تحليل حركة مرور الشبكة – "البيانات أثناء التنقل"
- خـــــــــدمات الشـــــــــبكةDNS :، (HTTP(S، SMB، RDP، FTP، SSH، إلخ.

- قد يتم تسجيلها بواسطة نقطة نهاية أو جهاز استشعار شبكي
- استخدام بيانات الشبكة لتحديد السلوك المشبوه
  - إيصال الاستغلال
  - نقل الملفات المشبوه
  - استكشاف الشبكة الداخلية والتحرك داخلها
  - حركة المرور للتحكم والقيادة/استخراج البيانات
  - استخدام مشبوه لبروتوكولات الشبكة داخل شبكتك

مراقبة أمن الشبكة

يمثـــل "المراقبـــة" العنصـــر الأول فـــي قائمـــة ريتشـــارد بيتليـــتش لأســـباب وجيهـــة. فـــإذا لـــم تـــتمكن مـــن رؤيـــة مـــا يحـــدث داخـــل الشـــبكة، ســـيكون مـــن الصـــعب للغايـــة، بـــل مـــن المســـتحيل، الـــدفاع عنهـــا. عنـــد مناقشـــة المراقبـــة، هنـــاك مصـــطلح يجـــب أن تكـــون علـــى درايـــة بـــه وهـــو "مراقبـــة أمـــن الشـــبكة". يشـــير مصـــطلح مراقبـــة أمـــن الشـــبكة (NSM) بشـــكلٍ ذاتـــي إلـــى تحليـــل مـــا يحـــدث داخـــل مؤسســـتك مـــن منظـــور الشـــبكة. تشـــمل NSM مراقبـــة حركـــة المـــرور، وتســـجيل التفـــاعلات بـــين الأجهـــزة، وتحليـــل ســـجلات الخـــدمات مثـــل HTTP و .DNSيـــتم تنفيـــذ NSM غالبًـــا مـــن خـــلال أجهـــزة متعـــددة تقـــوم بمراقبـــة حركـــة المـــرور علـــى الشـــبكة، وتســـجيل كـــل مـــا تلاحظـــه، أو تحديـــد النشـــاط المشـــبوه فقـــط. عـــادةً مـــا تســـتفيد NSM مـــن مقـــابس الشـــبكة، أو منافـــذ النســـخ المتطابقـــة فـــي المفـــاتيح، أو أجهـــزة أكثـــر تعقيـــدًا لمراقبـــة حركـــة المـــرور مباشـــرةً. ســـيتم مناقشـــة هذا الموضوع بمزيد من التفصيل في الكتاب الثاني.

أين نقوم بالمراقبة؟



أين نقوم بالمراقبة؟

السؤال الحقيقي هو: أين لا نقوم بالمراقبة؟ في الوضع المثالي، يجب أن يكون لدينا أجهزة استشعار لمراقبة أمن الشبكة (NSM) مثبتة في جميع الشبكات الفرعية، بالإضافة إلى جمع المعلومات على مستوى النقاط الطرفية لجميع الأجهزة داخلها. توضح الشريحة شبكة أساسية جدًا تحتوي على الإنترنت وموجّه حدودي في الأعلى، يقود إلى جدار ناري محيطي، والذي يدير حركة المرور للشبكة الداخلية أيضًا. في الشبكة، هناك خوادم متاحة على المحيط للإنترنت، بالإضافة إلى خوادم داخلية غير متاحة للجمهور. وفي الأسفل، هناك شبكة فرعية مليئة بأجهزة المستخدمين. إضافة إلى كل الأنظمة المحلية، لا يمكننا أن نغفل عن الأجهزة الموجودة خارج جدراننا، مثل الخدمات السحابية والعاملين عن بُعد والمزيد (وهو جزء كبير من شبكتنا، خاصةً بعد عام 2020).

في شبكة مثل هذه، يجب أن يكون كل جهاز جزءًا من عملية المراقبة. يمكن لجدران الحماية، والموجّهات، والمحولات إرسال معلومات حركة المرور، كما يمكننا استخدام أجهزة النسخ المتطابقة أو مقابس الشبكة للحصول على لقطات كاملة للبيانات. في السحابة، يوفر مقدمو الخدمات السحابية عادةً القدرة على تسجيل تدفق الشبكة واستخدام مقابس الشبكة الافتراضية لتسجيل كل حركة المرور داخل وخارج أي واجهة محددة.

لمراقبة الشبكة الخاصة بأجهزة المستخدمين خارج شبكاتنا، يجب أن نستفيد من العملاء أو وكلاء الأمن أو الوكلاء السحابية أو مصادر البيانات الخاصة بكل منصة لضمان مراقبة إعداداتها وحالتها الأمنية. العديد من أدوات الكشف والاستجابة على النقاط الطرفية (EDR) وحتى البرامج المجانية مثل Sysmon، يمكنها على سبيل المثال تسجيل معلومات حركة المرور الأمنية ذات الصلة مباشرة على النقاط الطرفية.

ما الذي يمكنك رؤيته على نقاط النهاية الخاصة بك؟

فكر في نقاط النهاية لديك...

- ما الذي يعمل الآن، وما هي الوسيطات التي تم استخدامها في سطر الأوامر؟
    - هل قام أحد بتثبيت برامج غير مصرح بها؟
    - ما هي السكربتات التي تم تشغيلها؟
- ما هي الثغرات التي قد يكون النظام عرضة لها؟
- هل حدثت تغييرات في ملفات النظام الحرجة أو التكوينات؟
- هل تحتوي أي أنظمة على عناصر بدء تشغيل مشبوهة؟
- من الذي قام بتسجيل الدخول إلى النظام وكيف؟

كيف نحصل على هذه الإجابات؟

ما الذي يمكنك رؤيته على نقاط النهاية الخاصة بك؟

بعد أن ناقشنا بعض مفاهيم مراقبة أمن الشبكة، دعونا نوجه انتباهنا إلى نقاط النهاية. على الرغم من أن مراقبة الشبكة جزء أساسي من استراتيجيتنا، فإن نقاط النهاية نفسها هي التي تحتفظ بالبيانات التي يسعى معظم المهاجمين للحصول عليها، وبالتالي فإن رؤية نقاط النهاية لا تقل أهمية عن رؤية الشبكة، إن لم تكن أكثر أهمية. معرفة البرامج المثبتة، والخدمات التي تعمل، وما إذا كانت عناصر التكوين الأساسية قد تغيرت، أو ما إذا تم تشغيل سكربتات، أو إضافة عناصر بدء تشغيل تلقائي، كلها معلومات مهمة للحفاظ على مراقبة الأجهزة في شبكتك.

تمتلك المنظمات عادةً رؤية جيدة لحركة المرور الشبكية، لكن قد تكون نقاط النهاية في وضع مختلف تمامًا. ظهرت العديد من الحلول مؤخرًا مثل أنظمة الكشف والاستجابة للنقاط الطرفية (EDR) وأيضًا أنظمة الكشف والاستجابة الموسعة (XDR) لدعم هذه القدرات، ولكن ليس كل منظمة تمتلكها أو تستطيع تحمل تكلفتها. إذا كنت قادرًا على الإجابة عن الأسئلة السابقة من منظور أجهزتك، فاعتبر نفسك محظوظًا ومتقدمًا في مجال المراقبة. وإذا لم تستطع، فلا تستسلم لافتراض أنك بحاجة إلى أحد هذه الأدوات التجارية للحصول على هذه الإجابات؛ هناك حلول مجانية مثل Sysmon من Sysinternals متاحة الآن لكل من Windows وLinux، ويمكنها المساعدة في تتبع بعض هذه البيانات الأساسية دون تكلفة! سنتناول مراقبة الأجهزة بعمق أكثر في الكتاب الثالث.

مراقبة نقاط النهاية والتطبيقات
وتعرف أيضًا باسم المراقبة الأمنية المستمرة (CSM):

- بيانات نقاط النهاية النموذجية - "البيانات الثابتة"
  - مراقبة التكوين والمقاييس الأساسية
  - فحص الثغرات الأمنية
  - مراقبة سلامة الملفات/السجل
  - العمليات والخدمات الجارية
  - عناصر التشغيل التلقائي
- **سجلات التطبيقات**
  - سجلات الوصول والمصادقة
  - سجلات تدقيق الأنشطة
  - أنشطة أخرى ذات صلة بالأمان

المراقبة الأمنية المستمرة

المراقبة الأمنية المستمرة (CSM) تمثل جانب الأمان القائم على المضيف في المعادلة الأمنية، وهو مصطلح يبدو أقل وضوحًا من مراقبة أمان الشبكة (NSM). تُعنى المراقبة الأمنية المستمرة بجمع بقية المعلومات — البيانات التي يمكن تسجيلها من نقاط النهاية في الشبكة. وتركز CSM على مراقبة التكوينات والمقاييس الأساسية، بالإضافة إلى تحليل وتسجيل المعلومات المتعلقة بتغييرات الملفات والسجلات، والعمليات، وعناصر التشغيل التلقائي وما شابه. كما تشمل تحديد وتتبع الثغرات الأمنية الموجودة في البيئة. ويشير مصطلح "المستمرة" في CSM إلى أن هذه المراقبة لا تتم بشكل "دوري أو متقطع للتحقق من بقاء الأشياء كما هي"، بل يجب أن تتم بشكل مستمر.

هذا يعني أنه في اللحظة التي يحدث فيها شيء غير متوقع على نقطة النهاية، مثل تشغيل ملف تنفيذي للفيروسات، سيتم إعلامك في الوقت الفعلي تقريبًا. وغالبًا ما يتم تحقيق هذا النوع من المراقبة من خلال سياسة قوية للتدقيق والتسجيل، مع مركزية ما يتم تسجيله في نظام إدارة أحداث الأمان والمعلومات (SIEM).

تصوير جمع أحداث نقاط النهاية

مصادر جمع البيانات من نقاط النهاية:

- سجلات جناح الأمان
- أدوات EDR و XDR وحزم حماية نقاط النهاية
- برامج مكافحة الفيروسات، HIDS/HIPS
- الماسحات الضوئية للثغرات، مراقبة سلامة الملفات (FIM)، التحكم في التطبيقات
- سجلات نظام التشغيل والتطبيقات
- سجلات المصادقة
- سجلات الخدمات والعمليات
- عناصر التشغيل التلقائي
- سجلات الوصول والتدقيق للتطبيقات

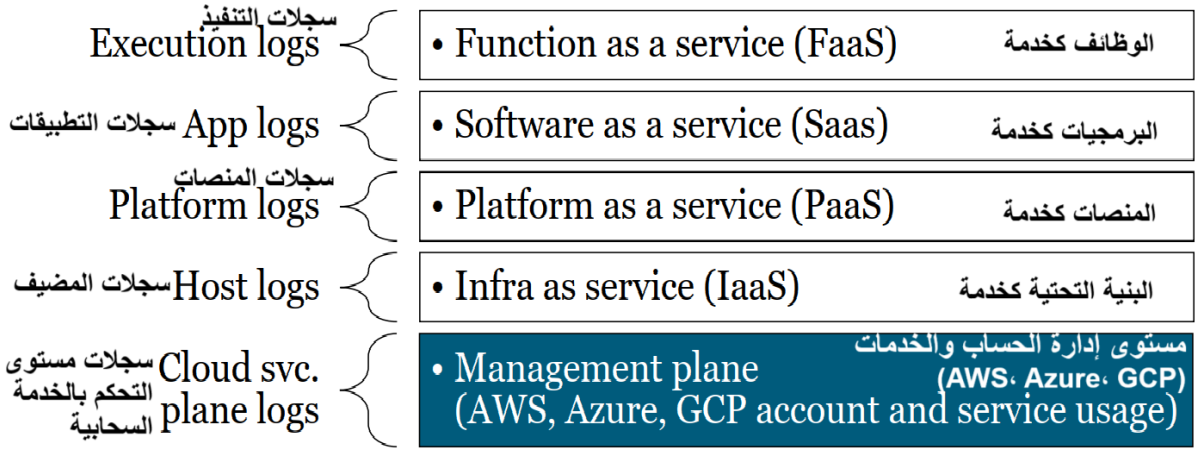
1 إرسال السجلات إلى نظام إدارة أحداث الأمان والمعلومات (SIEM)

تصوير جمع أحداث نقاط النهاية

تكون بيانات نقاط النهاية (CSM) عادةً موجهة نحو ملفات السجل، وبالتالي تركز على جمع معلومات نقاط النهاية بشكل موثوق وكامل. وغالبًا ما تقوم نقاط النهاية إما بتشغيل وكيل للسجلات يجمع المعلومات ويرسلها إلى SIEM، أو تحتوي على برنامج مخصص مثل EDR يجمع المعلومات في نظام منفصل.

ماذا عن السحابة؟

لقد اتجهنا جميعًا لاستخدام خدمات السحابة بمستويات تجريد مختلفة. كيف نقوم بتسجيلها؟ يعتمد ذلك على مستوى التجريد...



ماذا عن السحابة؟

قد تتساءل: "ماذا عن الخدمات السحابية؟" وهل تُعتبر هذه السجلات سجلات شبكة أم نقاط نهاية؟ بدايةً، لا تنشغل كثيرًا بتصنيفها، فالفكرة هي إطار لتنظيم أنواع البيانات.

- **البنية التحتية كخدمة – (IaaS)** عندما تشتري جهازًا افتراضيًا داخليًا من مزود خدمة سحابية، تكون السجلات مشابهة تمامًا لما لديك في أي جهاز تملكه وتتحكم فيه. في هذه الحالة، الجهاز افتراضي وعلى السحابة، لكن لا يزال بإمكانك تثبيت وكيل سجل SIEM/EDR، وتسجيلات نظام التشغيل يمكن جمعها كما هو معتاد في أغلب الأحيان. في حال الأجهزة الافتراضية على السحابة، يمكنك استخدام المنصة السحابية نفسها للحصول على تسجيلات مريحة. بعض موفري السحابة يقدمون إصدارًا خاصًا من نظام التشغيل مع إعدادات لتمكين هذه الميزات، تتضمن عوامل تسجيل محددة لجمع السجلات في لوحة مراقبة السحابة. مثال على ذلك، شراء جهاز Linux على AWS مع وكيل Amazon CloudWatchلتسجيل الأحداث المهمة في لوحة.CloudWatch
- **المنصات كخدمة – (PaaS)** تقع المنصات كخدمة بين IaaS وSaaS، والهدف هنا غالبًا هو تشغيل تطبيق برمجي محدد دون الحاجة لشراء البنية التحتية أو تثبيت التطبيق بنفسك، مع الحفاظ على قدر من التحكم في التطبيق نفسه. مثال على ذلك هو شراء خادم قاعدة بيانات. يتعين أن تقدم هذه التطبيقات سجلات أمان قابلة للتسجيل والمراقبة للنشاطات المشبوهة، كما يتم تطبيق استراتيجية التسجيل الأمني لقواعد البيانات الخاصة بك باستثناء تسجيلات نظام التشغيل الذي أصبح غير مرئي.
- **البرمجيات كخدمة – (SaaS)** هذا النوع من التطبيقات السحابية شائع جدًا. تقوم الشركات بتشغيل تطبيقات مختلفة كأنظمة إدارة الموارد البشرية أو أدوات إدارة المعرفة. ومن هنا تأتي أهمية تسجيل من يدخل إلى النظام، وتدقيق ما يقومون به داخل التطبيق، وتسجيل عمليات الوصول مع إدخال وإخراج البيانات حسب الإمكان لرصد محاولات الاختراق المحتملة. السؤال هنا هو، هل سيوفر مزود SaaS مستوى الرؤية المطلوب؟ الآن "تطبيقهم"، لذا هم من يحددون السجلات المتاحة لك.
- **الوظائف كخدمة – (FaaS)** ماذا عن أعلى مستوى من التجريد، "الخادم المستضاف كوظائف" أو ما يعرف بـFaaS ؟ يتضمن هذا خدمات مثلAWS Lambda ، حيث تدفع

لأمازون لتشغيل أجزاء (وظائف) من الكود بناءً على عدد مرات الاستدعاء وموارد المعالج المستخدمة. في هذا السياق، يتم التركيز على مراقبة مقاييس الاستدعاء لضمان تماشيها مع التوقعات، وتسجيلات الإدخال والإخراج في الوظائف الخاصة بك، حيث يمكنك تضمين شيفرة لتسجيل البيانات المدخلة، والمخرجة، والإجراءات المتخذة، ومراقبة هذه السجلات لمؤشرات على مشاكل الأمان.

- **مستوى إدارة السحابة** –لا تنسى سجلات الخدمة السحابية الجديدة! يجب عليك تسجيل من يقوم بتسجيل الدخول، وماذا يفعل من حيث إنشاء، أو إنهاء، أو تعديل البرامج والبنية التحتية السحابية وأي بيانات اعتماد يتم استخدامها للوصول. الشركات التي تهمل ذلك قد تجد بيانات اعتمادها قد سُرقت، مما سمح لشخص غير مصرح له بتسجيل الدخول وإنشاء جهاز GPU مكلف لتعدين العملات المشفرة على حسابك!

عندما لا تكفي بيانات الشبكة ونقاط النهاية

السيناريو 1 – ملف البرمجيات الضارة	السيناريو 2 – فشلEDR
نظام يتصرف بشكل مريب ويقوم بـ: • التواصل مع عنوان IP جديد مرتبط بنطاق غير معروف. • تحميل ملف باسم."calc.exe" • يبدأ النظام في التصرف بغرابة بعد هذا الطلب. • نحتاج إلى إجابات سريعة، فأين نجدها؟	• تقوم بتثبيت مجموعة حماية جديدة لنقاط النهاية (EDR). • يتمكن المهاجمون من خداع موظف باستخدام طريقة لا يلتقطها نظام EDR في البداية. • يستخدم المهاجمون الوصول لإيقاف التسجيلات وتعطيل.EDR • يستمر الهجوم على الجهاز دون إعاقة. • كيف نعلم إذا قام أحدهم بتعطيل برامج الأمان؟

عندما لا تكفي بيانات الشبكة ونقاط النهاية

إليك مثالين شائعين حيث قد تكون بيانات كل نوع من هذه البيانات غير كافية.

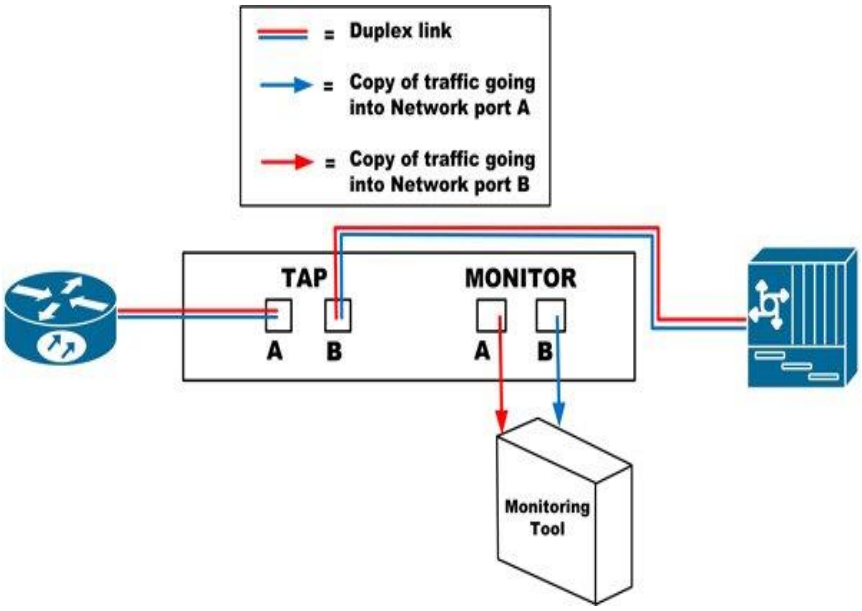
السيناريو 1 – عند التعامل مع البرمجيات الضارة

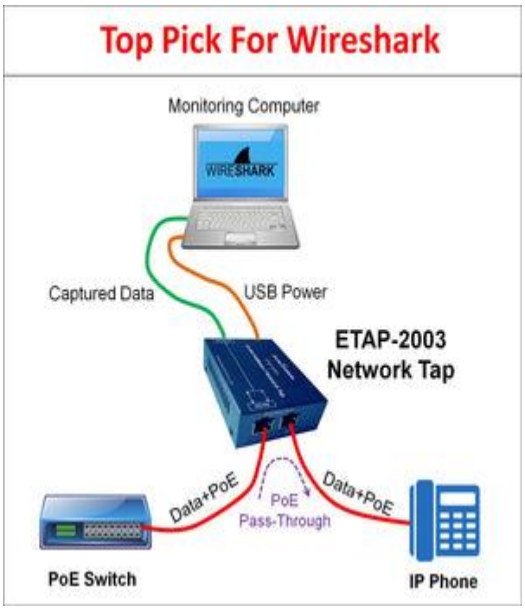
في هذه الحالة، الهدف الأساسي هو الحصول على إجابات بأسرع وقت ممكن حول ما حدث، حتى نتمكن من تحديد مدى الضرر واحتوائه ومعالجته. لنفترض أن انتباهك قد توجه أثناء عملية صيد التهديدات إلى تفاعل بين جهاز على الشبكة وعنوان IP ودومين غير معروفين. على الرغم من أن العنوان والدومين غير مدرجين في قوائم استخبارات التهديدات، يبدو أن الجهاز تصرف بغرابة أثناء هذا التفاعل. تشك في وجود خطأ ما، ولديك حزمة بيانات (PCAP) من هذا التفاعل، ولحسن الحظ، لديك بيانات TLS مفككة للتفاعل. تقوم بجلب المعلومات وتكتشف أن ملفًا اسمه "calc.exe" قد تم تحميله. ما هي خطوتك التالية؟ إذا كانت بياناتك مقتصرة على الشبكة فقط، فسيتطلب الأمر تحليل الملف في بيئة معزولة (sandbox) أو بوسائل أخرى لتحديد طبيعته وما قد يقوم به عند تشغيله على الجهاز، مما قد يستغرق وقتًا ثمينًا يسمح للمهاجمين بحرية أكبر قبل أن تتمكن من إيقافهم. أما إذا كان لديك سجلات نقاط النهاية، فيمكنك الحصول على إجابات لهذه الأسئلة بسهولة عن طريق مراجعة سجلات إنشاء العمليات للجهاز ومشاهدة ما حدث عند تشغيل الملف.

السيناريو 2 – فشل EDR في الكشف عن الهجوم

هذا الموقف قد يتجاهله بعض مزودي البرامج الأمنية أو يزعمون أنه غير محتمل، ولكن الحقيقة أن ذلك يحدث بشكل متكرر مع آثار مدمرة. في هذا السيناريو، يتمكن مهاجم من الوصول إلى أحد أنظمتك، ويفشل EDR في اكتشافه، ومع الوصول الذي حصل عليه، يتمكن من إيقاف مراقبة نقاط النهاية. قد يكون الأمر مؤلمًا أن ندرك أن المهاجمين يمكنهم فعل ذلك، رغم أن مزودي البرمجيات الأمنية وأنظمة التشغيل يحاولون جعل هذه المهمة صعبة وبطرق خفية. لكن الحقيقة تبقى أن ذلك يحدث في العديد من الحالات. الحجة هنا بسيطة: لا يمكن الاعتماد على نقاط النهاية كمراقبين موثوقين. الاعتماد على جهاز مخترق ومصاب ليؤدي ما نريده قد يكون وصفة لفشل محتمل. ورغم أن هذه الأجهزة قد تقوم بالمهمة بشكل صحيح غالبًا، إلا أنه في حالة مواجهة مهاجم متقدم، هل ستظل بيانات نقاط النهاية عالية الجودة موثوقة؟ ربما لا. الحل؟ الحصول على مصدر بيانات موثوق من الشبكة عبر وصلة الشبكة(network tap) ، وهي وسيلة لا يمكن ببساطة "إيقافها". بهذه

الطريقـــة، حتـــى إذا قـــام المهـــاجمون بقتـــل عمليـــات المراقبـــة، ســـيكون لـــديك ســـجل للحركـــة داخـــل وخـــارج الجهاز يمكن استخدامه كطريقة احتياطية للكشف.





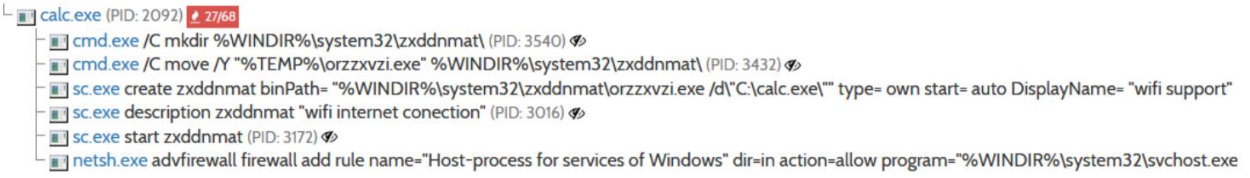
بيانات نقاط النهاية توفر تفاصيل أكثر

بشكل عام، تكون بيانات نقاط النهاية هي المصدر الأكثر تفصيلًا للبيانات:

- تتضمن تقريبًا جميع الأنشطة ذات الصلة بالأمان من النظام.
- يتم إسناد النشاط الشبكي إلى الملفات التي تولده.

إلقِ نظرة على شجرة إنشاء العمليات من السيناريو 1:

- هل هذا يُعتبر تهديدًا؟
- ما الصلاحيات التي كانت قيد التشغيل؟
- كيف نقوم بتنظيف النظام من هذا النشاط؟



بيانات نقاط النهاية توفر تفاصيل أكثر

بوجه عام، إذا كان عليك الاختيار بين مصادر بيانات نقاط النهاية والشبكة، فإن بيانات نقاط النهاية ستكون الخيار الأفضل. فهي أكثر تفصيلًا - حيث يمكن لنقاط النهاية تسجيل تفاصيل دقيقة جدًا حول العمليات التي تم إنشاؤها والأنشطة المرتبطة بها، إضافة إلى تفاعلاتها مع الشبكة (نعم، بيانات الشبكة التي تجمعها البرامج المثبتة على نقطة النهاية، حيث يبدو هنا أن نوعي البيانات يتداخلان معًا).

بالعودة إلى السيناريو #1، لنفترض أن برنامج calc.exe قد تم تشغيله، ولكن أداة EDR لدينا قامت بتسجيل التفاصيل. يمكننا الآن رؤية أسماء العمليات ومعاملات سطر الأوامر المرتبطة بتحميل الملف المشبوه مباشرةً. نستطيع رؤية أن calc.exe قام بكتابة ملف باسم عشوائي في مجلد windows\system32، وأنه أنشأ خدمة باسم عشوائي على جهاز Windows متخفيًا كخدمة Wi-Fi، وأضاف قاعدة جدار ناري جديدة. إذا أردنا تنظيف الجهاز يدويًا، فمن المحتمل أن يؤدي التراجع عن كل عنصر في قائمة العمليات إلى تحقيق ذلك.

لكن بدون بيانات نقاط النهاية، سيستغرق اكتشاف ما حدث أو ما سيحدث مع هذا البرنامج الضار وقتًا أطول على الأرجح. ستحتاج إلى الاعتماد على بيئة معزولة (sandbox) أو تقرير مفتوح المصدر يوفر هذه التفاصيل، وهذا ليس مضمونًا دائمًا؛ حيث يمكن لبعض البرامج الضارة اكتشاف تشغيلها في بيئة معزولة وتخرج من العملية. وبالتالي، بدون هذه البيانات التفصيلية من نقاط النهاية، قد لا تتمكن من اكتشاف الأمر على الإطلاق، خاصة إذا كان البرنامج الضار مخصصًا من مهاجم متقدم.

[1]https://www.hybridanalysis.com/sample/8a1c844413ffa69968758facbc48126a0a9f54234fe251bd1f8cb4e39ac112c0?environmentId%20=100

نظرة عامة على مصادر البيانات للمراقبة

بيانات NSM	بيانات نقاط النهاية والتطبيقات
• استخراج الشبكة • أجهزة التوجيه والمحولات • جدران الحماية الشبكية • IDS/IPS/NDR • الوكيل(Proxy) • جدران الحماية لتطبيقات الويب • سجلات الخدمة • DHCP، DNS، HTTP(S)، SMTP، SMB، FTP، SSH، Kerberos، إلخ.	• سجلات المصادقة • برامج مكافحة الفيروسات، HIDS/HIPS، EDR • سطر الأوامر للعمليات • الملفات التنفيذية • أدوات مسح الثغرات • DLP (حماية البيانات من التسرب) • سجلات الوصول للتطبيقات • سجلات التدقيق للتطبيقات

نظرة عامة على مصادر البيانات للمراقبة

عند جمع البيانات، من المفيد أن تميز في ذهنك بين نوعين من البيانات، ليس بناءً على ما إذا كانت بيانات نصية أم لا، ولكن بناءً على ما إذا كانت تلك البيانات تتعلق بحركة مرور الشبكة أو الأنشطة التي تحدث على نقطة النهاية. يمكن أن تأتي بيانات الشبكة من العديد من الأجهزة المختلفة، بعضها يسجل حركة المرور الفعلية، بينما يقوم البعض الآخر بتحويلها إلى سجلات تصف حركة المرور التي سيتم جمعها باستخدام نظام .SIEM بغض النظر عن الطريقة التي يتم بها تسجيل المعلومات، فهي في النهاية تقدم للمحلل ملاحظاته حول ما تم "رؤيته على الشبكة."

تشمل المصادر الشائعة لبيانات الشبكة:

- أدوات استخراج الشبكة مثلZeek
- بيانات NetFlow من أجهزة التوجيه والمحولات
- سجلات جدران الحماية التي قد تحتوي على إجراءات الحظر/السمح أو، في حالة "جدران الحماية الجيل التالي"، معلومات التطبيق الفعلية من الطبقة 7
- سجلات IDS/IPS أو NDR (الكشف والاستجابة للشبكة) مع اسم القاعدة التي تطابقها وسجل محتمل لحركة المرور نفسها
- سجلات الوكيل التي يمكن أن تبين أي مستخدم كان يزور أي موقع، بما في ذلك سمات الطبقة 7 مثل عناوين URL وطرقHTTP
- سجلات الخدمة من الخوادم التي تعمل على تطبيقات مثل Apache أو DNS من Windows/BINDأوDHCP

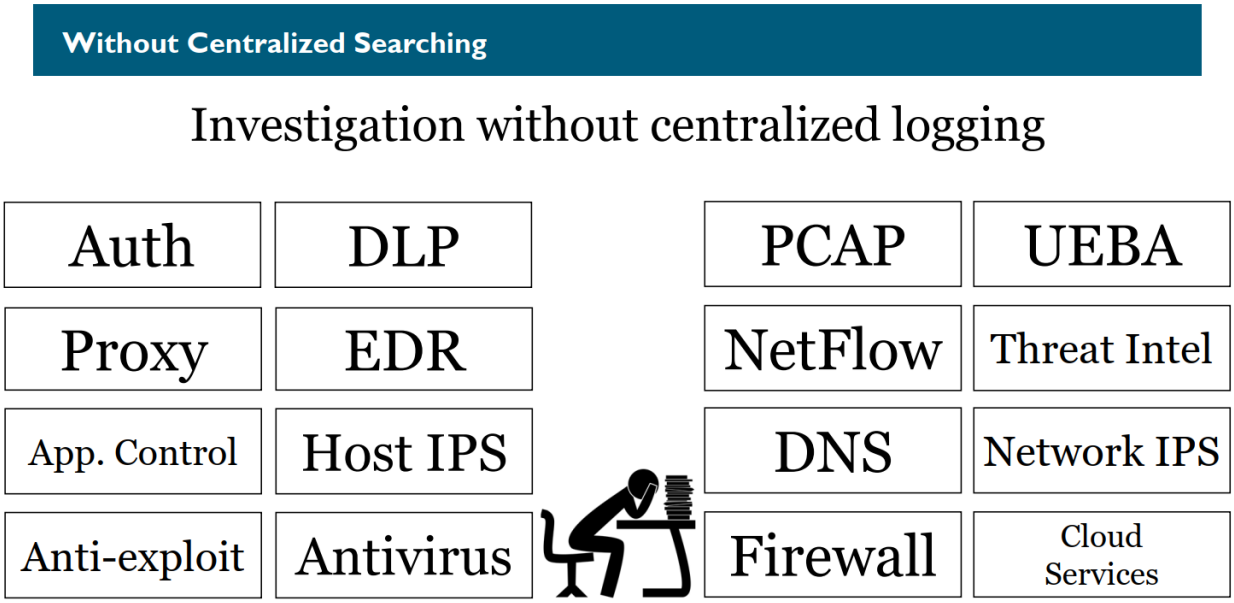
توفر بيانات نقاط النهاية الجزء الآخر من اللغز عند دمجها مع سجلات الشبكة. تشمل هذه السجلات عناصر مثل:

- بيانات المصادقة التي تُظهر محاولات تسجيل الدخول الناجحة والفاشلة
- سجلات برامج مكافحة الفيروسات التي تُظهر الملفات التي تم تحديدها على أنها خبيثة
- سجلات HIDS/IPS من المضيف التي قد تُظهر الملفات التي تم تعديلها، أو إذا تم إنشاء أي عمليات مشبوهة
- سجلات إنشاء العمليات التي تصف كيفية إنشاء كل عملية جديدة
- سجلات المعلومات والأخطاء من التطبيقات والأنظمة

- سجلات DLP التي قد تُظهر كيفية تحريك المستخدمين للملفات أو تفاعلهم مع البيانات الحساسة
- سجلات الوصول لتطبيق ما، مثل الطلبات الموجهة إلى خادم ويب
- سجلات التدقيق التي تم إنشاؤها لتطبيق ما – الإجراءات التي يتخذها المستخدم المسجل الدخول داخل تطبيق مثل تطبيق إدارة الموارد البشرية

ضع في اعتبارك أن بعض هذه المصادر قد تحتوي على نفس البيانات، لكن قد يوفر أحدها تفاصيل أكثر من الآخر. على سبيل المثال، قد تُظهر سجلات جدار الحماية الشبكي أن جهازًا كان يحاول التواصل على المنفذ 4444) المنفذ القياسي لبرنامج(Meterpreter ، ولكن سجلات جدار الحماية على مستوى المضيف أو EDR يمكن أن تُظهر أي عملية أنشأت هذه الحركة، وسطر الأوامر الذي تم استخدامه لاستدعاء تلك العملية. يساعدك هذا في التعرف على العملية الضارة فورًا، والتحقيق فيها، ثم القضاء عليها.

بدون البحث المركزي

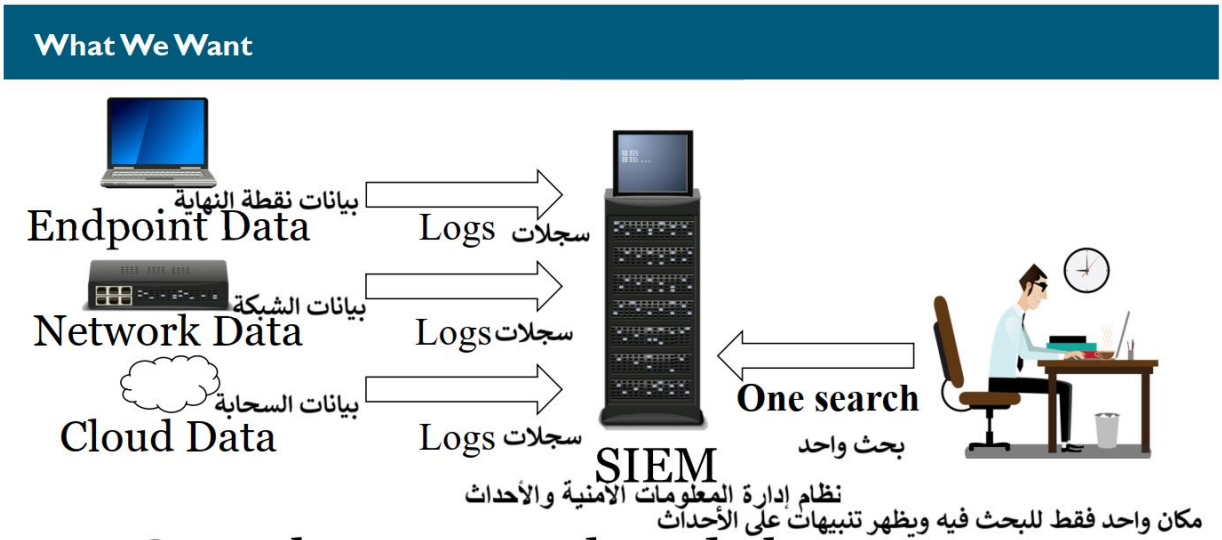


بدون البحث المركزي:

تعد مركزية السجلات والبيانات موضوعًا مهمًا آخر لعمل مركز عمليات أمن فعال. إذا لم تتمكن من جمع بيانات الشبكة ونقاط النهاية وتطبيقات السحابة وتوحيدها بحيث تصبح متاحة في واجهة بحث موحدة، فقد تصبح محاولة التحقيق في حادث أمني محتمل أمرًا مرهقًا. ضع في اعتبارك أن جميع أدوات الأمان وميزات تسجيل السحابة تقريبًا تأتي مع واجهة بحث خاصة بها. هذه ميزة رائعة عندما تحتاج إلى التحقيق في تنبيه باستخدام جميع ميزات المصدر المخصصة، ولكن كيف تعرف في البداية أي الأدوات قد تحتوي على معلومات حول تنبيه معين؟

يقوم نظام إدارة المعلومات الأمنية والأحداث (SIEM) بمهمة توحيد السجلات هنا. فهو يوفر مستودعًا مركزيًا لجميع بيانات المراقبة من الشبكة ونقاط النهاية ويمنحك مكانًا واحدًا مناسبًا للبحث عبرها جميعًا. بدون SIEM يوحد السجلات، إذا اضطررت للتحقيق في نشاط متعلق بعنوان IP معين، ستضطر إلى تسجيل الدخول إلى كل تطبيق بشكل فردي ومحاولة جمع أجزاء الحادث معًا – وهي طريقة غير فعّالة تمامًا للقيام بالأمر.

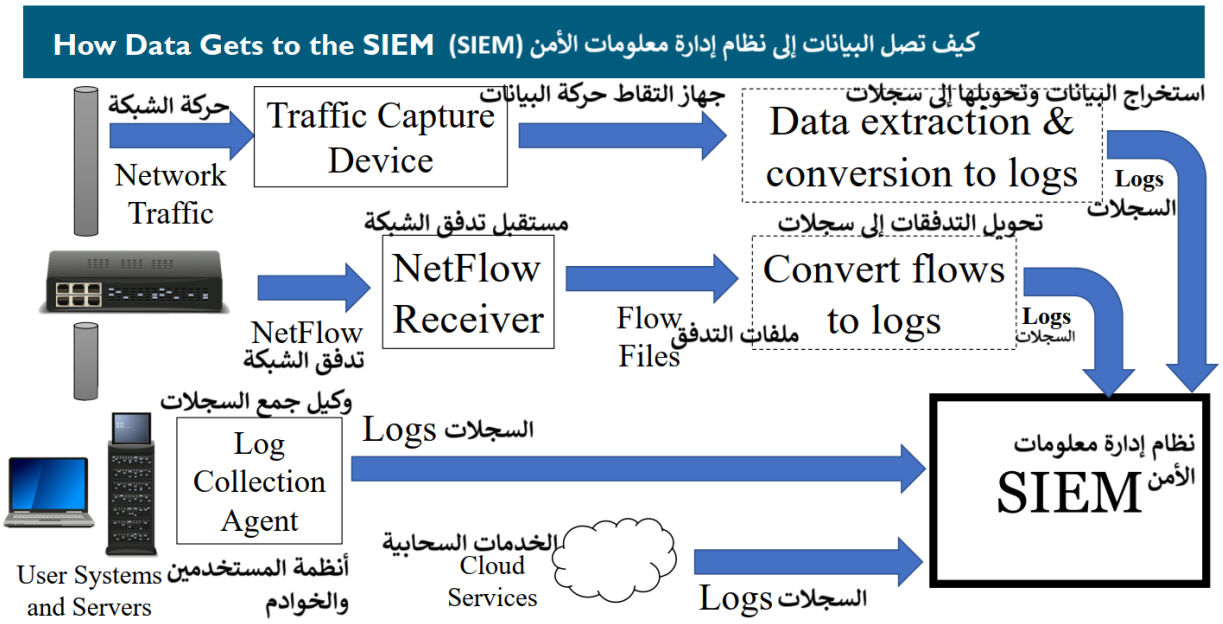
ما نريده



ما نريده

إذن، الوضع المثالي هو مركزية السجلات. يجب أن يتم توحيد معلومات مراقبة الشبكة (NSM) ومراقبة السحابة (CSM) بطريقة تتيح لك الوصول إليها جميعًا من خلال نظام إدارة المعلومات الأمنية والأحداث (SIEM). وبهذه الطريقة، إذا انطلق تنبيه بشأن عنوان IP خبيث على نظام كشف التسلل، يمكنك إجراء بحث واحد عن هذا العنوان عبر جميع مصادر البيانات في SIEM لمعرفة الأدوات الأخرى التي قد تحتوي على معلومات حوله. قد تكشف هذه العملية أن لديك سجلات بروكسي، وNetFlow، وتسجيلات PCAP كاملة، وضربة في صندوق تحليل البرمجيات الخبيثة، وكلها تظهر في وقت واحد. بدون مركزية السجلات، سيتعين عليك التحقق من كل مصدر بيانات على حدة، مما يزيد من الجهد وصعوبة التحقق.

كيف تصل البيانات إلى نظام إدارة معلومات الأمن (SIEM)



كيفية وصول البيانات إلى نظام إدارة المعلومات الأمنية والأحداث(SIEM)

يكمن سر النجاح في استخدام نظام SIEM في إدخال أكبر قدر ممكن من البيانات، من جميع الأنواع (البيانات الخاصة بالنقاط الطرفية وبيانات الشبكة). ومع ذلك، قد يمثل ذلك تحدياً، حيث إن أنظمة SIEMتتعامل في الغالب مع السجلات النصية فقط) مع دعم مباشر محدود لتدفقات NetFlow والتقاط الحركة على أساس المنتج .(يعرض هذا المخطط عملية إدخال بيانات الشبكة إلى نظام SIEM، الذي يتعامل بشكل رئيسي مع السجلات.

لاحظ أن بيانات الشبكة ليست بطبيعتها سجلات نصية ويجب تحويلها إلى سجل. على سبيل المثال، لا يمكن إدخال بيانات NetFlow و PCAPإلى العديد من أنظمة SIEM بصيغتها الأصلية؛ إذ يجب أن تمر بعملية تحويل وسيطة إلى نص يمكن لنظام SIEM تحليله وتخزينه. هناك أدوات، مثل Zeek مفتوح المصدر، يمكنها مراقبة حركة الشبكة الخام وتلخيص البيانات الوصفية حول تلك الحركة وإرسال السجلات الناتجة إلى نظام SIEM بسهولة، وهذا هو النهج الأمثل.

نريد البحث ليس فقط في سجلات النقاط الطرفية بل أيضًا في حركة الشبكة ضمن نظام .SIEM أما بالنسبة للسجلات النصية من النقاط الطرفية، فيكون من السهل عادةً نقل هذه السجلات إلى نظام SIEMمن خلال الالتقاط بواسطة وكيل (agent) وإرسالها إلى SIEM للتحليل (سنغطي هذه العملية بالتفصيل في الكتاب الثالث).

مرة أخرى، الهدف هو إدخال أي بيانات تنتجها أدوات الأمان في نظام SIEM ، حيث إن توفر المزيد من البيانات في مكان واحد يزيد من احتمالية اكتشاف الهجمات.

ملخص لمفاهيم الشبكة الدفاعية

تتطلب الشبكة الدفاعية ما يلي:

مراقبة بيانات الشبكة.

- مراقبة حركة المرور من وإلى الإنترنت وكذلك داخل الشبكة الداخلية.
- مراقبة حركة البيانات المتبادلة داخل الخدمات السحابية ومن وإلى الشبكات السحابية) مثل سجلات.(AWS VPC
- جمع بيانات الطبقة السابعة على الأقل للحركة الحرجة.

مراقبة بيانات النقاط الطرفية والتطبيقات.

- جمع السجلات الأساسية من أجهزة سطح المكتب، الخوادم، والأجهزة.
- مراقبة تكوينات الشبكة وقيمتها الأساسية وإدراج معلومات الثغرات الأمنية.
- سجلات الوصول والتدقيق من التطبيقات والخدمات السحابية.

ملخص مفاهيم الشبكة الدفاعية

يهدف هذا القسم إلى تقديم مفاهيم سيتم الرجوع إليها في بقية الدورة. للدفاع عن شبكة حديثة بفعالية، يجب أن تكون الأحداث في شبكاتك الداخلية والسحابية مرئية، ويجب أن تدعم التفاصيل الناتجة من مراقبة النقاط الطرفية هذه الجهود. يمكن تصور ذلك في قسمين:

- مراقبة أمن الشبكة لـ "البيانات أثناء الحركة" على الشبكة.
- مراقبة أمنية مستمرة لـ "البيانات الساكنة" التي تمثل المعلومات حول النشاط على النقاط الطرفية.

من الناحية المعمارية، نهتم بالمراقبة لفهم أنواع الحركة الموجودة على الشبكة وتنفيذ تدابير وقائية في مواقع استراتيجية للكشف عن أكبر قدر ممكن من الحركة الضارة وصدها، مما يسهل عملنا. بالطبع، لا يمكن صد جميع الحركة الضارة، لذلك تشكل أجهزة NSM الداخلية، وسجلات مزودي الخدمات السحابية (الشبكة والنقاط الطرفية)، وجمع سجلات النقاط الطرفية خطوة ثانية مهمة للبحث عن أي نشاط ضار قد تجاوز الدفاعات الخارجية.

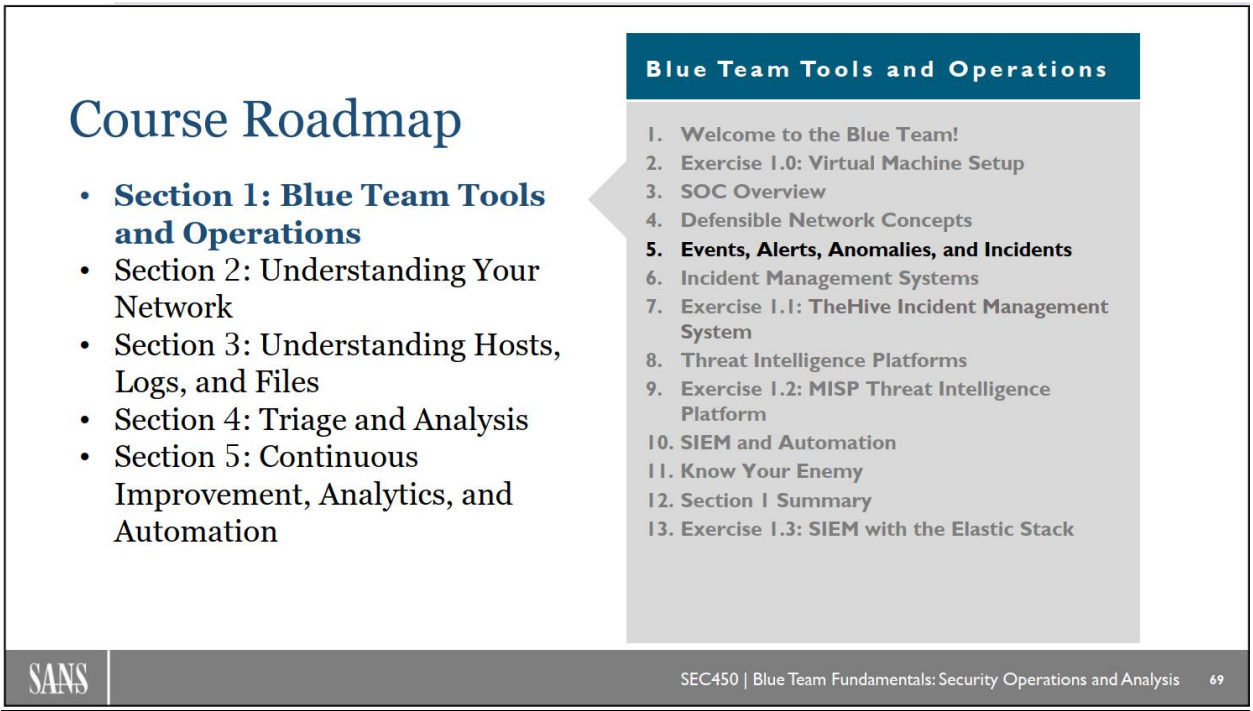
ملخص مركزية البيانات

تعد مركزية البيانات أمراً بالغ الأهمية، حيث تشمل الأمور التالية:

- ليس كل أداة تقوم بإنشاء السجلات أو مركزة البيانات بشكل تلقائي.
- في حال عدم مركزية البيانات، يجب استخدام أنظمة متعددة.
- استخدام أدوات متعددة يعد عملية معقدة ومعرضة للأخطاء وغير فعالة.
- تساعدنا وكلاء السجلات على جمع الملفات وتحويل التنسيقات الثنائية.
- تأخذ أنظمة SIEM السجلات كمدخلات، وتحول البيانات غير النصية!

ملخص مركزية البيانات

ينبغي أن يتم في النهاية مركزية بيانات المراقبة داخل نظام SIEM حيث يمكننا إجراء عمليات البحث، وإنشاء التصورات البيانية، وتطبيق قواعد الترابط، ومنطق التنبيهات بأعلى درجة من الدقة. يُعد عمل محلل عمليات الأمن في قراءة البيانات وتفسيرها مهمة أساسية، ونرغب في ضمان أن تكون البيانات متاحة بسهولة وتوفر أكبر قدر من السياق الممكن.



خريطة الدورة التدريبية

- **القسم الأول :أدوات وعمليات فريق الدفاع(Blue Team)**
- **القسم الثاني** :فهم الشبكة الخاصة بك
- **القسم الثالث** :فهم المضيفين، السجلات، والملفات
- **القسم الرابع** :التقييم والتحليل
- **القسم الخامس** :التحسين المستمر، التحليلات، والأتمتة

أدوات وعمليات فريق الدفاع(Blue Team)

1. مرحباً بك في فريق الدفاع!
2. التمرين 1.0: إعداد الآلة الافتراضية
3. نظرة عامة على مركز العمليات الأمنية(SOC)
4. مفاهيم الشبكة القابلة للدفاع
5. **الأحداث، التنبيهات، الشذوذ، والحوادث**
6. أنظمة إدارة الحوادث
7. التمرين 1.1: نظام إدارة الحوادثTheHive
8. منصات استخبارات التهديدات
9. التمرين 1.2: منصة استخبارات التهديداتMISP
10. إدارة الأمن والمعلومات (SIEM) والأتمتة
11. اعرف عدوك
12. ملخص القسم الأول

التمرين 1.3: إدارة الأمن والمعلومات باستخدام Elastic Stack

في هذه الوحدة:

تعريف الأحداث، التنبيهات، والحوادث.
تدفق سجلات الأحداث مقابل سجلات التنبيهات.
اعتبارات جمع الأحداث والتنبيهات.
الأهداف من فرز التنبيهات.
التنبيهات القائمة على التوقيع مقابل التنبيهات الشاذة.
وظيفة المحلل.

فهم أدواتك

في هذه الوحدة، سنبدأ باستكشاف تعريف الأحداث مقابل التنبيهات مقابل الحوادث، وكيفية دمج كل منها ضمن سير العمل كمحلل. سنتناول جمع الأحداث، والخيارات المتعددة للتنبيه، والاتجاهات والعمليات التي يجب أن تمر بها التنبيهات، وأخيرًا كيفية تكوين الحوادث. كما سنستعرض الفروق الدقيقة بين التنبيهات المستندة إلى الشذوذ والتنبيهات القائمة على "توقيع الشر".

الأحداث، التنبيهات، والحوادث

تعريفات:NIST SP800-61

الأحداث :أي وقوع يمكن ملاحظته في نظام أو شبكة.

التنبيهات :حدث ذو أهمية قد يكون غير مرغوب فيه أو غير مصرح به.

الحوادث :انتهاك أو تهديد وشيك بانتهاك سياسات الأمان الحاسوبية، أو سياسات الاستخدام المقبول، أو ممارسات الأمان القياسية.

الأحداث، التنبيهات، والحوادث

في البداية، يجب علينا مناقشة الفرق بين الأحداث، التنبيهات، والحوادث، حيث تعد هذه مفاهيم مهمة لفهم العمل داخل فريق عمليات الأمن. في مجال أمن المعلومات، تتمثل المهمة العامة في تسجيل الأحداث المتعلقة بالأمان التي تحدث على الأنظمة والشبكة، ووضع علامة على الأحداث المشبوهة كتنبيهات، وإذا تم تأكيد كونها ضارة، يتم التعامل معها كحوادث. التعريفات التي سنستخدمها في هذه الدورة للأحداث والحوادث تتماشى مع.NIST SP800-61.1

- **الأحداث** :أي وقوع يمكن ملاحظته في نظام أو شبكة. يمكن أن يكون هذا مثل تسجيل دخول مستخدم أو قيام شخص بفتح موقع إلكتروني.
- **التنبيهات** :حدث قد يكون غير مرغوب فيه أو غير مصرح به. مثال على ذلك هو تنبيه من نظام كشف التسلل يزعم أنه رصد حركة مرور لبرمجيات ضارة. لاحظ أن هذا غير مشمول في NIST 800-61 ولكنه سيكون مفيدًا للنقاش حول كيفية تفاعل أدوات الأمان. التنبيهات هي أحداث يتم اعتبارها مثيرة للاهتمام وفقًا لتعريف معين، بحيث ترغب في إعلام مركز عمليات الأمن بوقوع حدث.
- **الحوادث** :انتهاك أو تهديد وشيك بانتهاك سياسات الأمان الحاسوبية، أو سياسات الاستخدام المقبول، أو الممارسات الأمنية القياسية. عادةً تكون هذه الأحداث التي ستؤثر على سرية أو سلامة أو توافر بيانات العمل. بعبارة أخرى، حادث مؤكد. الأحداث التي تصبح تنبيهات يتم التحقق من صحتها كإيجابيات حقيقية تصبح حوادث.

بالمقارنة مع NIST ، تقدم مصادر أخرى مثل ITIL تعريفات مختلفة لهذه المصطلحات. سنستخدم التعريفات هنا كإرشادات. بشكل مختصر، تشكل كمية العناصر التي نراها وفقًا لهذه التعريفات كمرشح. جميع الوقائع التي يمكن ملاحظتها هي أحداث، وبعض تلك الأحداث المثيرة للاهتمام سيتم التنبيه عليها. يتم جمع التنبيهات) غالبًا في نظام (SIEM ويتم تصنيفها من قبل محلل يمكنه تأكيدها كحوادث. بمجرد تأكيد التنبيه كحادث، يتم معالجته في نظام إدارة الحوادث.

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

جمع الأحداث

غالبية السجلات التي يتم جمعها تندرج تحت تعريف الأحداث، أي أي حدوث يمكن ملاحظته.

```
Network connection detected:
UtcTime: 2018-09-23 16:16:16.054
ProcessId: 8012
Image: C:\Users\user1\AppData\Local\slack\app-3.3.1\slack.exe
User: win10\user1
Protocol: tcp
SourceIsIpv6: false
SourceIp: 10.150.159.161
SourceHostname: win10
SourcePort: 60201
SourcePortName:
DestinationIp: 52.85.81.133
DestinationHostname:
DestinationPort: 443
DestinationPortName: https
```

```
1335543155 315 127.0.0.1 TCP_MISS/301 -1 GET http://www.imdb.com/title/tt0056869 - NONE/- text/plain
```

```
117.201.11.139 - - [02/Jan/2017:02:35:54 -0800] "GET / HTTP/1.1" 200 34374 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1"
```

```
Feb 27 15:12:28 srv named[8978]: client 1.1.1.2#38595: query: https://allegro.pl IN A +E
```

```
Sep 23 08:54:56 ubuntu CRON[16355]: pam_unix(cron:session): session opened for user root by (uid=0)
```

ببساطة، هذه السجلات تخبرنا أن شيئًا ما حدث دون وجود دليل واضح على أنه أمر سيئ. على سبيل المثال، يمكن أن يكون حدثًا مثل زيارة شخص لموقع إلكتروني، أو تسجيل دخول شخص ما. في هذه الشريحة، توجد أمثلة على سجلات مثل: وكيل Squid، وسجل وصول خادم Apache، وطلب BIND DNS، ومصادقة Linux، واتصال شبكة Windows Sysmon. في معظم البيئات، تشكل هذه الأحداث غالبية البيانات التي يتم جمعها — سجلات توضح أن شخصًا ما قام بفعل معين دون أن يكون هناك شيء مثير للاهتمام في المحتوى ذاته.

يصبح السجل مثيرًا للاهتمام عند مركزيته ومعالجته بطريقة ما لمعرفة ما إذا كان يحتوي على أي معلومات مشبوهة. الأداة التي نستخدمها غالبًا لهذا الغرض هي نظام SIEM. يسمح لنا نظام SIEM بتحليل الأحداث وتطبيق معلومات استخبارات التهديدات، وربطها بسجلات أخرى، أو مطابقتها مع قائمة بعناوين IP أو نطاقات معروفة بأنها ضارة، مما قد يؤدي إلى ترقيتها إلى تنبيهات.

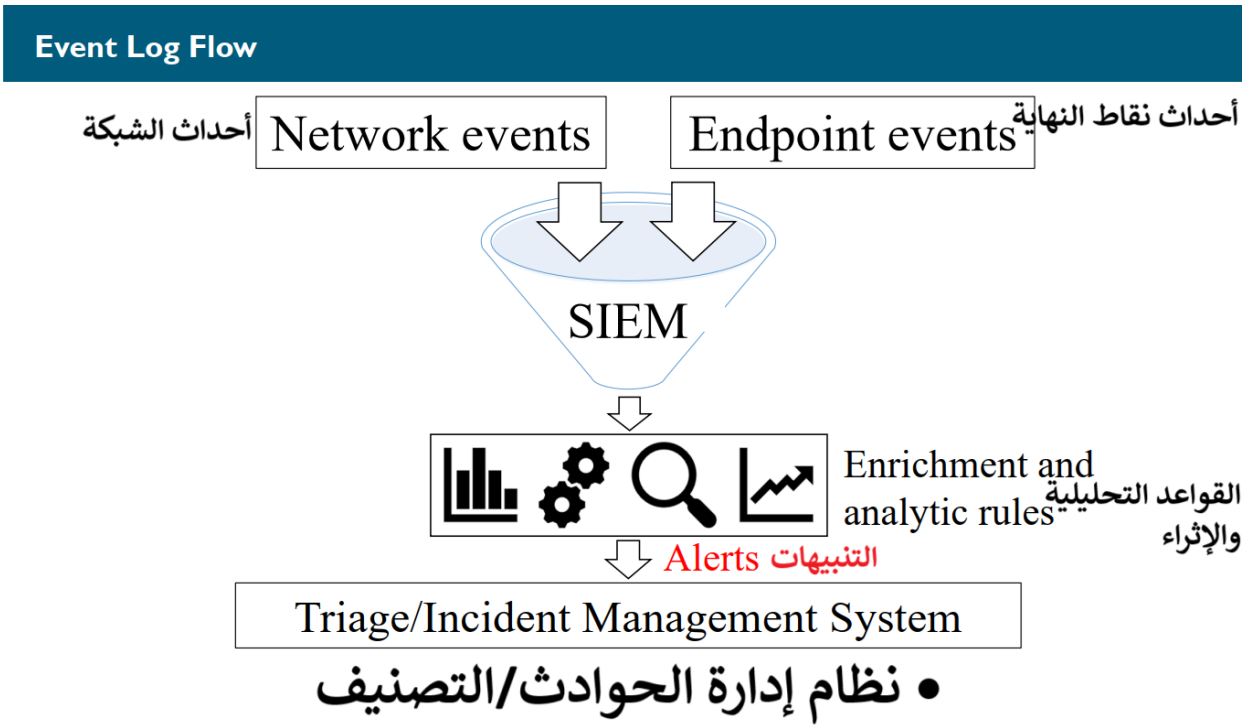
كم يجب أن أجمع؟

VS.

جمع الكثير من الأحداث يُعد مفيدًا للكشف... أو هل هو كذلك حقًا؟
قبل أن "تجمع كل شيء"، خذ في الاعتبار:
في معظم أنظمةSIEM ، يعني الحجم الأكبر = تكلفة أعلى.
البحث في المزيد من البيانات يستغرق وقتًا أطول.
العثور على الإشارات بين الضوضاء يكون أصعب وأبطأ وأكثر تكلفة إذا جمعت كل شيء.
الهدف :جمع السجلات ذات الصلة بالأمان.

كم يجب أن أجمع؟
في هذه المرحلة، من الجدير التطرق بإيجاز إلى موضوع جمع الأحداث. عندما يتعلق الأمر بجمع الأحداث في بيئتك للكشف عن الأنشطة الضارة، هل يجب عليك محاولة جمع كل شيء؟ ليس بالضرورة. إذ إن جمع الأحداث باستخدام الإعدادات الافتراضية من العديد من المصادر سيتضمن كمية كبيرة من الضوضاء التي لن تؤدي سوى إلى إبطاء نظامSIEM ، ورفع التكلفة، وتعقيد عملية العثور على "إبرة في كوم قش". لذا فكر في الأحداث التي تجمعها، وإذا وجدت أن بعض البيانات لا تقدم قيمة، فلا تتردد في استبعادها.
الهدف الذي يجب أن تتذكره هو أننا نرغب في جمع (وربما فقط جمع) السجلات ذات الصلة بالأمان. ما هي السجلات ذات الصلة بالأمان؟ هي أي سجلات تساعدك في اكتشاف مشكلة أمنية! ما هي السجلات التي يمكنها تحقيق ذلك هو موضوع سنتناوله لاحقًا في الدورة. حالياً، عليك أن تفهم أن معظم الفرق تجمع الكثير من البيانات غير الضرورية ولا تجمع ما يكفي من البيانات التي تحتاجها. هذا الهدف يتحرك باستمرار مع تطور الهجمات وقدرات التسجيل. للقيام بذلك بأفضل شكل، تحتاج إلى معرفة كيفية عمل السجلات، وما هو المتاح للجمع، وأنواع الهجمات التي قد تواجهها والأدلة التي تنتجها — وهي أمور مستمدة من معلومات استخبارات التهديدات. سنتناول كل هذه العناصر لاحقًا في الدورة أيضًا.
دورة "SEC555: SIEM with Tactical Analytics" للمدرب والمؤلف فيSANS ، جاستن هندرسون، هي مورد رائع لمن يرغب في إعداد SIEM بأكثر الطرق كفاءة ممكنة. الرسالة هنا هي أن جمع كل السجلات ليس بالضرورة الخيار الأفضل للكشف عن الأنشطة الضارة. يجب أن نسعى لأن نكون استراتيجيين في جمع الأحداث، مما يجعل تشغيل SIEM أسهل لجميع المشاركين.

تدفق سجلات الأحداث



تدفق سجلات الأحداث

يوضح الرسم التالي التدفق النموذجي لسجلات الأحداث في نظام مراقبة الأحداث. تحدث الأحداث على نقاط النهاية أو تُسجل بواسطة الأجهزة الشبكية، كما ناقشنا في القسم السابق، ثم تُحول إلى سجلات. تُجمع هذه السجلات وتُخزن في نظام SIEM عبر وسائل متعددة. يتميز SIEM بقدرته على التحليل الشامل، إثراء البيانات، وفحص السجلات، ويطبق مجموعة من القواعد التحليلية (الشروط للكشف عن الحالات ذات الأهمية) لإظهار أي أحداث قد تتطلب رد فعل.

بمجرد تحديد حدث يستدعي الاهتمام، يمكن رفع مستوى هذا السجل الفردي ليصبح تنبيهًا، ويُرسل عادةً مع أي معلومات إضافية ساعدت في التعرف عليه كاحتمال خبيث إلى قائمة الفحص، حيث يقوم المحلل بفحصه وربما إرساله إلى نظام إدارة الحوادث.

جمع التنبيهات

بعض السجلات تمثل تنبيهات!

12/12-06:22:52.879193 [**] [1:2014126:1] **ET CURRENT_EVENTS DRIVEBY Blackhole Likely Flash Exploit Request** /field.swf [**]
[**Classification: A Network Trojan was Detected**] [Priority: 1] {TCP}
192.168.45.10:1046 -> 78.46.173.138:80

Oct 30 09:50:48 1,2012/10/30 09:50:48,01606001116,**THREAT**,url,1,2012/04/10 04:38:23,192.168.0.2,204.232.231.46,0.0.0.0,0.0.0.0,rule1,crusher,,web-browsing,vsys1,trust,untrust,ethernet1/2,ethernet1/1,forwardAll,2012/04/10 04:38:24,12783,1,59024,80,0,0,0x200000,tcp,block-url,"**onlinebrandsecuritys.com/install/ws.zip**",(9999),**malware-sites**, informational,client-to-server, 0,0x0,192.168.0.0-192.168.255.255,United States,0

جمع التنبيهات

تذكر التفريق بين السجل وما يمثله هذا السجل. فبينما تمثل معظم السجلات أحداثًا، غالبًا ما تمثل السجلات المجمعة من الأجهزة الأمنية، مثل أنظمة كشف التسلل، تنبيهات. في هذا السياق، يظهر الصندوق العلوي تنبيهًا من سجلات Snort IDS يشير إلى مجموعة استغلال Blackhole، مما يُظهر أن الجهاز ذو عنوان IP 192.168.45.10 قد يكون قد تعرض للإصابة. أما السجل السفلي فهو من سجلات التهديد لجدار الحماية من Palo Alto ويشير إلى أن عنوان IP 192.168.0.2 قام بالاتصال بعنوان URL ضار معروف وهو "onlinebrandsecuritys.com" وقام بتنزيل ملف مضغوط مشبوه.

يتم إرسال كل من سجلات الأحداث والتنبيهات إلى نظام SIEM، ولكنها تختلف في أن سجلات التنبيه قد تطابقت بالفعل مع قائمة الأنشطة الخبيثة. وبالتالي، يجب التعامل مع هذه السجلات بشكل مختلف عن الأحداث العادية في SIEM، وهناك عدة طرق قد يختار مركز عمليات الأمن (SOC) اتباعها. هل يجب تصنيف هذه العناصر في وحدة التحكم الخاصة بنظام كشف التسلل قبل إرسالها إلى SIEM؟ أم ينبغي إرسال جميع سجلات التنبيه مباشرة إلى SIEM للتجميع المركزي؟ هل يجب إرسال سجل التنبيه مباشرة إلى نظام إدارة التذاكر لتفعيل الاستجابة؟ هناك العديد من الإجابات الصالحة لهذا القرار.

تصنيف التنبيهات

•مفاتيح نجاح التصنيف: الأولوية، السياق، والسرعة يتم إرسال التنبيهات التي تم إنشاؤها إلى واجهة واحدة (أو عدة واجهات) للتصنيف

	Count	rule.name	rule.uuid
	82,103	GPL ICMP_INFO PING Cisco Type.x	2100371
	30,613	ET JA3 Hash - Possible Malware - Various Trickbot/Kovter/Dridex	2028401
	15,673	ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC)	2021013
	13,785	ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)	2011540
	10,101	GPL SNMP public access udp	2101411
	9,319	ET HUNTING Suspicious HTTP Request to .bit domain	2018009
	9,059	ET HUNTING Suspicious GET To gate.php with no Referer	2030802
	9,059	ET INFO Suspicious Windows NT version 9 User-Agent	2015822

تصنيف التنبيهات

بشكل عام، يتم إرسال جميع التنبيهات التي يتم إنشاؤها إلى قائمة انتظار للتصنيف، كما يظهر في صورة وحدة التحكم الخاصة بـ Security Onion أعلاه. عادةً ما تعرض قوائم انتظار التصنيف قائمة بجميع التنبيهات التي تم تفعيلها مؤخرًا، وعدد مرات تفعيل كل تنبيه، ومصدر التنبيه، وتقييم درجة الخطورة، والمزيد. يجب أن تساعد قائمة انتظار التصنيف المعدة جيدًا في تسليط الضوء على أهم الأحداث للمحلل بحيث يمكنه العمل على الحالة ذات الأولوية القصوى في أي وقت. سنتناول كيفية تحسين أداء قائمة انتظار التصنيف لاحقًا في الدورة، ولكننا الآن نناقش تدفق البيانات فقط.

تختار بعض مراكز عمليات الأمن (SOC) تجميع جميع التنبيهات في قائمة انتظار واحدة، بينما يقرر آخرون إعداد عدة قوائم انتظار يجب العمل عليها بشكل مستقل.

[1] https://securityonionsolutions.com/software

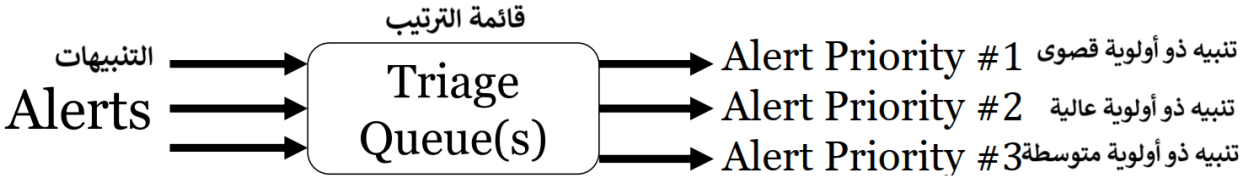
التصنيف الناجح

المدخلات: تنبيهات من جميع المصادر

المخرجات: تنبيهات مصنفة حسب الأولوية/الأعلى أهمية

الهدف:

- تسهيل التعرف على التنبيهات الأكثر أهمية أو الهجمات الأكثر خطورة (الأنظمة، البيانات، المستخدمون ذوو الأولوية العالية)
- إدارة حجم قائمة الانتظار



تنبيهات: هي إشعارات تحذيرية يتم توليدها عندما يتم اكتشاف نشاط مشبوه أو حدث قد يشير إلى وجود تهديد أمني.

تنبيه ذو أولوية قصوى: هذا النوع من التنبيهات يشير إلى تهديد خطير يتطلب إجراءً فوريًا لمنع حدوث أضرار جسيمة.

تنبيه ذو أولوية عالية: هذا النوع من التنبيهات يشير إلى تهديد محتمل يتطلب تحقيقا عاجلاً واتخاذ إجراءات وقائية.

تنبيه ذو أولوية متوسطة: هذا النوع من التنبيهات يشير إلى حدث غير عادي ولكنه قد لا يشكل تهديداً مباشراً. ومع ذلك، يستحق التحقيق والتقييم.

قائمة الترتيب: هي قائمة تحتوي على التنبيهات أو الأحداث الأمنية التي تتطلب تحليلاً وتصنيفاً. يتم ترتيب هذه الأحداث حسب الأهمية أو الأولوية لتحديد أيها يتطلب اهتماماً فورياً وأيها يمكن تأجيله.

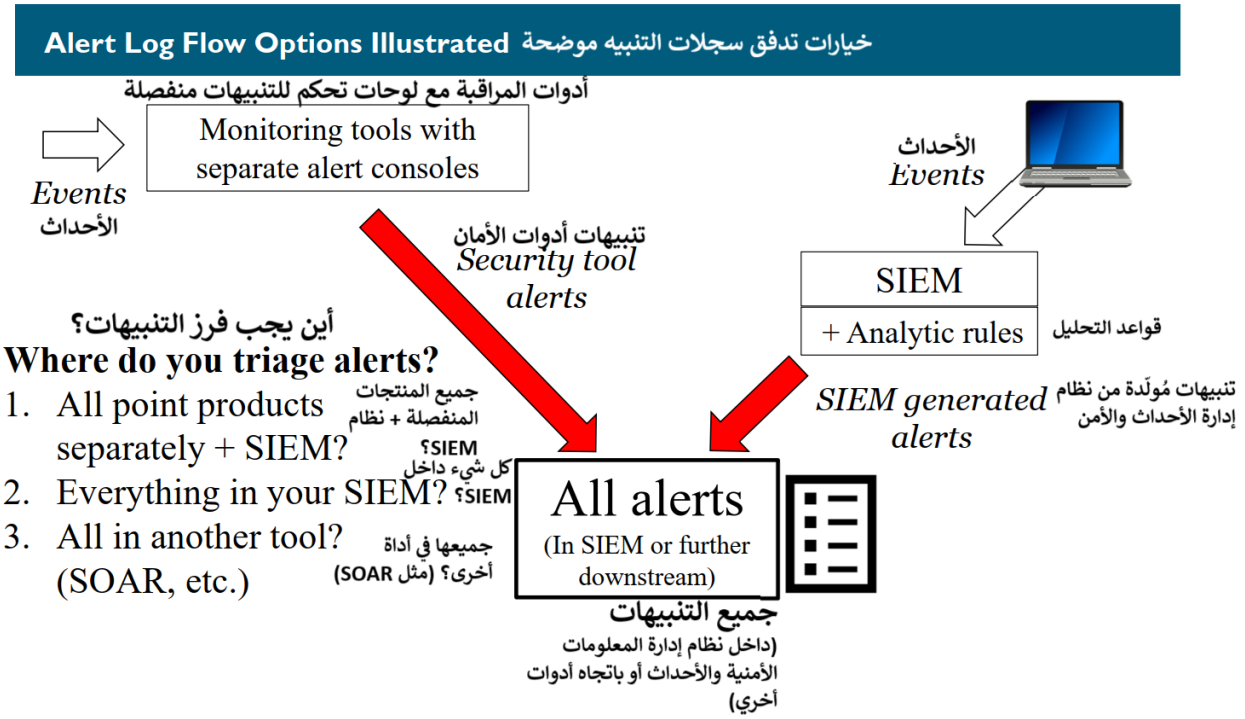
التصنيف الناجح

بمجرد أن تُصدر مرحلة الاكتشاف تنبيهات حول الأحداث ذات الصلة، يتم إرسال هذه التنبيهات جميعها إلى واحدة أو أكثر من قوائم الانتظار للتصنيف. وهنا يبدأ دور المحلل في مركز عمليات الأمن .(SOC) في هذه المرحلة، يجب على المحللين فرز النشاطات المحتملة الخبيثة واتخاذ قرار حكيم بشأن التنبيه الذي يبدو الأكثر إلحاحًا في الوقت الحالي. غالبًا ما تُتخذ هذه القرارات بناءً على عوامل مثل مدى تقدم الهجوم، مدى أهمية النظام المستهدف، صلاحيات الحساب الذي قد يكون تعرض للاختراق، وما إذا كان الهجوم يبدو فريدًا أو موجهًا بشكل خاص.

يجب أن تساعد الأدوات المحللين في تسهيل هذا الأمر. التجربة المثالية للتصنيف هي القدرة على النظر إلى قائمة الانتظار وتحديد الحالة التي تتطلب الاهتمام أولاً بشكل صحيح وسريع، ويكون ذلك عادةً بناءً على الهجمات التي تؤثر على الأصول، أو الحسابات، أو البيانات ذات الأولوية. يؤدي المحللون الفعّالون عملية التصنيف من خلال فهمهم لكيفية تطور الهجمات، وأين يمكن أن يحاول المهاجمون المناورة داخل بيئتهم الخاصة، والتكتيكات والتقنيات والإجراءات (TTPs) التي قد تُستخدم للهجوم. بمجرد أن تُحدد الأولويات، يتم اختيار التنبيه الأعلى للمتابعة والتحقق في المرحلة التالية.

سنتناول كيفية تحقيق النجاح في هذه المرحلة بمزيد من التفصيل في الكتاب الرابع، ولكن في الوقت الحالي، نضع الأهداف والتجربة المثالية للمحللين في التصنيف.

خيارات تدفق سجلات التنبيه موضحة



خيارات تدفق سجلات التنبيه موضحة

توضح هذه الشريحة نموذجًا لأماكن التنبيهات الشائعة حيث يتم إنشاؤها. يتمثل أحد الأماكن في أدوات مراقبة الأمان الفردية، مثل نظام كشف التسلل (IDS) أو حلول حماية نقطة النهاية (EDR). ولأن العديد من أدوات الأمان تقوم بإنشاء تنبيهاتها الخاصة مباشرةً، فإنها غالبًا ما تحتوي على لوحات تحكم خاصة بها وقوائم انتظار للتنبيهات حيث يمكن للمحللين تسجيل الدخول والتعامل مباشرة مع التنبيهات التي تم إنشاؤها بواسطة تلك الأدوات. وبالرغم من أنه يجب تسجيل هذه التنبيهات في نظام إدارة معلومات الأمان (SIEM) من أجل دمجها وتسجيلها لفترات طويلة، فإن ذلك يختلف عن المكان الفعلي الذي ينظر فيه المحللون إلى تلك التنبيهات ويقومون بفرزها.

لا تنس أن التنبيهات أيضًا يتم إنشاؤها في نظام SIEM. فعلى سبيل المثال، قد يقوم جهاز مكتبي يعمل بنظام Windows بتسجيل محاولات تسجيل دخول فاشلة متعددة. سيتم إرسال هذه الأحداث إلى SIEM، الذي سيتعرف على النمط المتكرر لمحاولات تسجيل الدخول الفاشلة ويقوم بإنشاء تنبيه. ستُجمع التنبيهات التي يولدها SIEM داخل النظام نفسه.

هذا يقودنا إلى السؤال الأساسي. هل يجب أن نقوم بجلب التنبيهات من أدوات كشف التسلل (IDS) إلى SIEM أو حتى أبعد من ذلك، ربما إلى منصة SOAR أو نظام إدارة الحوادث (ودمجها جميعًا في قائمة واحدة شاملة حيث يمكننا رؤية جميع التنبيهات من كافة الأجهزة في مكان واحد، أم يجب التعامل معها داخل أدواتها المنفصلة؟

خيارات تدفق سجلات التنبيه

خذ بعين الاعتبار الخيارات التالية:

1. فرز التنبيهات داخل لوحات تحكم المنتجات الأمنية الفردية.
2. فرز جميع التنبيهات في قائمة واحدة شاملة) داخل SIEM أو في أداة أخرى.(

حجة استخدام المنتجات الفردية :توفر أدوات الأمان عادةً واجهات أفضل لتحليل نوع التنبيهات الخاصة بها.

حجة استخدام قائمة شاملة:

- يوفر SIEM سياقًا شاملاً غير متاح في الأجهزة الفردية.
- العمل ضمن قائمة واحدة لتبسيط إدارة التنبيهات.

خيارات تدفق سجلات التنبيه

الحجة للخيار الأول –فرز التنبيهات داخل المنتجات الفردية يمكن أن يكون مفضلًا لأن هذه الأدوات غالبًا ما توفر واجهات وتدفقات عمل مصممة خصيصًا للتعامل مع البيانات التي تسجلها. على سبيل المثال، قد توفر التنبيهات من أدوات التقاط حزم البيانات (PCAP) إمكانية عرض محتوى الحزم واستخراج التفاصيل منها، وهو أمر قد لا يكون متاحًا في .SIEM العيب هنا هو أنه سيكون عليك التعامل مع عدة قوائم انتظار للتنبيهات، مما قد يصعّب العثور على أعلى الأولويات في الوقت المناسب.

الحجة للخيار الثاني –استخدام قائمة تنبيهات شاملة يعتبر خيارًا ذا فوائد كبيرة، وتفضله العديد من الفرق الأمنية. عندما يتم التعامل مع التنبيهات بهذه الطريقة، يوجد مكان واحد فقط لمراجعة التنبيهات وتحديد أولوياتها، مما يعد ميزة كبيرة. هناك أيضًا عامل مهم آخر، وهو توفير سياق إضافي من جميع مصادر البيانات ضمنSIEM ، وهذا غير متاح في المنتجات الفردية. يستطيع SIEMجمع المعلومات من عدة مصادر، مثل ما قدمه نظام كشف التسلل (IDS) وما سجلته الأحداث على نقطة النهاية، وتحويل كل هذه البيانات إلى تنبيه واحد عالي الدقة. دقة التنبيه تعد من الاعتبارات الأساسية لفريق الأمن، مما يدفع العديد لاختيار هذا المسار.

توجد فوائد إضافية إذا كانت هذه التنبيهات تُدفع إلى منصةSOAR ، حيث يمكنك أيضًا تشغيل إجراءات آلية على هذه التنبيهات. الجانب السلبي الصغير لهذه الطريقة هو نقص الواجهات المخصصة لتحليل أنواع معينة من التنبيهات، حيث قد لا يوفر SIEM نفس واجهة العرض التي تقدمها أدوات حماية نقطة النهاية(EDR) ، على سبيل المثال. يمكن تعويض هذا أحيانًا عن طريق الربط المباشر من واجهة SIEM إلى التنبيه في لوحة التحكم الخاصة بالأداة، مما يجعل الانتقال إليها سهلًا عند الحاجة.

نوعان من التنبيهات

تمييز مهم: "ما نوع التنبيه الذي أتعامل معه؟"

1. مطابقة توقيع لنشاط ضار معروف:
   - أمثلة: تحميل برمجيات خبيثة معروفة، اتصال بنطاق ضار، إلخ.
   - المعنى: "حدث شيء يبدو كأنه هجوم معروف"
   - الإجراء: التحقق مما إذا كان الكشف صحيحًا أو أنه إيجابي كاذب.
2. التنبيهات المبنية على الأنماط غير الاعتيادية:
   - أمثلة: تسجيل دخول مستخدم من جهاز أو موقع جديد، تسجيل دخول من مكان غير متوقع، استخدام بروتوكول غير عادي.
   - المعنى: "حدث أمر غير اعتيادي هنا، لكنه ليس بالضرورة ضارًا"
   - الإجراء: التحقيق - التحقق من الأنماط غير الاعتيادية وتحديد ما إذا كانت ضارة.

نوعان من التنبيهات: التنبيهات المعتمدة على التوقيعات والتنبؤ بالأنماط الشاذة

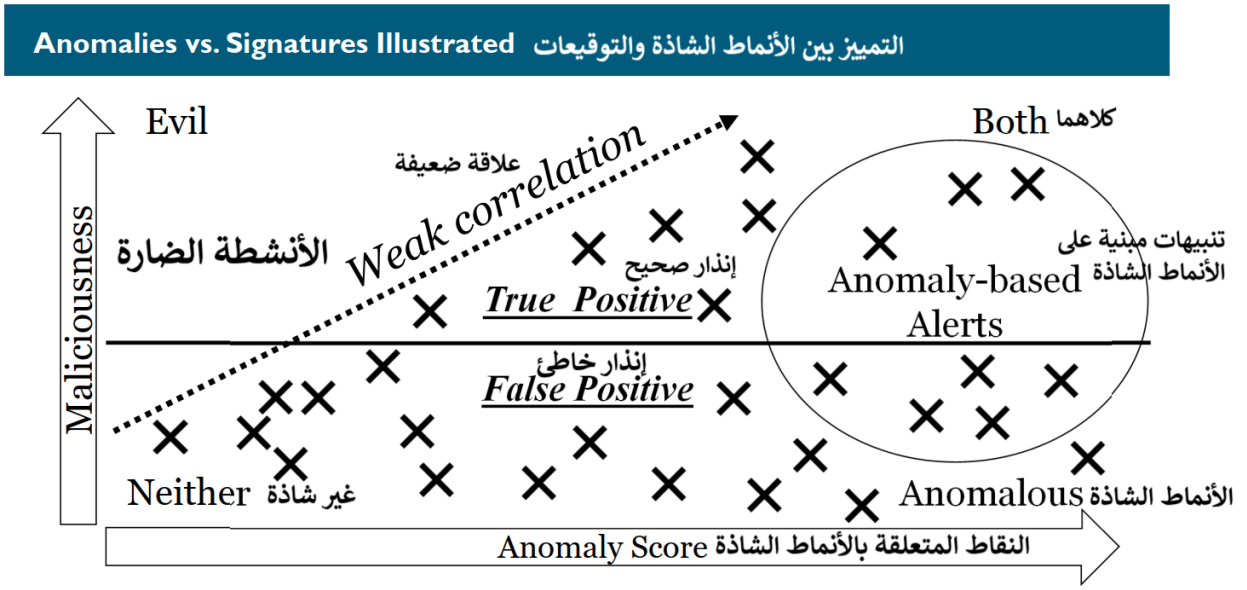
عند مراجعة تنبيه تريد التعامل معه، يمكن أن تبدأ بتصنيفه إلى نوعين رئيسيين - التوقيعات التي تحدد نشاطات ضارة معروفة، والتنبيهات المبنية على الأنماط غير الاعتيادية.

تنبيهات التوقيعات المعروفة تعتمد على التحقق من محتوى الترافيك، وعناوينURL ، وعناوينIP ، والملفات المرتبطة بالهجمات. الفكرة وراء هذه التنبيهات هي "إذا تم التعرف على العنصر بشكل صحيح، فهذا يعني أن هناك نشاطًا ضارًا بالتأكيد." تعتبر هذه الأنواع من القواعد عمومًا أكثر دقة وتنتج كشفًا عالي الموثوقية.

النوع الآخر من التنبيهات هو التنبيهات المبنية على الأنماط غير الاعتيادية. هذه التنبيهات لا تعتمد على قائمة بالمؤشرات المعروفة للأنشطة الضارة، بل تعتمد على الأنشطة غير المعتادة في البيئة. ما يعتبر غير اعتيادي يعتمد على معايير المؤسسة التي تنفذ القاعدة. غالبًا ما تتضمن هذه الأنشطة مثل نقل الملفات التنفيذية من مصدر غير متوقع، أو تحميل ملفات كبيرة، أو تسجيل دخول مستخدم من جهاز جديد لم يستخدمه من قبل، أو غيرها من الظروف المثيرة للاهتمام التي قد لا تكون بالضرورة ضارة.

يمكن أن تكون هذه القواعد "صحيحة" من ناحية أنها تميز بالفعل نمطًا غير اعتيادي، لكنها قد لا تكتشف هجومًا. كمحلل يتعامل مع هذه الأنواع من التنبيهات، عليك تنفيذ خطوتين: التحقق من أن التوقيع قد كشف بالفعل عن نمط غير اعتيادي، ثم تحديد ما إذا كان هذا النمط يمثل هجومًا. بناءً على نوع قواعد الأنماط التي قمت بتفعيلها ومدى تنظيم وتعريف بيئتك، من المرجح أن تجد أن هذه الأنواع من التنبيهات أكثر عرضة لإنتاج إنذارات كاذبة مقارنةً بالتنبيهات المعتمدة على "توقيع نشاط ضار معروف."

التمييز بين الأنماط الشاذة والتوقيعات



التمييز بين الأنماط الشاذة والتوقيعات

السبب في أن قواعد الكشف عن الأنماط الشاذة أكثر عرضة لإنتاج تنبيهات كاذبة يعود إلى الفرضية التي تستند عليها هذه القواعد. تحديدًا، يُعتقد أن الأحداث الشاذة تكون غالبًا ضارة أكثر من الأحداث غير الشاذة. رغم أنه من الممكن وجود نمط شاذ غير ضار، إلا أن كل نشاط ضار يجب أن يكون شاذًا بطريقة ما (وهذا هو سبب عدم وجود أي شيء في الجزء العلوي الأيسر من الرسم التوضيحي).

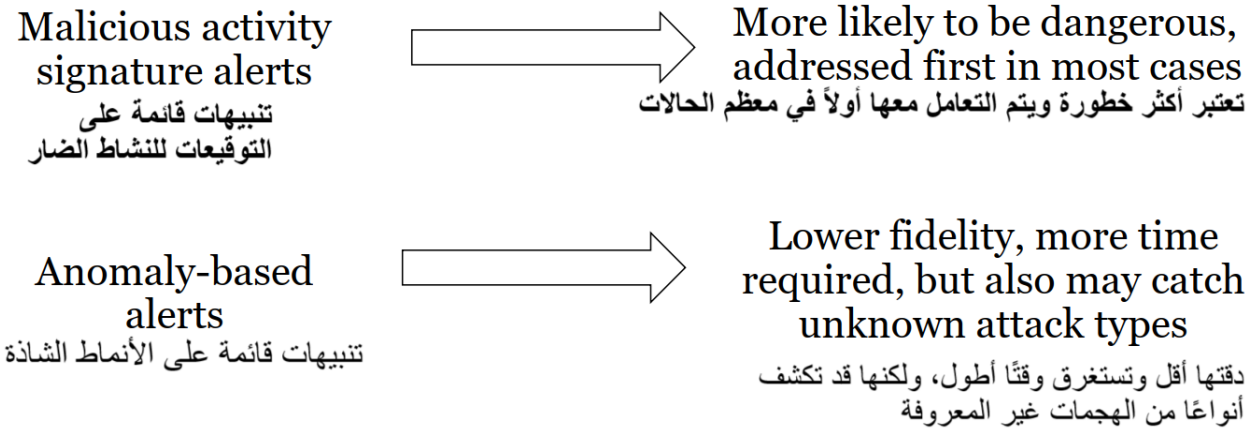
السؤال الأساسي هو ما إذا كان فريقك يمكنه تمييز الحدث كنمط شاذ أم لا، وقد يتطلب ذلك مصدر بيانات لا تقوم بجمعه حاليًا، على سبيل المثال. بناءً على هذه العلاقة، من الناحية الرياضية، يمكننا القول إن الأحداث الشاذة والضارة مرتبطة على الأقل بعلاقة ضعيفة، مما يعني أن استخدام الكشف عن الأنماط الشاذة يهدف إلى تقليل الضوضاء، مع الأمل في زيادة فرصنا لاكتشاف نشاط ضار وسط الكم الهائل من الأحداث التي تحدث في بيئتنا.

وبالتالي، على الرغم من أن التنبيهات المعتمدة على الأنماط الشاذة قد تنتج تنبيهات كاذبة، فإنها تبقى طريقة معقولة لمحاولة اكتشاف الهجمات، خاصة تلك التي لا تمتلك توقيعًا مباشرًا (مثل الهجمات الجديدة)، حيث قد يكون الدليل الوحيد المتاح هو نمط شاذ.

أفضل طريقة لتحسين دقة التنبيهات المعتمدة على الأنماط الشاذة هي إثراء بياناتها بسياق إضافي أو ربط النشاط بأحداث أخرى صادرة من نفس المضيف أو المستخدم. قد يظهر ذلك معلومات إضافية ترفع التنبيهات المعتمدة على الأنماط الشاذة إلى مستوى أعلى من الدقة في الكشف. سيتم التطرق إلى تفاصيل القيام بذلك بشكل أوسع في الدروس القادمة.

تصميم سير العمل حول نوعي التنبيهات

تـــــــذكير: أولويـــــــة الفـــــــرز لمعالجـــــــة العناصـــــــر الأكثـــــــر خطـــــــورة أولاً



تصميم سير العمل حول نوعي التنبيهات

التفريـق بـين نـوعي التنبيهـات يمكـن أن يسـاعدك فـي تحديـد كيفيـة تصـميم سـير العمـل المـرتبط بتوليـد كـل نـوع مـن التنبيهـات وتوجيـه كيفيـة فرزهـا. علـى سـبيل المثـال، إذا وجـدت أن التنبيهـات المعتمـدة علـى الأنمـاط الشـاذة تسـتنزف الكثيـر مـن وقـت المحللـين، يمكنـك اختيـار التركيـز علـى الأولويـات أولاً — أي علـى التنبيهـات التـي تعـرف بأنهـا ضـارة — وفصـل التنبيهـات الشـاذة ذات الدقـة المنخفضـة إلـى قائمـة مسـتقلة أو تجميعهـا والتعامـل معهـا بمجـرد بلـوغ حـد معـين مـن النشـاط. يمكـن أن يمنـع ذلـك تكـدس المحللـين بتلـك التنبيهـات ذات الدقـة المنخفضـة؛ وسـيتم مناقشـة تكتيكـات أخـرى مشـابهة فـي الكتـاب الخامس لاحقًا في الدورة.

التنبيهـات الشـاذة التـي تـم تعزيزهـا بشـكل كبيـر أو التـي يمكـن ربطهـا بأحـداث أخـرى قـد تقـع فـي نطـاق "الدقـة العاليـة". إذا تـم فصـل سـير العمـل بنـاءً علـى دقـة التنبيهـات، يمكـن إرسـال هـذه العناصـر عبـر مسار التنبيه العادي.

مناقشة: نظام كشف التسلل — (IDS) قائم على التوقيعات أم على الأنماط الشاذة؟

ضع في اعتبارك الأسماء التالية لبعض قواعد:Snort

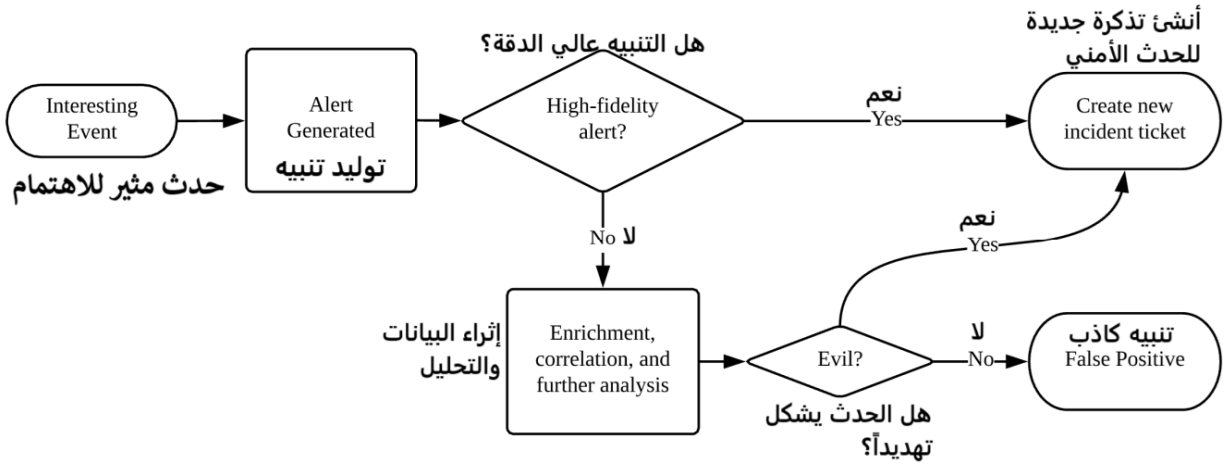
1. ET ET EXPLOIT Apache log4j RCE Attempt (http ldap) (CVE-2021-44228)
2. ET POLICY ZIPPED EXE in transit
3. ET POLICY Wget User Agent
4. ET PHISHING Potential ACH Transaction Phishing Attachment
5. ET JA3 Hash - Suspected Cobalt Strike Malleable C2
6. ET POLICY TLS/SSL Server Certificate Exchange on Unusual Port
7. ET MALWARE [TGI] Cobalt Strike Malleable C2 Response (O365 Profile)
8. ET CHAT IRC JOIN command
9. ET POLICY PDF File Containing JavaScript

مناقشة: نظام كشف التسلل — (IDS) قائم على التوقيعات أم على الأنماط الشاذة؟

فيما يلي بعض الأمثلة على القواعد التي قد يستخدمها نظام كشف التسلل لديك. بالنظر إلى القائمة فقط، ما هو التنبيه الذي تودّ الاستجابة له أولاً؟ وأيّ من هذه التنبيهات يبدو أنه يمثل تنبيهًا بتوقيع ضار معروف مقابل تعريف عن نمط شاذ؟ قد يكون من الصعب التمييز بين بعضها؛ والمشكلة الأولى تكمن في فهم معنى كل من هذه الأسماء، وقد تحتاج إلى البحث عن الأدوات أو الثغرات أو الظروف المرتبطة بها، ولماذا قد تكون ضارة.

بالنظر إلى العناصر الموجودة في الشريحة، فإن تنبيهات **POLICY** وتنبيه **IRC** تعتبر من الأنماط الشاذة (حتى وإن كانت بروتوكولات مثل **IRC** غير مرغوب بها في معظم المؤسسات، فإن التنبيه يشير فقط إلى "وجود اتصال عبر **IRC**"). أما جميع العناصر الأخرى فهي تمثل حالة ضارة معروفة. تشير قواعد **POLICY** في هذه المجموعة إلى نقل ملفات، واستخدام وكيل مستخدم خاص بأدوات سطر الأوامر، ومنافذ **TLS** غير قياسية، وملفات **PDF** تحتوي على **JavaScript**. لا تعدّ هذه العناصر بالضرورة ضارة، ولكنها قد ترتبط بأنواع معينة من الهجمات أو مراحلها. لفهم ما إذا كانت تلك النشاطات جزءًا من هجوم أم لا، سيتطلب الأمر التحقق من المستخدمين، والنظم، والبيانات المحددة المعنية. وكحال معظم التنبيهات القائمة على الأنماط الشاذة، لا يمكن تصنيفها بدقة عالية بشكل مستقل، ولكن يمكن بسهولة الوصول لذلك بإضافة القليل من السياق الإضافي.

التدفق العام للعملية



التدفق العام للعملية

إليك التدفق العام للعملية للمواضيع التي نوقشت في هذا القسم. الفكرة الأساسية هي أن بعض الأحداث ستؤدي إلى توليد تنبيهات. قد تكون هذه التنبيهات عالية الدقة، وفي بعض الحالات قد تكون ذات دقة عالية بما يكفي لتحويلها مباشرة إلى تذاكر حوادث. ومع ذلك، إذا لم تكن كذلك، كما في حالة القواعد القائمة على الأنماط الشاذة، فيجب استخدام سياق إضافي وربط البيانات للتحقق من مدى شرعية التنبيه. سيسهم ذلك في منع الإيجابيات الكاذبة من الوصول إلى مرحلة تتطلب المزيد من الجهد للتخلص منها.

إضافةً إلى ذلك، يُعد تتبع جميع التنبيهات التي تُطلق في نظام إدارة المعلومات والأحداث الأمنية (SIEM)أمرًا هامًا، حيث يمكن تحديد القواعد المفرطة النشاط وضبطها، وهي عملية ينبغي إجراؤها بشكل منتظم.

للحصول على مزيد من المعلومات حول التنبيهات والأنماط الشاذة، راجع الندوة التالية من تقديم **جاستن هندرسون وتيم غارسيا**.

https://www.sans.org/webcasts/high-fidelity-alerts-alert-anomaly-sibling-rivalry-107875

ملخص الأحداث والتنبيهات والحوادث

هدفك هو فهم:

- الفرق بين الأحداث، والتنبيهات، والحوادث
- تدفق التنبيهات بين الأدوات
- أنواع التنبيهات:
  - القائمة على التوقيعات/قوائم مؤشرات التهديد(IOC)
  - القائمة على الأنماط الشاذة
  - كيفية التعامل مع كل نوع
- كيف تساعد عملية الإثراء وربط البيانات في تقليل العمل غير الضروري
- إذا كانت التنبيه تشير إلى هجوم، أنشئ قضية وابدأ التحقيق!

ملخص الأحداث والتنبيهات والحوادث

يغطي هذا القسم الفروقات بين الأحداث، والتنبيهات، والحوادث، ويفصل بين الحوادث القائمة على الأنماط الشاذة وتلك القائمة على التوقيعات. مع هذه التعريفات وفهم تدفق الأحداث والتنبيهات، يمكننا الآن الانتقال إلى الأدوات التي ستدير هذه المعلومات والحوادث الناتجة عن تحليلها.

Course Roadmap

- **Section 1: Blue Team Tools and Operations**
- Section 2: Understanding Your Network
- Section 3: Understanding Hosts, Logs, and Files
- Section 4: Triage and Analysis
- Section 5: Continuous Improvement, Analytics, and Automation

Blue Team Tools and Operations

1. Welcome to the Blue Team!
2. Exercise 1.0: Virtual Machine Setup
3. SOC Overview
4. Defensible Network Concepts
5. Events, Alerts, Anomalies, and Incidents
6. **Incident Management Systems**
7. Exercise 1.1: TheHive Incident Management System
8. Threat Intelligence Platforms
9. Exercise 1.2: MISP Threat Intelligence Platform
10. SIEM and Automation
11. Know Your Enemy
12. Section 1 Summary
13. Exercise 1.3: SIEM with the Elastic Stack

خريطة الدورة التدريبية

- القسم الأول :أدوات وعمليات فريق الدفاع(Blue Team)
- **القسم الثاني** :فهم الشبكة الخاصة بك
- **القسم الثالث** :فهم المضيفين، السجلات، والملفات
- **القسم الرابع** :التقييم والتحليل
- **القسم الخامس** :التحسين المستمر، التحليلات، والأتمتة

أدوات وعمليات فريق الدفاع(Blue Team)

1. مرحباً بك في فريق الدفاع!
2. التمرين 1.0: إعداد الآلة الافتراضية
3. نظرة عامة على مركز العمليات الأمنية(SOC)
4. مفاهيم الشبكة القابلة للدفاع
5. الأحداث، التنبيهات، الشذوذ، والحوادث
6. أنظمة إدارة الحوادث
7. التمرين 1.1: نظام إدارة الحوادثTheHive
8. منصات استخبارات التهديدات
9. التمرين 1.2: منصة استخبارات التهديداتMISP
10. إدارة الأمن والمعلومات (SIEM) والأتمتة
11. اعرف عدوك
12. ملخص القسم الأول
13. التمرين 1.3: إدارة الأمن والمعلومات باستخدام Elastic Stack

تنظيم البيانات في مركز عمليات الأمن (SOC)

الحلول اللازمة لمجموعة عمليات الأمن الموحدة:

1- تنظيم وإدارة تنبيهات الحوادث وتتبع الحوادث النشطة.
2- جمع وتنسيق وتحديث استخبارات التهديدات.
3- إدارة بيانات السجلات، التصور، الارتباط، البحث، والتنبيه.
4- أتمتة إجراءات التحقيق.
5- مستودعات الأكواد.
6- تخزين البيانات غير المنظمة.

تنظيم البيانات في مركز عمليات الأمن (SOC)

يتطلب تشغيل مركز عمليات الأمن (SOC) قدرات ضخمة على تخزين وتنظيم البيانات. في الوحدات القادمة، سنستعرض المكونات الأساسية لتقنيات SOC المستخدمة في العمليات اليومية — نظام إدارة الحوادث، منصة استخبارات التهديدات، إدارة المعلومات الأمنية والأحداث (SIEM)، أدوات الأتمتة والتنسيق، وقواعد البيانات العامة. كل منها يلعب دورًا حاسمًا في عمليات الأمن، لذا فإن فهم استخداماتها ومدخلاتها ومخرجاتها يمثل أساسًا هامًا سنعتمد عليه في باقي الدورة.

الأدوات المستخدمة لتنظيم وبحث بيانات مركز عمليات الأمن(SOC)

نظام إدارة الحوادث(IMS)

- يُعرف أيضًا بمنصات الاستجابة لحوادث الأمن(SIRP)
- لتتبع التنبيهات، حالة الحوادث، والمؤشرات المرتبطة بها.

منصة استخبارات التهديدات(TIP)

- لتجميع مؤشرات التهديدات ومعلومات استخباراتية أعلى مستوى.

إدارة المعلومات الأمنية والأحداث(SIEM)

- لجمع السجلات، والفهرسة، والبحث، والارتباط والتنبيه.

تنسيق الأمن والأتمتة والاستجابة(SOAR)

- لأتمتة المهام الشائعة وتنسيق سير العمل.

قاعدة بيانات المعرفة ومستودعات الأكواد

- لتخزين جميع الوثائق/الأكواد، كتيبات العمل، ودراسات الحالة المتعلقة بمركز العمليات الأمنية.

الأدوات المستخدمة لتنظيم وبحث بيانات مركز عمليات الأمن(SOC)

بالنسبة لأدوات SOC والبيانات، لا تنتهي القصة عند الأدوات التي تقوم بالكشف. هناك مجموعة من التطبيقات الأخرى التي تعمل عادةً على تنظيم والتفاعل مع المعلومات التي يتم جمعها من أجهزة الأمان. أحد هذه الأدوات هو نظام إدارة الحوادث، حيث يتم التحقيق والعمل على جميع الحوادث المسجلة. غالبًا ما تشبه هذه الأنظمة أنظمة التذاكر المستخدمة في مكاتب الدعم، ولكن يجب أن تحتوي على تعديلات وميزات إضافية لتلبية احتياجات فرق الأمن.

أداة أخرى هي منصة استخبارات التهديدات .(TIP) عندما يتم العمل على الحوادث وجمع المعلومات حول الخصوم، يجب أن يكون هناك مكان منظم لوضع هذه البيانات بحيث يمكن حفظها واستخدامها عمليًا. ينبغي أن تحتوي هذه الأنظمة على معلومات تكتيكية منخفضة المستوى مثل مؤشرات الاختراق، وأيضًا معلومات استخباراتية استراتيجية أعلى حول ما يفعله الخصوم وكيف يفعلون ذلك ولماذا.

SIEMهو أداة لا تنتج أي بيانات مباشرة بنفسها، بل تقوم بتجميع جميع البيانات من مصادر أخرى. تجمع معلومات المستشعرات الشبكية وسجلات نقاط النهاية وتجعلها متاحة للبحث والتصور. يعتبر أفضل مصدر للمعلومات في العديد من البيئات نظرًا لقدرته على تقديم نظرة شاملة. وبسبب هذه القدرة، يضيف SIEM غالبًا قواعد تنبيه إضافية) إلى جانب تلك الموجودة في (IDS قد تطلق تنبيهات بناءً على محتوى السجلات التي يجمعها.

SOARهو إضافة جديدة نسبيًا ويُستخدم لمساعدة فرق الدفاع الأزرق في أتمتة وتنسيق إجراءات الاستجابة أو التحقيق بناءً على المدخلات من أدوات أخرى. على سبيل المثال، يمكن استخدام منصة SOARلأتمتة التحقيق في أي جهاز يتم اكتشافه إيجابياً بواسطة مكافحة الفيروسات. يمكن للأداة مراقبة سجلات مكافحة الفيروسات، تحديد الجهاز المعني، ثم تشغيل سلسلة من نصوص جمع البيانات والاختبار للتأكد من أن النظام في الحالة المتوقعة وغير مخترق. يمكنك رؤية سبب انتشار هذه الأدوات بسرعة، حيث أنها تتيح للمحللين التركيز على التحليل العميق بدلاً من جمع البيانات الروتينية والأتمتة.

قواعد البيانات المعرفية ومستودعات الأكواد تساعد مركز العمليات الأمنية في تتبع جميع البيانات التي لا تتناسب مع إحدى الفئات الأخرى. قد تتضمن هذه الوثائق العامة للموظفين الجدد، ودراسات الحالة، والنصوص البرمجية، أو أي معلومات أخرى ذات أهمية عامة لمركز العمليات الأمنية.

ملاحظة : من أجل النقاش، سنغطي جميع هذه الوظائف كما لو أنها مكونات برمجية منفصلة. في الواقع، العديد من بائعي SOAR و SIEM وغيرهم يجمعون عدة من هذه الوظائف، مثل إدارة الحوادث، في برنامج واحد.

أنظمة إدارة الحوادث(IMS)

خيارات برمجيات إدارة الحوادث:

1. حلول التذاكر التقليدية.
2. حلول مدمجة في أنظمة.SIEM
3. برمجيات مخصصة لإدارة الحوادث الأمنية.

- **الحلول التجارية :**تتوفر العديد من الخيارات، لذا يُنصح باختيار النظام بناءً على سير العمل المفضل والتكاملات والمتطلبات.
- **المصادر المفتوحة :**تتوفر خيارات أقل، لكنها جيدة للفرق ذات الميزانية المحدودة.

هذا قرار في غاية الأهمية –اختر بعناية!

- **يتطلب اختباراً شاملاً !**قم بوضع الحل محل الاختبار الجاد.
- لا تدع الإدارة تتأثر بالوعود المبالغ فيها من البائعين.

أنظمة إدارة الحوادث(IMS)

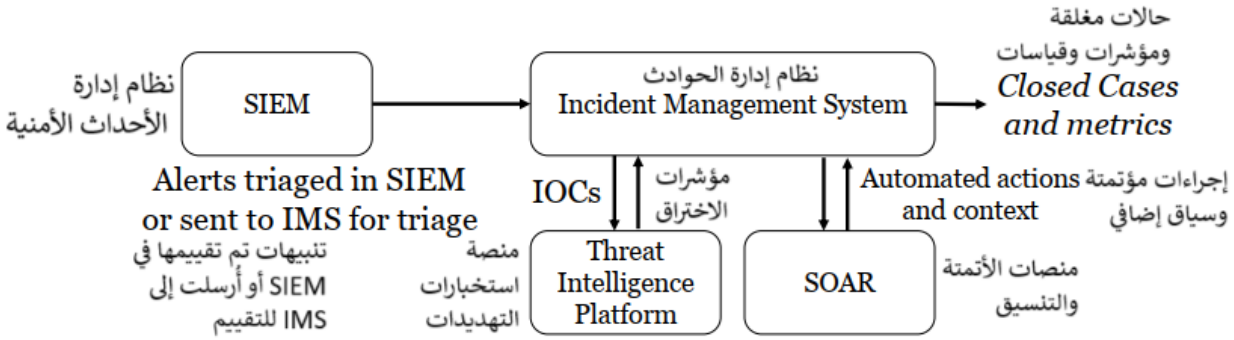
تُعد أنظمة إدارة الحوادث المكان الذي تسجل فيه فرق الدفاع الأزرق تحقيقاتها والإجراءات المتخذة عند وقوع حادثة. عادةً ما تحصل الفرق على الحلول من أحد المصادر الثلاثة: بائع يُقدم برمجيات تذاكر عامة مثل التي يستخدمها مكتب الدعم، نظام مدمج داخل أحد الأدوات مثلSIEM ، أو نظام تذاكر مخصص للأمن. تعتبر الأنظمة المخصصة للأمن غالباً الأفضل لأنها مصممة لتحقيق أهداف فريق الأمن. غالباً ما تحتوي هذه الأنظمة على جميع ميزات أنظمة التذاكر التقليدية، لكنها تتضمن ميزات إضافية مهمة للمتخصصين في الأمن، مثل القدرة على تسجيل مؤشرات الاختراق (IOCs) المرتبطة بالتحقيقات وتكاملها مع منصات استخبارات التهديدات.

إذا طرحت هذا السؤال على مجموعة من المتخصصين في أمن المعلومات، ستجد أن ردودهم حول أنظمة إدارة الحوادث ليست غالباً بحماس كبير. يجب أن تدرك أن هناك العديد من أنظمة التذاكر المتاحة، ولا يوجد نظام مثالي، لكن بعض الأنظمة تكون أفضل في مهام محددة ولديها واجهة استخدام أفضل من غيرها. من وجهة نظر الكاتب، يجب أن تكون واجهة النظام وتجربة الاستخدام العامة من أهم المعايير التي تضعها في الاعتبار عند الاختيار، حيث سيستخدم المحللون هذا النظام طوال اليوم وكل يوم، ويمكن أن يؤدي الاختيار السيئ في هذا المجال إلى سنوات من الألم والإحباط.

لا تفترض أن الخيارات التجارية ستكون بالضرورة أفضل من الأنظمة المجانية مفتوحة المصدر. هناك خيارات في كلا النوعين قد تكون ذات واجهات مؤلمة أو تفتقر إلى الميزات الضرورية، مما يؤثر سلباً على تجربة المحللين. لذا، من الضروري أن تخضع النظام لتجربة اختبار شاملة قبل اتخاذ القرار، حيث أن العديد من المشكلات لن تظهر حتى يتم وضع النظام في اختبار عملي.

نظم إدارة الحوادث – عرض النظام

- تستقبل IMS (نظام إدارة الحوادث) التنبيهات/الحوادث، وتُنشئ حالة في قائمة التذاكر.
- تُخصص الحالات للمحللين إما كحالات منفردة أو كخطوات فرعية ضمن كتيب العمل.
- يعمل المحلل على تنفيذ جميع المهام في كتيب العمل حتى الانتهاء، ثم يغلق الحالة.
- يربط العناصر القابلة للملاحظة بالحالات على مدى الوقت.



نظم إدارة الحوادث – عرض النظام

من خلال النظر إلى نظام إدارة الحوادث (IMS) كنظام مجرد، يتمثل المدخل في سجلات التنبيهات التي تأتي إما مباشرة من جهاز أمني أو من نظام SIEM. تحتوي هذه السجلات على عدة حقول تحتوي معلومات مفيدة تتعلق بالمشكلة المحتملة، وتكوّن هذه الحقول التفاصيل الأولية التي تُدرج في حالة أو تذكرة أو كيفما يُطلق عليها في النظام.

عند معالجة هذه الحالات، قد تتكامل نظم إدارة الحوادث مع أدوات أخرى مثل منصة استخبارات التهديدات (TIP) أو نظام تنسيق الأتمتة والاستجابة الأمنية (SOAR). يتيح هذا التكامل تخزين بيانات متعلقة بالتذكرة مثل أسماء النطاقات الضارة في منصة استخبارات التهديدات، كما تُستخدم في منصة SOARلإثراء المعلومات وجمع السياقات الإضافية.

عندما يدخل السجل إلى نظام إدارة الحوادث ويضاف إليه السياق إما يدويًا أو عبر منصةSOAR ، يستخدم المحللون النظام للعمل على الحالة، وإجراء التحليل، وتحديد ما إذا كان هناك حاجة للاستجابة للحادث. بمجرد التعامل مع الحادث وتوثيق جميع التفاصيل الخاصة بالإجراءات المتخذة، يُصبح المخرج من النظام مكتبة تحتوي على حالات مغلقة وتصنيفاتها والقياسات المرتبطة بها.

ميزات نظام إدارة الحوادث

- تختلف أنظمة إدارة الحوادث بشكل كبير
- سيكون هذا من أدواتك الرئيسية؛ لذا يجب أن تستمتع باستخدامه
- هناك بعض الميزات غير الواضحة ولكنها مهمة ومفيدة، تشمل:

○ قاعدة بيانات معرفية/ويكي مدمجة ○ تخصيص سير العمل ○ إمكانية الإغلاق والفتح والتعديل الجماعي ○ سير عمل قائم على الكتيب التشغيلي	○ تكامل الأتمتة ○ ملاحظات بنصوص منسقة ○ صور وجداول مدمجة ○ تكامل قاعدة بيانات المؤشرات ○ تنقل سريع باستخدام لوحة المفاتيح

ميزات نظام إدارة الحوادث

بعض الميزات التي قد لا تُعتبر في البداية مهمة لكنها تضيف فائدة كبيرة لأنظمة إدارة الحوادث هي تلك المذكورة أعلاه.

- **سير العمل القائم على الكتيب التشغيلي** يساعد في توجيه المحللين، خاصةً الجدد منهم، على مسار منظم لضمان تنفيذ جميع الخطوات الصحيحة بترتيب منطقي.
- **تكامل الأتمتة** (أو أن يكون جزءًا من منصة الأتمتة) يعدّ مهمًا لإنجاز الخطوات التي يمكن أتمتتها من كتيب العمل بشكل تلقائي.
- **النصوص المنسقة والصور والجداول** تجعل تدوين الملاحظات وقراءتها تجربة أفضل وأسهل مقارنةً بإدخال النصوص العادية. القدرة على تضمين لقطات الشاشة والنصوص البارزة باللون الأحمر يمكن أن تكون قيمة لمن يقرأ التحليل لاحقًا.
- **تكامل قاعدة بيانات المؤشرات/منصة استخبارات التهديدات** هو ميزة ضرورية. بدونها، قد يصبح ربط اسم مجال معين أو قيمة تجزئة مع تذكرة، أو ربطه برؤى سابقة، أمرًا معقدًا أو مستحيلًا.
- **التنقل السريع باستخدام لوحة المفاتيح** يعدّ أكثر كفاءة من استخدام الماوس. يجب أن يتمكن المحللون من ملء الحقول والانتقال بسرعة إلى الحقل التالي، واستخدام الماوس بأقل قدر ممكن عند إدخال المعلومات في النظام. قد يبدو ذلك أمرًا بسيطًا، ولكنه قد يكون موفرًا للوقت بشكل كبير.
- **قاعدة معرفية مدمجة** يمكن أن تكون ميزة مفيدة، مما يمنح المحللين إمكانية الوصول إلى المعلومات في المكان الذي يحتاجون فيه إليها في معظم الأوقات.
- **تخصيص سير العمل** يساعد الفرق في تكييف النظام ليتماشى مع الحالات والعمليات الخاصة بفريق مركز عمليات الأمن. يفضل أن يكون النظام قابلًا للتكييف مع العملية الخاصة بك، وليس العكس.
- **إجراءات الإغلاق/الفتح/التعديل الجماعي** تساعد في حالات فتح أو إغلاق عدة تذاكر مرة واحدة، أو عندما يكون هناك خطأ نتج عنه عدد كبير من التنبيهات. لا شيء أكثر إزعاجًا من الحاجة إلى إغلاق 100 تنبيه يدويًا بسبب قاعدة كتبت بطريقة سهلة الإثارة.

الكتب التشغيلية

- تختلف الكتب التشغيلية في تعريفها من مركز عمليات أمن المعلومات (SOC) إلى آخر.
- في هذا الدرس: "مجموعة من الإجراءات المتوقعة للاستجابة للتنبيهات."
- غالباً ما يتم تنفيذها من خلال نظام إدارة الحوادث (IMS) أو منصة التنسيق والأتمتة الأمنية (SOAR).
- تحتوي على خطوات إلزامية واختيارية للتحليل والإغلاق.
- ترشد المحللين نحو تحليل موحد وشامل.
- تكون فريدة لكل نوع من الحالات (مثل كتاب تشغيل للتصيّد الاحتيالي مقابل كتاب تشغيل للبرمجيات الضارة).

مثال على موجة رسائل إلكترونية ضارة تم استلامها

الكتب التشغيلية

كوسيلة لتحسين الكفاءة، تسعى العديد من مراكز عمليات الأمن إلى تحقيق اتساق في التحقيقات للحالات المتشابهة. لضمان إجراء تحليل كامل واستجابة متناسقة، يتم إعداد قوائم أو مسارات عمل يمكن تطبيقها على كل حالة من نفس النوع. يُطلق على هذه الخطوات غالباً مصطلح "الكتب التشغيلية" (وهذا هو الاستخدام في هذا الدرس، وقد تستخدم المصطلح بشكل مختلف). الفكرة هي أنه حتى إذا كان المحلل جديداً على الفريق أو على أمن المعلومات بشكل عام، فإن الكتب التشغيلية ستقوده إلى المسار اللازم، بغض النظر عما إذا كان بإمكانه إنتاج خطوات الاستجابة بنفسه أم لا. وبهذا، يتم تعزيز قدرات مركز العمليات الأمنية بأكمله وضمان أفضل استجابة ممكنة، بغض النظر عن الشخص الذي يتولى المسؤولية عن التذكرة.

تأتي الكتب التشغيلية بأشكال متنوعة ويجب أن تتماشى مع العناصر اللازمة للتحقيق الكامل في الحادثة. على سبيل المثال، خطوات كتاب تشغيلي بسيط للتعامل مع موجة رسائل إلكترونية ضارة معروضة على الشريحة. في بعض الحالات، قد لا تنطبق جميع خطوات الكتاب التشغيلي أو قد لا تكون ضرورية للوضع الحالي؛ ولذلك، يمكن تصنيف خطوات الكتاب التشغيلي على أنها اختيارية أو إلزامية. بمجرد اكتمال كل خطوة إلزامية، يمكن إغلاق الحالة داخل النظام. وبالتالي، بمجرد أن يعين المحلل نفسه حالة في نظام إدارة الحوادث، فإن هذا يترجم غالباً إلى تعيين مجموعة من الخطوات الجزئية التي تشكل الكتاب التشغيلي. يجب إتمام هذه الخطوات قبل إغلاق الحالة) ما لم يدعم الكتاب التشغيلي تعيين الخطوات الفردية لمحللين مختلفين – يدعم نظام TheHive ذلك.)

إطارات تصنيف الحوادث

فيه كذا خيار لتصنيف الحوادث. شوف معايا بعض الأمثلة:

1. **نظام VERIS**: ده اختصار لمصطلحات تسجيل الأحداث ومشاركة الحوادث
   - بيغطي 4 حاجات أساسية: الشخص اللي عمل، الإجراء اللي اتاخد، الأصل اللي اتأثر، وسمات الحادث (اتأثر إزاي).
   - بيتم جمع بيانات تقرير خرق البيانات السنوي (DBIR) بالشكل ده.
2. فئات نظام الإبلاغ عن الحوادث منUS-CERT
   - بيدي تفاصيل متوسطة.
   - بيحدد "إيه اللي حصل"، "إزاي حصل"، وتأثير الحادث.

إطارات تصنيف الحوادث

المقاييس تعتبر من أهم الحاجات اللي نظام التذاكر بتاعك ممكن يوفرها، علشان كده تصنيف الحوادث بييجي على أول قائمة متطلبات نظام إدارة الحوادث. لما نيجي نتكلم عن التصنيف، هنلاقي فيه كذا إطار مختلف، وكل واحد فيهم ليه مميزات وعيوب. في الآخر، اختيارك لإطار التصنيف هيعتمد على احتياجات شركتك والأسئلة اللي عايز تجاوب عليها بخصوص كل حادث.

أنظمة زي **VERIS**(تسجيل الأحداث ومشاركة الحوادث) بتدي تصنيف مفصّل جدًا يوضح وسيلة الوصول، الدوافع، وتأثير الحادث. أما الأطر الأبسط، زي إرشادات **US-CERT**للإبلاغ عن الحوادث، فبتسهّل التصنيف شوية، بس ممكن تفتقد لبعض التفاصيل.

الأطر البسيطة سهلة وسريعة في الاستخدام، لكن ممكن تخلي اكتشاف الأنماط أصعب لو في بيانات مهمة مش موجودة. الأطر الشاملة ممتازة علشان تجيب مقاييس قابلة للتنفيذ، بس ممكن تكون متعبة في استخدامها علشان فيها اختيارات كتير. فالأفضل يكون في "نهج وسطي" بين التفاصيل وسهولة الاستخدام.

نقطة أخيرة عن تصنيف الحوادث: استطلاعات الرأي بتقول إن كتير من المؤسسات بتحط نظام تصنيف خاص بيها أو بتستخدم النظام اللي موجود مع أدوات الأمان بتاعتها. وده تمام لو النظام بيخدمهم كويس (هنكلم عن أهداف التصنيف بعد شوية). مش لازم تستخدم إطار قياسي (مع إنه ممكن تستفيد منه)، بس خليك عارف إن لو عملت نظام تصنيف خاص بيك هيكون أصعب إنك تقارن نفسك بالمؤسسات التانية.

[1] VERIS: http://veriscommunity.net/

[2] US CERT: https://us-cert.cisa.gov/incident-notification-guidelines

إنشاء كتب تشغيل ناجحة

دليل لإنشاء كتب التشغيل:

1. التخطيط الدقيق:
   - فكر: ما الهدف الذي تحاول تحقيقه؟
   - ما هي الإجراءات التي ستوصلك إلى الهدف بأفضل وأسرع طريقة؟
2. اختيار الخطوات الأنسب وترتيبها:
   - لا تُفرط في تحديد الإجراءات لتجنب أن تصبح كتب التشغيل معقدة وغير قابلة للإدارة.
3. تحديد الخطوات الإلزامية والاختيارية.
4. تحويل هذه الخطوات إلى تدفق عمل (Workflow) داخل نظام إدارة الحوادث.(IMS)
5. التحديث المستمر بناءً على نجاح التنبيهات أو التحقيقات التي تستخدم هذه الكتب.

إنشاء كتب تشغيل ناجحة

تتناول هذه الفقرة نصائح لإنشاء واستخدام كتب التشغيل بنجاح داخل مركز عمليات الأمن.(SOC)

1. التخطيط الدقيق:
   - قبل البدء في كتابة الخطوات، خذ وقتك للتخطيط بشكل منهجي. قسّم المشكلة إلى أجزاء متعددة. اسأل نفسك: "بالنسبة لهذا النوع من القضايا، ما هي الإجراءات التي يمكنني اتخاذها؟."
   - أدوات مثل **ATC's RE&CT** https://github.com/atc-project/atc-react يمكن أن تكون مفيدة جدًا في هذه المرحلة.
2. تحديد أفضل الخيارات:
   - بعد العصف الذهني حول الخطوات المحتملة، استشر الفريق لتحديد أفضل الخيارات. الهدف ليس فقط إيجاد حل، بل الحل الأسرع والأكثر كفاءة لتحقيق نتيجة محددة.
   - حدد ترتيب الخطوات بعناية. على سبيل المثال، قد ترغب في تنفيذ خطوات الاحتواء السريعة قبل إجراء تحليلات البيانات المتعمقة.
   - كن دقيقًا بما يكفي لتوجيه الفريق في الاتجاه الصحيح، لكن تجنب إنشاء كتب تشغيل معقدة بشكل يجعلها غير قابلة للإدارة أو غير مناسبة للسيناريوهات الواقعية.
3. تصنيف الخطوات إلى إلزامية واختيارية:
   - حتى الخطوات الإلزامية قد لا تكون ضرورية دائمًا، لأن كل موقف يختلف عن الآخر. ومع ذلك، حاول تصنيفها لتشجيع أفضل الممارسات في جمع الأدلة والتحليل.
4. تنفيذ الخطوات في النظام:
   - بمجرد تحديد الخطوات، أدخلها في نظام إدارة الحوادث (IMS) أو منصة الاستجابة الأمنية والتنسيق الآلي .(SOAR) تُعتبر هذه الآن كتب تشغيل في مرحلة المسودة يمكن للفريق اختبارها.
5. اختبار كتب التشغيل وقياس أدائها:
   - استخدم كتب التشغيل عند ظهور مواقف تناسبها وقيّم أدائها.
   - ما مدى سرعة تنفيذ الخطوات؟ هل هناك خطوة واحدة تحتاج إلى تقسيمها لعدة خطوات؟ هل تم نسيان أي شيء؟
   - تعامل مع كتب التشغيل كمستندات ديناميكية تُحدّث باستمرار استنادًا إلى الأدوات والتهديدات. اسأل دائمًا: "كيف أعرف أن هذا الكتاب لا يزال يخدم الفريق بأفضل طريقة ممكنة؟".

أطر تصنيف الحوادث

هناك العديد من الخيارات لتصنيف الحوادث، ومنها:

1. **VERIS** (Vocabulary for Event Recording and Incident Sharing)
   - يركز على العناصر الأربعة:(4 A's)
     - الفاعل.(Actor)
     - الإجراء.(Action)
     - الأصول.(Asset)
     - السمات (Attributes - كيفية التأثير)
     - يتم جمع بيانات تقرير **DBIR** السنوي باستخدام هذا الإطار.
2. تصنيفات نظام الإبلاغ عن الحوادث التابع لـUS-CERT
   - يوفر مستوى متوسطًا من التفاصيل.
   - يحدد "ماذا حدث" و"كيف حدث" وتأثيره.

أطر تصنيف الحوادث

تُعدُّ المقاييس إحدى أهم المخرجات التي يمكن لنظام إدارة التذاكر إنتاجها، مما يجعل ميزات تصنيف الحوادث من بين الأولويات الأساسية لنظام إدارة الحوادث. عند الحديث عن التصنيف، هناك عدة أطر متاحة، ولكل منها نقاط قوة وضعف.

في النهاية، يعتمد اختيار إطار التصنيف على احتياجات المنظمة والأسئلة التي تحاول الإجابة عنها فيما يتعلق بكل حادثة. على سبيل المثال، يوفر نظام **VERIS** (Vocabulary for Event Recording and Incident Sharing) تصنيفًا عالي التفصيل يشرح طريقة الهجوم، الدوافع، وتأثير الحادثة. أما الأطر الأبسط، مثل إرشادات الإبلاغ عن الحوادث الخاصة بـ **US-CERT**، فإنها تجعل عملية التصنيف أسهل وأسرع لكنها تفتقر لبعض التفاصيل المهمة.

الأطر البسيطة تكون أسرع وأسهل في الاستخدام، لكنها قد تجعل من الصعب اكتشاف الأنماط إذا لم تُسجل بيانات ذات صلة. أما الأطر الشاملة فهي رائعة للحصول على مقاييس قابلة للتنفيذ، لكنها قد تعاني من ضعف في سهولة الاستخدام بسبب كثرة الخيارات المتاحة. غالبًا ما يكون التحدي في الأطر المفصلة هو ضمان التزام جميع أفراد الفريق بملء البيانات بطريقة متسقة، بالإضافة إلى إقناعهم بملء جميع العناصر المطلوبة لكل حادثة يعملون عليها. لهذا، فإن اتباع نهج "وسط" يجمع بين التفاصيل وسهولة الاستخدام يعد الخيار الأمثل.

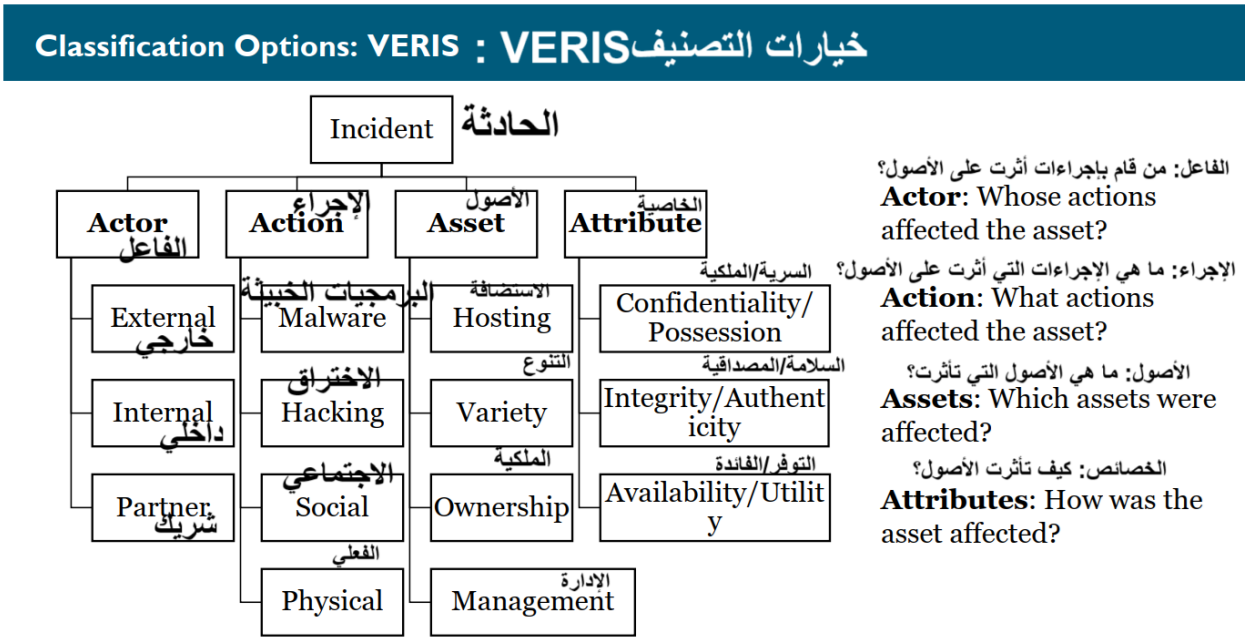
ملاحظة أخيرة حول تصنيف الحوادث:

تشير استطلاعات الرأي بين المتعلمين إلى أن العديد من المؤسسات تطور نظام تصنيف خاص بها أو تستخدم الأنظمة المدمجة في أدواتها الأمنية. وهذا أمر مقبول إذا كانت هذه الأنظمة تلبي احتياجات المنظمة. (سنناقش أهداف التصنيف قريبًا). لا يتعين عليك استخدام إطار معياري بالضرورة، رغم أن الاستلهام من الأطر المعيارية قد يكون مفيدًا. لكن عليك أن تدرك أن عيب عدم استخدام إطار معياري هو صعوبة مقارنة مؤشرات الأداء الخاصة بك مع مؤشرات المؤسسات الأخرى إذا قمت بتطوير نظام تصنيف خاص بك.

[1] VERIS: http://veriscommunity.net/

[2] US CERT: https://us-cert.cisa.gov/incident-notification-guidelines

خيارات التصنيف: VERIS



خيارات التصنيفVERIS :

نظـام VERIS هـو واحـد مـن أكتـر الأطـر شـمولية لتصـنيف الحـوادث اللـي موجـودة دلـوقتي. الشـريحة دي بتعـرض بعـض الفئـات الأساسـية اللـي ممكـن تتصـنف تحـت ال 4A's (Actor، Action، Asset، Attribute) جوا كل فئة من دول فيه اختيارات فرعية ممكن تستخدمها لو حابب.

يعنـي مـثلًا، تحـت "العمل/البرمجيـات الضـارة"(Malware) ، ممكـن تضـيف حاجـة زي "الوسـيلة" و"التنـوع" علشـان توضـح نـوع البرمجيـات الضـارة وطريقـة توصـيلها. تقـدر تلاقـي شـروحات أكتـر عـن هيكلية التصنيف دي على صفحة GitHub الخاصة بنظام VERIS.

لـو نـاوي تبنـي أو تطـور إطـار تصـنيف خـاص بيـك، نظـام VERIS يعتبـر مصـدر إلهـام ممتـاز، لأنـه شـامل جـدًا وقـد يعطيـك أفكـارًا لحاجـات ممكـن تتبعهـا أو قـوائم لاختيـارات تقـدر تحطهـا فـي الحقـول اللـي مكنـتش هتفكر فيها من غيره.

[1] http://veriscommunity.net

تصنيف الحوادث وفق نظامUS-CERT

يعتمد نظام تصنيف الحوادث التابع للحكومة الأمريكية على **نظام تقييم الحوادث السيبرانية الوطنية (NCISS)**المستند إلى قانون **FISMA**لعام 2014. يتم تعريف هذا النظام في الدليل **NIST SP800-61 Rev. 2**، ويستخدم المتوسط الحسابي المُوزَّن لإنشاء درجة تصنيف للحوادث تتراوح بين 0 و100.

تصنيفات بناءً على نظام النقاط NCISS (من 0 إلى 100) باستخدام فئات موزونة:

- **الأثر الوظيفي :**من "لا تأثير" إلى "تعطيل الخدمة/فقدان السيطرة DoS."
- **الأثر على المعلومات :**من "لا تأثير" إلى "تدمير نظام حيوي."
- **إمكانية الاسترداد :**من "استرداد عادي" إلى "غير قابل للاسترداد."
- وسائل الهجوم:
  - مواقع الويب، التصيد الاحتيالي، الوسائط الخارجية، انتحال الهوية، سوء الاستخدام، السرقة، وغيرها.
- سمات الحادث:
  - موقع النشاط الملحوظ: من "شبكة المحيط[1]" إلى "أنظمة السلامة."
  - تصنيف الجهات المهاجمة والتأثير المحتمل.

تصنيف الحوادث وفق نظامUS-CERT

يُعدُّ نظام **US-CERT**أحد الأساليب المستخدمة لتصنيف الحوادث، والذي طورته الحكومة الأمريكية لتلبية متطلبات قانون تحديث أمن المعلومات الفيدرالي لعام 2014 .(**FISMA**) يعتمد هذا النظام على إطار **NCISS**(نظام تقييم الحوادث السيبرانية الوطنية) الوارد في الإصدار الثاني من الدليل **NIST SP800-61 Rev. 2**.يتم حساب درجة الحادث باستخدام متوسط حسابي مُوزَّن يُنتج رقمًا بين 0 و100.

الفئات الرئيسية للنظام

يُقسِّم النظام الحوادث إلى عدة فئات، ولكل فئة وزن خاص بها يؤثر على التصنيف العام. تتضمن الفئات:

- التأثير الوظيفي:(Functional Impact)
  - من "لا تأثير" إلى "تعطيل الخدمة/فقدان التحكم DoS."
- النشاط المُلاحظ:(Observed Activity)
  - تحليل نشاط الهجوم بناءً على المصدر والكيفية.
- موقع النشاط المُلاحظ:(Location of Observed Activity)
  - من "شبكة المحيط" إلى "أنظمة الأمان والسلامة."
- تصنيف الفاعل:(Actor Characterization)
  - تحليل خصائص الجهة المهاجمة وتأثيرها المحتمل.
- تأثير المعلومات:(Information Impact)
  - من "لا تأثير" إلى "تدمير أنظمة حرجة."
- قابلية الاسترداد:(Recoverability)

---

[1] تشير"شبكة المحيط" أو "Perimeter network" إلى طبقة أمنية خارجية تحيط بالشبكة الداخلية لحماية النظام من التهديدات الخارجية. كلمة "محيطية" تعكس بشكل دقيق هذا الدور الحامي والحدودي. ومن أمثلتها الجدار الناري Firewall

- من "استرداد عادي" إلى "غير قابل للاسترداد."
- الاعتماد بين القطاعات:(Cross-Sector Dependency)
  - تحديد التأثير المحتمل على القطاعات الأخرى.
- التأثير المحتمل:(Potential Impact)
  - تقييم مدى الخطورة بناءً على البيانات والمعطيات المتاحة.

آلية الحساب والتصنيف

تُضرب إجابة كل فئة في وزنها الخاص، ويتم حساب النتيجة النهائية لتحديد أولوية الاستجابة للحادث، والتي يمكن أن تكون على مستويات:

- طارئة.(Emergency)
- شديدة.(Severe)
- عالية.(High)
- متوسطة.(Medium)
- منخفضة.(Low)
- أساسية.(Baseline)

ملاحظة:

قد لا تتوافق جميع الفئات أو الأوزان مع احتياجات المؤسسات التجارية بشكل كامل، ولكن يمكن تعديلها لإنشاء نظام مشابه يعتمد على نهج كمي. كما يمكن تجربة عرض تفاعلي للنظام عبر الرابط المشار إليه.

[1] https://us-cert.cisa.gov/CISA-National-Cyber-Incident-Scoring-System

[2] NCISS Scoring Demo: https://us-cert.cisa.gov/nciss/demo

نصائح لتصنيف الحوادث بنجاح

ابدأ بالتخطيط المسبق مع وضع النهاية في الحسبان – حدِّد الأسئلة والاتجاهات التي ترغب في تتبعها، ثم قم بتطوير مقاييس خاصة بها:

- ما الأرقام التي ستحتاجها للإجابة على تلك الأسئلة؟
- ما هو "الحد الأدنى" للإجراء بناءً على تلك الأرقام؟
- ما الإجراءات التي ستتخذها بناءً على هذه المقاييس؟

أمثلة على الأسئلة والمقاييس المهمة:

- **معرفة أساليب الهجوم الفعالة :**تتبّع مسارات التسليم الناجحة للهجمات.
- **تقييم عبء العمل :**راقب متوسط طول قوائم الانتظار أو عبء العمل على التذاكر.
- **تتبع محاولات التصيد :**سجّل عدد رسائل البريد الإلكتروني المبلغ عنها أو المحظورة وحوادث التصيد.
- **قياس وقت التواجد :**راقب متوسط الوقت اللازم للاعتراف بالحوادث أو احتوائها.
- **تقييم أداء فريق الأمان :**تتبع عدد الحوادث الحرجة وتأثيرها.

نصائح لتصنيف فعّال

الهدف من تصنيف المقاييس ليس مجرد جمع الأرقام، بل هو تحسين الأداء والاستعداد الأفضل للتعامل مع الحوادث المستقبلية. لذا، يجب أن يُركّز تصنيف الحوادث على ما يساعدك على فهم:

1. ما يعمل وما لا يعمل في آليات الهجوم.
2. ما هو فعال أو غير فعال كآلية دفاع.
3. أداء الفريق وفعاليته.

كيفية تحقيق ذلك؟

1. **ابدأ بالتخطيط مع وضع الأهداف النهائية في الحسبان :**فكر في الأسئلة التي ستحتاج إلى الإجابة عنها باستمرار لتحسين الأداء.
2. حول هذه الأسئلة إلى مقاييس قابلة للتتبع:
   - لا تجمع الأرقام بشكل عشوائي.
   - كل مقياس يتم تتبعه يجب أن يخدم غرضًا واضحًا.
3. تأكد من أهمية البيانات التي تجمعها:
   - هل يوجد "حد أدنى للإجراء" بناءً على هذه البيانات؟
   - هل تعرف ما هو "الوضع الطبيعي" لتحديد الحالات غير الطبيعية؟
   - ما الإجراء الذي ستتخذه إذا تجاوزت البيانات الحدود المسموح بها؟

أسئلة مثل هذه تساعد على ضمان جمع بيانات ذات قيمة وفائدة عملية.

نظام إدارة الحوادث TheHive [2]

نظام مفتوح المصدر رائع للتعلم ويُستخدم في هذه الدورة

- يتم تنظيم الحوادث وتعيينها باستخدام مفهوم "الحالة.(Case) "
- تتبع الحالات خطوات محددة مسبقًا في "قالب حالة (Case Template) "أو ما يُعرف بـ "كتاب الإرشادات.(Playbooks) "
- تحتوي الحالات على "مهام (Tasks) "يجب إنجازها (خطوات كتاب الإرشادات).
- تتضمن المهام "سجلات عمل (Worklogs) "لتوثيق الملاحظات المتعلقة بتنفيذ المهمة.
- يمكن ربط الحالات بـ"عناصر قابلة للرصد (Observables) "مثل مؤشرات الاختراق (IOCs).
- يتم إثراء العناصر القابلة للرصد من خلال "محللات (Analyzers) "مُفعّلة داخل محرك Cortex[3].

نظام إدارة الحوادث TheHive

باعتباره أداة تمثيلية لهذه الدورة، سنستخدم نظام إدارة الحوادث (IMS) المجاني مفتوح المصدر *TheHive*. سنلقي نظرة على كيفية عمله خلال الشرائح التالية. نحن ندرك أن العديد منكم قد لا يستخدم *TheHive* في أماكن عملكم (على الرغم من أنه مستخدم في العديد من المؤسسات). لذلك، أثناء وصفنا لتدفق العمل والمصطلحات والميزات هنا، حاول أن تربطها بنظام إدارة الحوادث الذي تستخدمه. الهدف هنا هو مقارنة الأنظمة المختلفة وتوسيع منظورك كأنظمة تحليلية لفهم تدفقات العمل المحتملة.

يشبه *TheHive* معظم أنظمة إدارة الحوادث الموجهة نحو الأمن السيبراني في أنه يدعم:

- **إدخال التنبيهات :**استقبال التنبيهات من أنظمة المراقبة.
- **إنشاء الحالات :**إنشاء حالات لمعالجة الحوادث.
- **كتب الإرشادات :(Playbooks)** تُعرف باسم "قوالب الحالات (Case Templates) "داخل النظام.
- **المهام :**تُنشأ داخل كتب الإرشادات، ولكل مهمة سجلات عمل خاصة لتوثيق الملاحظات.
- **المؤشرات المرتبطة بالحالة :**يتم تخزينها ضمن "عناصر قابلة للرصد.(Observables) "

يمكن لهذه العناصر القابلة للرصد أن تُرسل تلقائيًا إلى منصات استخبارات التهديدات، أو تُثْرى باستخدام قطعة برمجية مكمِّلة تُعرف بمحرك *Cortex*.

التدفق الرئيسي للعمل

يقوم المحللون بالتقاط الحالات المليئة بالمهام، وعند إكمال جميع المهام، تُغلق الحالة، وينتقل المحلل إلى العنصر التالي.

[1] https://thehive-project.org/

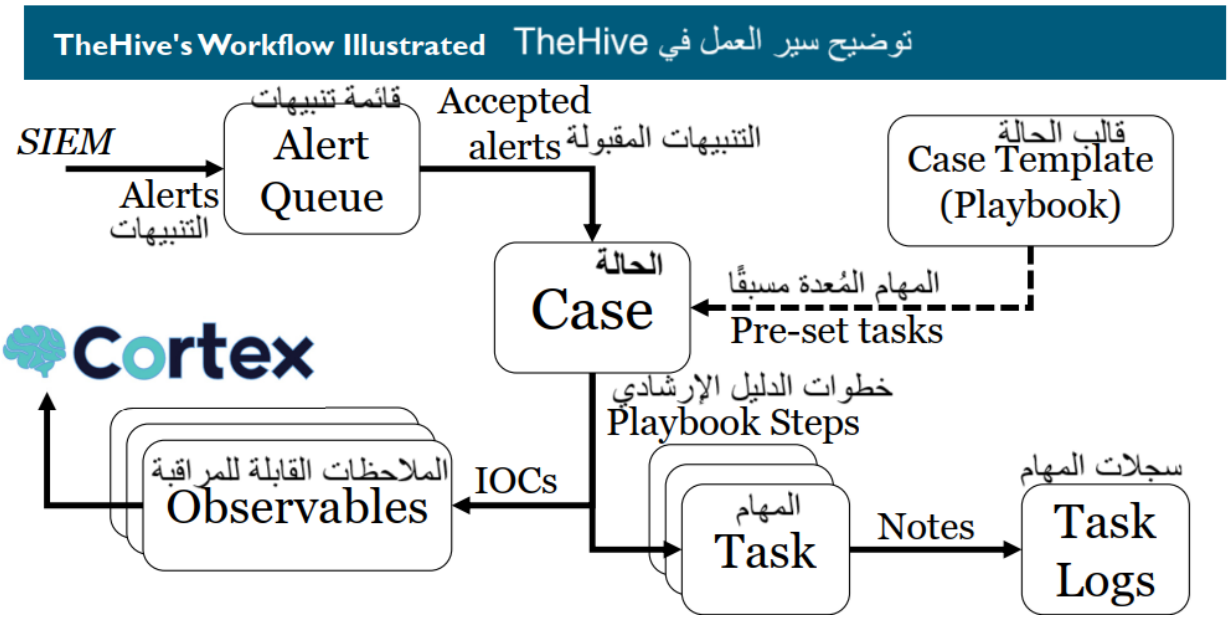
---

[2] TheHiveهي منصة مفتوحة المصدر مصممة خصيصًا لإدارة حوادث الأمن السيبراني بشكل فعال. تعمل كمركز تحكم واحد يتيح لفريق الأمن جمع وتحليل وربط جميع البيانات المتعلقة بالحوادث الأمنية، مما يسهل عملية التحقيق والاستجابة.

[3] محرك Cortex هو قلب نظامSOC ، حيث يقوم بجمع وتحليل كميات هائلة من البيانات من مختلف مصادر المؤسسة، مما يمكّن فريق الأمن من اكتشاف التهديدات المحتملة واتخاذ إجراءات وقائية بشكل فوري وفعال .

تعتمد فعالية نظام SOC بشكل كبير على قوة محرك Cortex في الكشف عن الأنماط الشاذة وتحليل السلوك، مما يساهم في تحسين استجابة فريق الأمن للأحداث الأمنية و تقليل وقت الاكتشاف والاستجابة.

توضيح تدفق العمل في TheHive[4]



توضيح تدفق العمل في TheHive

تعرض هذه الشريحة توضيحًا للكيانات المستخدمة في نظام *TheHive* وكيفية ارتباطها ببعضها البعض. في الأعلى، يقوم نظام إدارة الأحداث الأمنية (*SIEM*) بإرسال التنبيهات إلى قائمة التنبيهات في *TheHive*. يمكن التعامل مع هذه التنبيهات بطريقتين: إما رفضها باعتبارها نتائج إيجابية خاطئة، أو قبولها كحالة.(*Case*)

آلية العمل:

1. الحالات والقوالب:
   - كل حالة يمكن أن تحتوي على مهام مستمدة من قالب حالة تم إنشاؤه مسبقًا (فكر في قالب الحالة كدليل إرشادي أو *Playbook*.)
   - تتكون المهام من خطوات يجب إنجازها لإغلاق الحالة.
2. العناصر القابلة للرصد:(*Observables*)
   - يمكن إضافة عناصر مثل عناوينIP ، أسماء المستخدمين، أسماء الأجهزة، الروابط (*URLs*)، أو القيم المشفرة (*Hashes*) إلى الحالة.
   - يعمل محرك *Cortex*(محرك أتمتة تكميلي) على تطبيق مجموعة من المحللات (*Analyzers*)على هذه العناصر، مما يثري البيانات ويوفر معلومات إضافية تساعد المحلل على فهم سياق العناصر المدخلة.
3. الاستجابات الآلية:(*Responders*)
   - يمكن إنشاء إجراءات آلية بناءً على البيانات الموجودة في التذكرة.(*Ticket*)
   - تتضمن هذه الإجراءات إرسال رسائل بريد إلكتروني أو بدء مهام جمع البيانات والاستجابة.

---

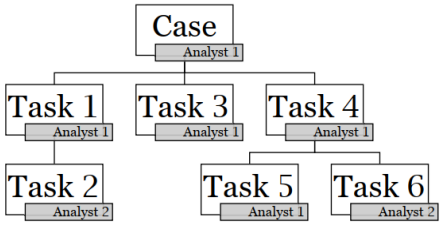
[4] TheHive هي منصة مفتوحة المصدر مصممة خصيصًا لإدارة حوادث الأمن السيبراني بشكل فعال. تعمل كمركز تحكم واحد يتيح لفريق الأمن جمع وتحليل وربط جميع البيانات المتعلقة بالحوادث الأمنية، مما يسهل عملية التحقيق والاستجابة.

ميزة Cortex في الأتمتة:

- مـــن خـــلال اســـتخدام المحلـــلات (*Analyzers*) والمســـتجيبين(*Responders*) ، يجعـــل *TheHive* البيانات والسياق متاحين بنقرة زر واحدة.
- يعمل *Cortex*كمنصة أتمتة تساعد المحللين على تحسين كفاءة العمل وتوفير الوقت.

تعيين الحالات والمهام TheHive:

تتيح منصة *TheHive* تعيين كل من الحالات (*Cases*) والمهام (*Tasks*) إلى المحللين بشكل منفصل، مما يوفر درجة عالية من التخصيص لا تتمتع بها جميع أنظمة إدارة الحوادث.(*IMSs*)



مزايا التعيين التفصيلي:

التخصيص الدقيق:

- يسمح بتعيين أجزاء صغيرة من الحالة، مما يمكن أكثر من شخص من العمل على نفس الحادث في وقت واحد.
- في بعض الأنظمة الأخرى، يتم تعيين الحالات فقط ككيان كامل، مما يعني أن المحلل الذي يبدأ الحالة يجب أن يُكملها بالكامل. إذا واجه المحلل صعوبة في تنفيذ خطوة معينة، قد يتعطل التقدم.

تشغيل فرق SOC بلا طبقات:

- يمكن أن تتكيف هذه الميزة بسهولة مع مراكز عمليات الأمن (SOC) التي لا تعتمد على هيكل هرمي أو طبقات.
- يُمكن للمحللين الجدد التعامل مع المهام الأسهل بينما يتولى المحللون الأكثر خبرة المهام المعقدة.
- على سبيل المثال:
- المحلل الجديد (#1) يتعامل مع المهام الأبسط.
- المحلل الخبير (#2) يُكمل الخطوات الأكثر تعقيدًا مثل تحليل البرمجيات الخبيثة أو تحليل الذاكرة.
- يمكن للمحلل الجديد مراجعة سجلات العمل (*Worklogs*) الخاصة بالمحلل الخبير، مما يُمكّنه من التعلم مع مرور الوقت.

تحقيق توازن أفضل في عبء العمل:

- تُسهّل هذه المرونة توزيع المهام بشكل متوازن بين أعضاء الفريق.

تيسير تسليم المهام بين النوبات:

- مع القدرة على تعيين المهام الفردية، يصبح تسليم الحالات بين النوبات أكثر سلاسة، حيث يمكن للمحللين الجدد استكمال المهام بناءً على ما تم تسجيله في سجلات العمل.

فوائد العمل الموازي:

- يمكن لمحللين مختلفين العمل على تذكرة واحدة في نفس الوقت دون تعارض.
- عند الانتهاء من المهمة، يمكن للمحلل الأصلي مراجعة سجلات العمل الخاصة بالمهام التي أنجزها الآخرون.
- هذا النهج لا يُنجز المهمة فحسب، بل يُصبح أيضًا دليلًا تعليميًا يوضح كيفية تنفيذ هذه الخطوات في المستقبل.

مثال لقالب حالة TheHive:


Case # 6 - [Phishing Wave - attachments] Phishing wave reported - "Invoice #4251 - OVERDUE"

Group	Task	Date	Assignee	Actions
Recon	Are the users who received the email related in any way?		Analyst1	Start
Delivery	Check how many emails are delivered organization wide		Analyst1	Start
Delivery	Identify source email addresses and IPs		Analyst1	Start
Exploit	What exploit does the file use?		Analyst2	Start
Install	What happens if the attachment is opened?		Analyst2	Start
C2	What domains/IPs are used for command and control?		Analyst2	Start
Resposne	Block email address of sender		Analyst1	Start

مثال لقالب حالة TheHive:

يوضح هذا المثال شكل تبويب المهام داخل حالة تم إنشاؤها حديثًا. تم تعبئة قائمة المهام مسبقًا باستخدام قالب حالة يُدعى *"Phishing Wave – attachments"*، وهو محدد باسم الحالة باستخدام بادئة خاصة.

تفاصيل قالب الحالة:

- الغرض من القالب:
  - صُمم هذا القالب ليعكس الأسئلة التحقيقية الشائعة والإجراءات الاستجابية التي ينبغي اتخاذها في أي حالة تتضمن حملة تصيد احتيالي تحتوي على ملف خبيث.
  - يسهم ذلك في ضمان وجود هيكل منظم للتحقيق والاستجابة.
- تصنيف المهام حسب مراحل سلسلة القتل الإلكتروني:(Cyber Kill Chain)
  - تُقسم المهام إلى مجموعات مهام تمثل المراحل المختلفة من سلسلة القتل الإلكتروني، مثل:

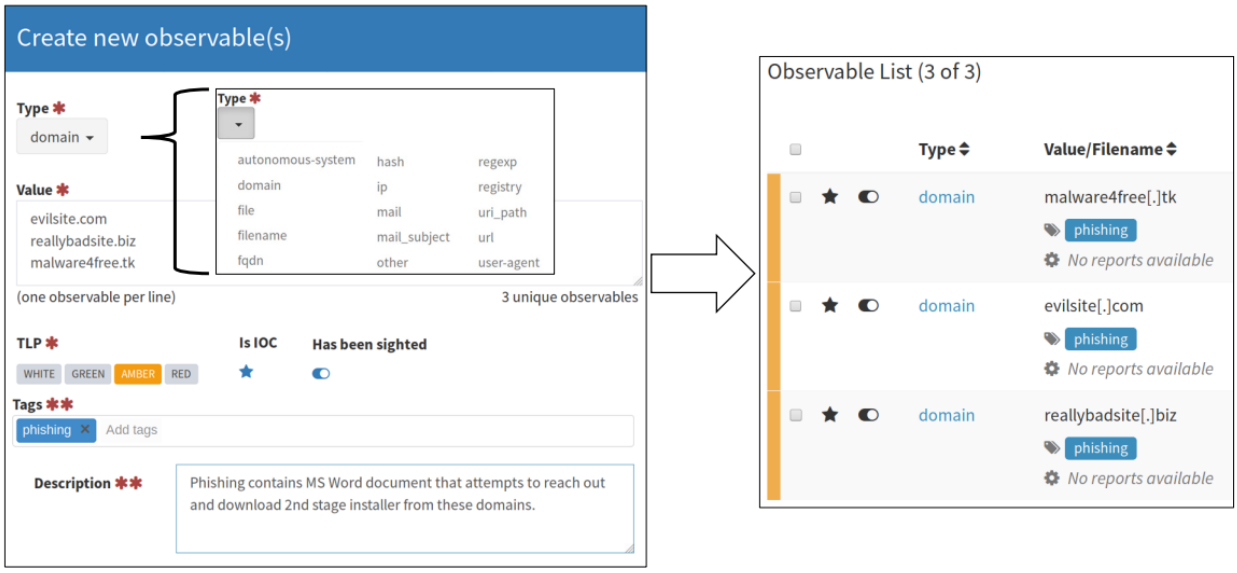
1- التوصيل(Delivery)	2- الاستغلال(Exploit)	3- التثبيت(Install)

  - تُعرض مجموعات المهام على الجانب الأيسر لواجهة المستخدم، مما يُسهل التنقل والتعرف على مراحل التحقيق.
- توزيع المهام بين المحللين:
  - تظهر كل مهمة على سطر منفصل مع تحديد المحلل المسؤول عنها، مثل *Analyst1* أو *Analyst2*.
  - يُمكن للمحلل المعين بدء العمل على المهمة بالنقر على زر "بدء (*Start*) "المخصص لها.

فوائد استخدام قوالب الحالات:

- الهيكلة والتنظيم:
  - تضمن القوالب أن جميع الحالات ذات الطبيعة المماثلة تُعالج بطريقة موحدة ومنظمة.
- تحسين التعاون:
  - تُسهل قوالب المهام التعاون بين المحللين من خلال تقسيم العمل بشكل واضح.
- توفير الوقت:
  - يُقلل استخدام القوالب من الوقت المطلوب لإعداد المهام يدويًا لكل حالة، مما يتيح استجابة أسرع للحوادث.

TheHive: إدخال العناصر القابلة للملاحظة(Observable Entry)



TheHive: إدخال العناصر القابلة للملاحظة(Observable Entry)

يتيح *TheHive* ربط العناصر القابلة للملاحظة (*Observables*) بحادث معين على مستوى الحالة. تُستخدم هذه العناصر لتوثيق مقتطفات بيانات مثيرة للاهتمام تم اكتشافها أثناء التحقيق، لكنها ليست بالضرورة تمثل بنية تحتية خبيثة أو ملفات ضارة.

تفاصيل ميزة العناصر القابلة للملاحظة:

- أنواع العناصر القابلة للملاحظة:
  - يحتوي *TheHive* على معظم الخيارات المطلوبة مسبقًا لأنواع هذه العناصر، ويتم عرضها في القائمة المنسدلة الخاصة بـ *Type*.
  - إضافة أنواع جديدة سهلة وتُتيح تخصيص النظام ليتناسب مع متطلبات التحقيق.
- إدخال العناصر بشكل جماعي:
  - يمكن إدخال عدة عناصر من النوع نفسه دفعة واحدة عن طريق فصلها بخطوط منفصلة، مما يجعل إدخال كميات كبيرة من البيانات أكثر كفاءة وسرعة.
- تمييز "مؤشرات الاختراق:(IOC) "
  - يمكن تمييز العنصر القابل للملاحظة على أنه *مؤشر للاختراق* (Indicator of Compromise)باستخدام أيقونة النجمة *"is IOC"*.
  - إذا لم يكن العنصر يمثل مؤشر اختراق، فيمكن تصنيفه كجزء من البيانات المرتبطة بالحالة فقط.

مثال تطبيقي (كما يظهر في الصورة):

- الوضع الافتراضي:
  - تمت إضافة ثلاثة نطاقات (*Domains*) كمؤشرات اختراق.

- تم تفعيل خيار *"has been sighted"*(تمت مشاهدته) لأنه في هذا السيناريو الافتراضي، تم استلام بريد تصيد احتيالي يحتوي على مستند *MS Word* مع ماكرو[5] يعمل تلقائيًا.
- هذا الماكرو حاول الاتصال بالنطاقات المضافة، مما يجعلها جزءًا من محاولة اختراق نشطة في بيئة العمل.

- سيناريو مختلف:
- إذا كانت العناصر القابلة للملاحظة لم تُشاهد مسبقًا داخل المنظمة، فيمكن إلغاء تحديد خيار *"has been sighted"*للإشارة إلى أن هذه العناصر لم يتم مواجهتها في البيئة حتى الآن.

فوائد هذه الميزة:

- التوثيق الدقيق:
- تسهل توثيق البيانات المهمة التي تم العثور عليها خلال التحقيق.
- تحليل شامل:
- تمكين المحللين من تصنيف وتحديد عناصر الخطر بدقة، سواء كانت معروفة أو غير معروفة سابقًا.
- التخصيص والتعاون:
- القدرة على إضافة أنواع جديدة وتخصيص النظام يتيح تكاملًا أفضل مع احتياجات الفريق ويعزز التعاون أثناء التحقيقات.

---

[5] ما هي الماكرو؟

الماكرو هي عبارة عن سلسلة من الأوامر أو الإجراءات التي يتم تسجيلها أو برمجتها لتنفيذ مهمة معينة بشكل تلقائي في تطبيقات مثل .Microsoft Word يمكن استخدام الماكرو لأتمتة المهام المتكررة وتسريع العمل، ولكنها في نفس الوقت يمكن أن تكون أداة خطيرة في يد المهاجمين.

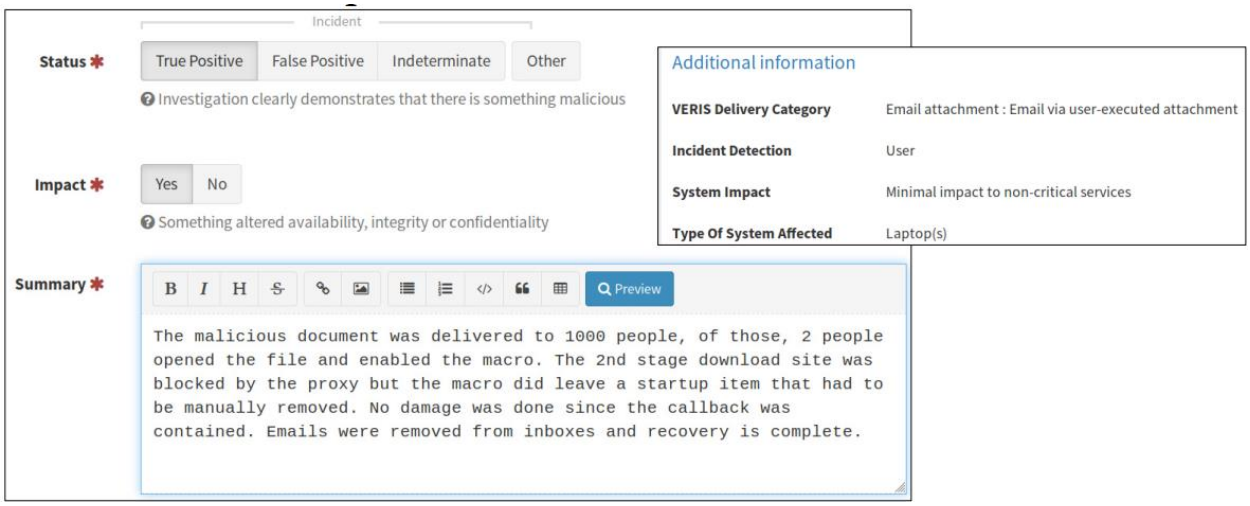
كيف تعمل الماكرو؟

تتم كتابة الماكرو بلغة برمجة خاصة مثل(VBA (Visual Basic for Applications ، والتي تسمح بتخصيص وتوسيع قدرات تطبيقات .Microsoft Office يمكن للمستخدمين إنشاء الماكرو الخاصة بهم أو تنزيلها من مصادر خارجية.

ما هو نظام استخبارات التهديدات السيبرانية **CTI** Cyber Threat Intelligence ؟

- استخبارات التهديدات السيبرانية (CTI) هي عملية جمع وتحليل المعلومات حول التهديدات الإلكترونية المحتملة أو الحالية التي تستهدف الأفراد أو المؤسسات. الهدف من ذلك هو فهم دوافع المهاجمين وأساليبهم واتخاذ إجراءات وقائية لحماية الأنظمة والبيانات.
- بمعنى آخر، CTIهي بمثابة نظام إنذار مبكر يحمي الأنظمة من الهجمات الإلكترونية عن طريق توفير معلومات استخباراتية حول التهديدات المحتملة وتساعد على اتخاذ قرارات أمنية أفضل.

إغلاق الحالات فيTheHive: Case Closure



إغلاق الحالات فيTheHive: Case Closure

عند الانتهاء من المهام المطلوبة، يمكن تصنيف الحالات وإغلاقها.

عملية إغلاق الحالة:

عندما يتم العمل على الحالة حتى اكتمالها، والذي يُعرَّف بإتمام جميع المهام المطلوبة في خطة العمل (*playbook*):

1. تصنيف الحالة:
   - يتم تحديد إذا كانت الحالة *إيجابية حقيقية* أو *إيجابية كاذبة*.
2. إضافة التصنيفات:
   - تحديد جميع الفئات المرتبطة بالحادث.
3. كتابة ملخص نهائي:
   - تقديم وصف مختصر عن محتوى التذكرة وكيف تم حلها.

مثال على الملاحظات النهائية:

في الشريحة، يظهر مثال لملاحظة ختامية حول حالة تصيد احتيالي ناجح.

- تفاصيل إضافية مرفقة:
  - *متجه التسليم* .(Delivery Vector)
  - طريقة اكتشاف الحادث.
  - الأثر الناتج.
  - أنواع الأنظمة المتأثرة.

أهمية التصنيف وإغلاق التذاكر:

- تحليل الاتجاهات:
  - يمكن جمع هذه البيانات على مدار الوقت عبر جميع التنبيهات لإنشاء تقارير توضح الأنماط في أنواع الهجمات التي يتعامل معها مركز العمليات الأمنية.(*SOC*)
- تحسين الدفاعات:
  - يوفر تصنيف التذاكر وتحليل البيانات الناتجة أفضل مصدر لاستخبارات التهديدات.
  - يمكن معرفة أنواع الهجمات الأكثر شيوعًا والأكثر تأثيرًا، مما يتيح تحسين الدفاعات وتبرير الاستثمارات المستقبلية لتعزيز هذه الجوانب.

- آلية للتغذية الراجعة:
  - تشكل هذه الأنشطة آلية حيوية لتقديم ملاحظات لفريق استخبارات التهديدات، مما يعزز الأداء العام لمركز العمليات الأمنية.

الخلاصة:

إغلاق التذاكر لا يقتصر على إنهاء العمل فقط، بل يشمل جمع البيانات وتحليلها لبناء رؤى قوية تدعم الدفاعات المستقبلية وتعزز استخبارات التهديدات.

التمرين 1.1: نظام إدارة الحوادثTheHive

هنا رابط على مواقع THM لغرفة التدريب على مشروع TheHive الرابط هنا:
https://tryhackme.com/r/room/thehiveproject

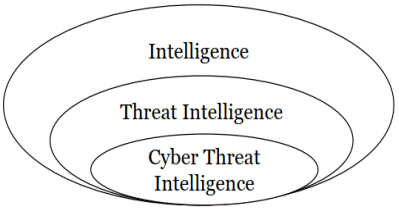
خريطة الدورة التدريبية

- **القسم الأول :أدوات وعمليات فريق الدفاع(Blue Team)**
- **القسم الثاني** :فهم الشبكة الخاصة بك
- **القسم الثالث** :فهم المضيفين، السجلات، والملفات
- **القسم الرابع** :التقييم والتحليل
- **القسم الخامس** :التحسين المستمر، التحليلات، والأتمتة

أدوات وعمليات فريق الدفاع(Blue Team)

1. مرحباً بك في فريق الدفاع!
2. التمرين 1.0: إعداد الآلة الافتراضية
3. نظرة عامة على مركز العمليات الأمنية(SOC)
4. مفاهيم الشبكة القابلة للدفاع
5. الأحداث، التنبيهات، الشذوذ، والحوادث
6. أنظمة إدارة الحوادث
7. التمرين 1.1: نظام إدارة الحوادثTheHive
8. **منصات استخبارات التهديدات**
9. التمرين 1.2: منصة استخبارات التهديداتMISP
10. إدارة الأمن والمعلومات (SIEM) والأتمتة
11. اعرف عدوك
12. ملخص القسم الأول
13. التمرين 1.3: إدارة الأمن والمعلومات باستخدام Elastic Stack

ما هي استخبارات التهديدات السيبرانية؟



ما هي استخبارات التهديدات السيبرانية؟

أولاً: ما المقصود باستخبارات التهديدات السيبرانية؟

- ليست مجرد قائمة بعناوين IP ونطاقات مشبوهة...
- **تعريف مبسط:** بيانات تهديد سيبراني مُحللة تُوفر ميزة استراتيجية وتكتيكية ضد الخصوم.
  - تُساعد في تحديد أولويات الموارد الدفاعية.
  - تعتمد على مبدأ "الهجوم يُغذي الدفاع."
- تتكون من عدة مكونات.
  - دعونا نستعرض هذه المكونات...

ما هي استخبارات التهديدات السيبرانية؟

مصطلح شائع لكنه غامض:

على الرغم من سماعنا المتكرر لعبارة "استخبارات التهديدات السيبرانية"، إلا أن هناك الكثير من اللبس حول معناها. ومع أن المصطلح يبدو غير واضح في بعض الأحيان، فإن العديد من الخبراء قدموا تعريفات عملية له.

جوهر الفكرة:

جميع التعريفات تتفق على هدف رئيسي واحد:

- تحقيق ميزة استراتيجية وتكتيكية على الخصوم.
- يتم ذلك من خلال فهم التكتيكات والتقنيات والإجراءات (TTPs) التي يستخدمها الخصوم لتحقيق أهدافهم.

مبدأ "الهجوم يُغذي الدفاع":

- هذا المفهوم يؤكد على أهمية الاستفادة من معرفة سلوك الخصوم لتعزيز التحضير الدفاعي.
- هذه هي الفكرة الأساسية وراء استخبارات التهديدات السيبرانية.

قبل الغوص في منصات استخبارات التهديدات:

لنناقش مكونات استخبارات التهديدات السيبرانية لفهم المفهوم بشكل أفضل. سنستخدم مخطط *فين* (Venn Diagram) المستوحى من كتاب متميز حول هذا الموضوع بعنوان: *Intelligence-Driven Incident Response* [6]

المؤلفان: **سكوت جي. روبرتس** و**ريبيكا براون**، وهما من مدربي شركة SANS.

لماذا المكونات مهمة؟

- يساعد تعريف كل طبقة من طبقات استخبارات التهديد في فهم المفهوم الشامل.

---

[6] حمل الكتاب من الرابط هنا https://drive.google.com/file/d/1YLHVJ8CmXDRciTs0h2Ndxt1c-rGyhgh1/view?usp=sharing

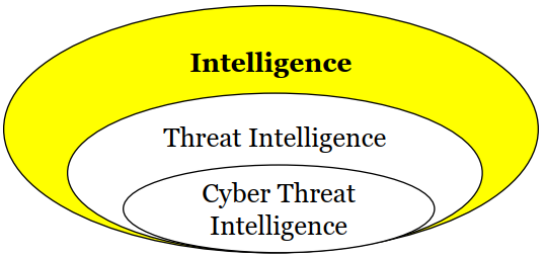
- يوضح كيف تُساهم منصات استخبارات التهديدات (TIPs) في تحقيق أهدافنا في مجال استخبارات التهديد السيبراني.(CTI)

الخلاصة:

استخبارات التهديدات ليست مجرد معلومات خام؛ إنها مجموعة بيانات مُحللة تقدم رؤى استراتيجية وتكتيكية تُساعد المؤسسات على التصدي للتهديدات السيبرانية بفعالية أكبر.

[1] https://www.oreilly.com/library/view/intelligence-driven-incident-response/9781491935187/

تعريف الاستخبارات



"جمع المعلومات الخارجية من مصادر متعددة وتحليلها وفقًا لمتطلبات قائمة لتقديم تقييم يؤثر على اتخاذ القرارات".

سكوت جي. روبرتس وريبيكا براون، من كتاب الاستجابة للحوادث القائمة على الاستخبارات: التغلب على الخصوم

أمثلة على الاستخبارات:

- **تقرير الطقس :**هل أحتاج إلى ارتداء معطف اليوم؟
- **تقرير المرور :**كم من الوقت أحتاج للوصول إلى العمل؟

شرح تعريف الاستخبارات

ما هي الاستخبارات؟

يمكن تلخيصها بالاقتباس أعلاه من كتاب سكوت جي. روبرتس وريبيكا براون.

- يحتوي هذا التعريف على العناصر الأساسية، مثل:
  - التحليل.
  - مقارنة البيانات مع متطلبات محددة.
  - استخدام النتائج لدعم اتخاذ قرارات فعّالة.

نقاط مشتركة في تعريفات الاستخبارات:

غالبًا ما تشمل التعريفات فكرة التحليل المنهجي لتوجيه القرارات بناءً على متطلبات محددة.

تعريف أكثر عمقًا من سيرجيو كالتاجيرون

سيرجيو كالتاجيرون، مدير استخبارات التهديد والتحليلات في شركة *Dragos, Inc.*، قدم تعريفًا أكاديميًا أوسع عبر منشور له، يشير فيه إلى أن:

"الاستخبارات هي عملية جمع ومعالجة المعلومات المتعلقة بالتهديدات ووكلائها التي تحتاجها المنظمة لصياغة سياساتها الأمنية، ولتنفيذ أنشطة غير قابلة للتعقب خارج حدود المنظمة لدعم تلك السياسات. وتشمل الاستخبارات حماية العملية والمنتجات، وكذلك الأفراد والمنظمات المرتبطة، من الكشف غير المصرح به".

وأضاف:

"أقترح أن استخبارات التهديدات السيبرانية ليست سوى تطبيق مبادئ الاستخبارات والحرفية الأمنية في مجال أمن المعلومات".

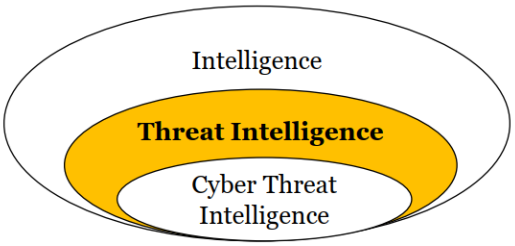
الخلاصة

- الاستخبارات هي عملية تحليلية منظمة تُستخدم لدعم اتخاذ القرارات الاستراتيجية.
- في مجال الأمن السيبراني، تُطبق نفس المبادئ لتوفير فهم أعمق للتهديدات والوكلاء المهاجمين، مما يُمكن المنظمات من تعزيز سياساتها الأمنية واتخاذ إجراءات دفاعية فعّالة.

[1] https://www.oreilly.com/library/view/intelligence-driven-incident-response/9781491935187/

[2] http://www.activeresponse.org/threat-intelligence-definition-old-new/

تعريف التهديد



كيف نُعرِّف التهديد؟

- "مزيج من النية، القدرة، والفرصة – "*روب إم. لي*.
  - **النية :**رغبة الفاعل الخبيث في استهداف منظمتك.
  - **القدرة :**الوسائل التي يمتلكها للقيام بذلك (مثل أنواع معينة من البرمجيات الضارة).
  - **الفرصة :**الثغرة التي يحتاجها المهاجم (مثل نقاط الضعف في البرمجيات، أو الأجهزة، أو العنصر البشري).

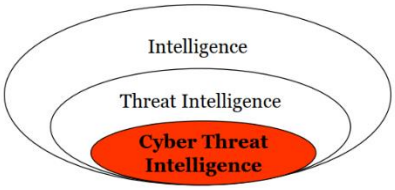
شرح تعريف التهديد

عندما نضيف كلمة "تهديد" إلى مصطلح الاستخبارات، ما نوع التهديد الذي نتحدث عنه؟

روب إم. لي، مدرب معتمد من *SANS* والرئيس التنفيذي ومؤسس شركة *Dragos, Inc.*، يوضح أن التهديد يُعرف استنادًا إلى ثلاثة عناصر رئيسية:

1. **النية :**يجب أن يكون لدى الكيان الخبيث الدافع لمهاجمة المنظمة.
2. **القدرة :**يجب أن يمتلك الوسائل التقنية أو الموارد اللازمة لتنفيذ الهجوم.
3. **الفرصة :**يجب أن تكون هناك ثغرة أو ضعف يمكن استغلاله لتحقيق الهجوم.

[1] http://www.robertmlee.org/intelligence-defined-and-its-impact-on-cyber-threat-intelligence/



تعريف استخبارات التهديدات السيبرانية

"استخبارات التهديدات هي تحليل الخصوم – قدراتهم، دوافعهم، وأهدافهم؛ واستخبارات التهديدات السيبرانية (CTI[7]) هي تحليل كيفية استخدام الخصوم للمجال السيبراني لتحقيق أهدافهم".

سكوت ج. روبرتس وريبيكا براون، Intelligence-Driven Incident Response: Outwitting the Adversary

محاور التعريف الأساسية

- **يتطلب التحليل البشري**
- **تحديد التكتيكات والتقنيات والإجراءات (TTPs) وأهداف الفاعلين الخبيثين**
- **إنتاج مخرجات تقود عملية اتخاذ القرار**

توضيح تعريف استخبارات التهديدات السيبرانية

ما هي إذًا استخبارات التهديدات السيبرانية؟

هي مزيج من المفاهيم التي نوقشت مسبقًا ولكن في سياق المجال السيبراني. وفقًا لموقع *dictionary.com*، يُعرَّف "السيبراني" بأنه:

"متعلق أو مميز بثقافة الحواسيب، تكنولوجيا المعلومات، والواقع الافتراضي".

بالتالي، استخبارات التهديدات السيبرانية تتعلق بإجراء تحليل للتهديدات ضمن نطاق الحواسيب وتكنولوجيا المعلومات.

الاقتباس أعلاه من كتاب *Intelligence-Driven Incident Response* يجمع هذه العناصر:

"استخبارات التهديدات هي تحليل الخصوم – قدراتهم، دوافعهم، وأهدافهم؛ واستخبارات التهديدات السيبرانية (CTI) هي تحليل كيفية استخدام الخصوم للمجال السيبراني لتحقيق أهدافهم".

مايكل كلوبيرت، المؤلف المشارك لورقة *Lockheed Martin Cyber Kill Chain*، يوسع هذا المفهوم من خلال تقسيمه إلى العمليات والتحليل في استخبارات التهديدات السيبرانية:

- **العمليات:**

"أُعرّف عمليات استخبارات التهديدات السيبرانية بأنها الإجراءات التي تُتخذ في الفضاء السيبراني لاختراق وحماية المعلومات والقدرات المتاحة في هذا المجال".

- **التحليل:**

"أُعرِّف تحليل استخبارات التهديدات السيبرانية بأنه تحليل تلك الإجراءات والفاعلين، الأدوات، والتقنيات وراءها لدعم العمليات".

- **المجال:**

" أُعرِّف مجال استخبارات التهديدات السيبرانية بأنه اتحاد بين العمليات والتحليل في هذا السياق".

---

[7] استخبارات التهديدات السيبرانية (CTI) هي عملية جمع وتحليل المعلومات حول التهديدات الإلكترونية المحتملة أو الحالية التي تستهدف الأفراد أو المؤسسات. الهدف من ذلك هو فهم دوافع المهاجمين وأساليبهم واتخاذ إجراءات وقائية لحماية الأنظمة والبيانات.

بمعنى آخر، CTIهي بمثابة نظام إنذار مبكر يحمي الأنظمة من الهجمات الإلكترونية عن طريق توفير معلومات استخباراتية حول التهديدات المحتملة وتساعد على اتخاذ قرارات أمنية أفضل.

الهدف الأساسي لاستخبارات التهديدات السيبرانية

على الرغم من اختلاف الصياغات، يتمحور التعريف حول هدف واحد:

"تحليل بيانات التهديدات السيبرانية لتحويلها إلى معلومات حول الفاعلين الخبيثين تساعدنا في فهم تكتيكاتهم، تقنياتهم، إجراءاتهم(TTPs) ، وما يمكن أن تكون أهدافهم".

- يجب أن يتم هذا التحليل وفقًا لمتطلبات محددة لتحقيق هدف التحليل.
- إنتاج مخرجات موجهة للجمهور المستهدف لمساعدتهم في اتخاذ قرارات أو تقديم نتائج قابلة للتنفيذ.

[1] https://www.oreilly.com/library/view/intelligence-driven-incident-response/9781491935187/

[2] http://www.activeresponse.org/threat-intelligence-definition-old-new/

الذكاء السيبراني الجيد مقابل السيئ

طريقة مبسطة لتوضيح ذلك:

- **"IOC = Observable + Context"** (مؤشرات الاختراق = الظاهرة + السياق)
- عند تسجيل البيانات، قم بتضمين أكبر قدر ممكن من التفاصيل التي تتمنى أن يراها الآخرون.

على اليسار مثال ل CTI لا يحتوي على سياق أو وصف لما حدث ويصنف بأنه فقير المحتوي لانه لا يوضح شيئ

على اليمين مثال اخر لكتابة السياق أو الوصف بشكل احترافي حيث فيه توضيح مفصلسواء باسم البرنامج أو ال domain name وال URL ... إلخ

Poor CTI – No Context

The IOC "hxxp://malwareC2[.]net" was associated with a Trojan.SuperMalware campaign in June 2020.

A simplified way to put this:

- "IOC = Observable + Context"[1]
- When recording, include as much detail for others as you would want to see

Excellent CTI – with Context

On 6/10/2020 spoofed "email[@]spoofedomain[.]com" sent "Invoice" themed emails that included the malicious URL "hxxp://totallynotlegit[.]com/probablymalware[.]exe" [MD5: 32 characters] (T1566.002), which is detected as Trojan.SuperMalware.

When executed, "probablymalware[.]exe" [MD5: 32 characters] creates a Scheduled Task named "DoingBadStuff" (T1053.005) and begins C2 over port 443 to "hxxp://malwareC2[.]net" (T1071.001).

الذكاء السيبراني الجيد مقابل السيئ

في مدونة رائعة على *Medium* للكاتب *آندي بيازا*، يُبرز الكاتب مثالًا ممتازًا لما يجب أن تكون عليه استخبارات التهديدات السيبرانية (CTI) وما يجب ألا تكون عليه.

هل سبق أن تلقيت تنبيهًا يعتمد على تطابق في استخبارات التهديدات وتساءلت: **"ماذا يفترض أن أفعل بهذه المعلومات؟"**

إذا كان الجواب نعم، فمن المحتمل أنك تلقيت قائمة من العناصر السيئة(مثل عناوين IP أو نطاقات) دون سياق يوضح سبب اعتبارها سيئة.

الشريحة أعلاه توضح مثالًا من آندي حول استخبارات التهديدات السيبرانية السيئة على اليسار، وأخرى أفضل بكثير على اليمين مع السياق اللازم لتفسير المطابقة بشكل صحيح.

آندي يوضح الهدف من CTI باستخدام عبارته المميزة التي يسهل تذكرها:
"IOCs = Observable + Context" *(مؤشرات الاختراق = الظاهرة + السياق)*

- الظاهرة :(Observable) هي المؤشر "السيئ" الذي يتطابق عليه نظامك (مثل SIEM أو IDS).
- السياق :(Context) هو البيانات الداعمة التي تفسر سبب اعتبار هذه الظاهرة تهديدًا.

نقل التحديات الشائعة داخل مراكز عمليات الأمن(SOC)

واحدة من أبرز التحديات التي تواجه العديد من مراكز عمليات الأمن هي أن تغذية استخبارات التهديدات[8] غالبًا ما تكون مجرد قائمة من "الظواهر" دون أي سياق مصاحب. هذا يؤدي إلى مواقف شائعة، حيث يحصل المحللون على تنبيه يفيد بأن شخصًا ما تواصل مع عنوان IPسيئ معروف، ولكنهم يتركون لمعرفة:

- **لماذا تم تصنيفه سيئًا؟**
- **متى تم تصنيفه سيئًا؟**

وفقًا لآندي، إذا لم يكن لدى منصة استخبارات التهديدات (TIP) الخاصة بك خاصية "الوصف " (Description)لمؤشرات الاختراق، فأنت لا تملك TIP حقيقية. بل لديك مجرد "جامع للظواهر."

الخلاصة

استخبارات التهديدات لا يمكن أن تكون مجرد قائمة من المؤشرات الذرية السيئة (Atomic Observables).

- في أفضل الحالات، ستكون مؤلمة ومضيعة للوقت.
- في أسوأ الحالات، ستكون عديمة القيمة.

لذلك، يجب أن تتضمن CTI سياقًا كافيًا لتفسير وتحليل التهديدات بشكل فعّال.

مقال آندي مصدر رائع للمعرفة حول منصات استخبارات التهديدات والموضوعات ذات الصلة، ويمكن العثور عليه عبر الرابط:

https://klrgrz.medium.com

[1] https://klrgrz.medium.com/cti-is-better-served-with-context-getting-better-value-from-iocs-496343741f80

[8] نضرب مثالاً هنا بأن رجلا من رجال الشرطة وصل له خبر ان فلان يقتل فلان فقط ولا يوجد أي معلومة أخري فكيف سيوقف رجل الشرطة عملية القتل هذه ؟!؟!؟!؟! بالطبع لن يستطيع إلا بعد بذل مجهود رهيب وفى الغالب لن يستطيع فى النهاية.

منصات استخبارات التهديدات ودورها

هناك نوعان من الأطراف المعنية باستخبارات التهديدات:

- **المنتجون** و**المستهلكون** لاستخبارات التهديدات.
- تحتوي العديد من مراكز عمليات الأمن (SOCs) على فريق مخصص لاستخبارات التهديدات.
  - يقوم فريق استخبارات التهديدات بإنتاج المعلومات.
  - بينما يستهلكها المحللون.
- تعتمد وظائف المحللين بشكل أساسي على استخدام بيانات التهديدات والمعلومات والتحليل لاكتشاف وحماية الأنظمة من الاختراقات.

دور منصات استخبارات التهديدات(TIPs)

- تساعدك منصات استخبارات التهديدات في إتمام هذه المهام عبر:
  - إنشاء **قاعدة معرفة** تحتوي على بيانات التهديدات الخاصة بك، بالإضافة إلى المعلومات والاستخبارات ذات الصلة.
  - **أتمتة تبادل البيانات** مع الأدوات الأمنية الأخرى وإجراء الاستعلامات بسهولة.
- **ولكنها لا تنتج استخبارات التهديدات لك!**

منصات استخبارات التهديدات ودورك كمحلل

عندما نتحدث عن استخبارات التهديدات، هناك دائمًا جانبين رئيسيين:

- **إنتاجها**
- **واستهلاكها**[9]

كمحللي SOC ، ستتركز أغلب مهامك على **استهلاك** استخبارات التهديدات، بينما قد يتم إنتاجها بشكل رئيسي من قبل فريق مخصص لاستخبارات التهديدات داخل المركز.

في عملك اليومي، من المرجح أنك ستتعامل بشكل مكثف مع بيانات التهديدات والمعلومات والتحليل من خلال:

- **التحقق من التنبيهات**
- **البحث عن التهديدات**
- **التحقيق في الحوادث**

كل هذه الأنشطة ستعتمد بشكل أساسي على الرجوع إلى استخبارات التهديدات في مرحلة ما لضمان حماية الأنظمة واكتشاف التهديدات بفعالية.

---

[9] "استهلاك CTI يشمل تحويل المعلومات والتحليلات التي ينتجها الخبراء إلى إجراءات وقائية فعالة، مثل تقييم التهديدات وتحديد الأولويات وتطوير استراتيجيات الدفاع. المستهلكون الرئيسيون لـ CTI هم متخذو القرارات وفرق العمليات الأمنية والمحللون".

ميزات منصات استخبارات التهديدات

تعتمد فرق الدفاع (Blue Team) بشكل كبير على قوائم المؤشرات (Indicators) للتنبيهات، مثل:

- **عناوين IP الضارة**
- **النطاقات**
- **البصمات الرقمية (Hashes)**[10] وغيرها.

متطلبات الحلول لمنصات استخبارات التهديدات

يجب أن توفر منصات استخبارات التهديدات القدرة على:

1. **تخزين المعلومات والتحليلات الخاصة بالمؤشرات المعروفة**:
   - الاحتفاظ ببيانات التحليل والمعلومات المتعلقة بالمؤشرات في قاعدة بيانات منظمة.
2. **إجراء استعلامات تلقائية وسريعة عبر واجهة برمجية**:**(API)**
   - تسهيل الوصول إلى البيانات المخزنة دون الحاجة إلى عمليات بحث يدوية بطيئة.
3. **تسجيل السياق حول العناصر المخزنة** (ليس مجرد قائمة):
   - مثال: "عنوان IP 1.2.3.4 متعلق بالموقع الشرير evilsite.com ، والذي قدّم مجموعة استغلال في 19-02-2020."
4. **إيجاد الارتباطات بين الأحداث المختلفة**:
   - القدرة على تحديد العلاقة بين المؤشرات والأحداث المتعددة عبر قواعد البيانات.
5. **مشاركة المؤشرات مع المنظمات الأخرى**:
   - دعم التعاون وتبادل المعلومات بين الجهات لتحسين الدفاع المشترك.

شرح ميزات المنصات

الهدف الرئيسي لمنصة استخبارات التهديدات هو **تخزين وتحليل البيانات والمعلومات المتعلقة بالتهديدات والمؤشرات التي تم جمعها**، مع تقديمها بطريقة سهلة للبحث والتفاعل.

الواجهة والتكامل:

- يجب أن تحتوي قاعدة البيانات على واجهة سهلة الاستخدام تتيح للمستخدمين إجراء عمليات البحث يدويًا عند التحقيق في الحوادث.
- يجب أن توفر **إمكانيات تكامل قوية** مع الأدوات الأمنية الأخرى، مثل **أنظمة إدارة الحوادث (IMS)**و**أنظمة إدارة المعلومات الأمنية والأحداث(SIEM)** ، باستخدام واجهات برمجية (APIs).

الأهمية:

- إذا كانت بيانات استخبارات التهديدات مغلقة في نظام خاص وغير متاحة للتكامل مع أدوات الأمان الأخرى، فستكون فائدتها محدودة للغاية.
- **التواصل بين الأدوات الأمنية المختلفة** هو ميزة أساسية لضمان تحقيق أقصى استفادة من المنصة.

---

[10] مصطلح ترجمة ال **Hash** بأنه **"البصمة الرقمية"** لم اجده ولم اقتبسه من مكان اخر وذكرت هذه الملاحظة حتي إذا وجدت من يعترض عليه فهو من ترجمتي الخاصة وليس من ترجمة معتمدة و للعلم لم ابحث فى ترجمته كثيرا حيث لم اجد له ترجمة تعبر عن وظيفته أفضل من **"البصمة الرقمية"**.

متطلبات منصة استخبارات التهديدات

المؤشرات أو تفاصيل التكوين منخفضة المستوى؟

- معظم منصات استخبارات التهديدات (TIPs) تتعامل بسهولة مع مؤشرات الاختراق.(IOCs)
- تشمل هذه المؤشرات: عناوينIP ، أسماء الملفات، النطاقات، قيم التجزئة (البصمة الرقمية) (Hashes)، روابطURL ، وغيرها.
- **ميزة مهمة :**إدخال كميات كبيرة من البيانات بسهولة ودمجها مع أدوات أخرى.
- بعض المنصات توفر ميزات إضافية أكثر شمولاً:
  - هل تخزّن تكوينات البرمجيات الضارة؟ هل تحتاج إلى حقول غير قياسية؟
  - كيف تريد الربط بين العناصر المخزنة؟
  - هل يعدّ مشاركة البيانات وظيفة أساسية؟
  - ما حجم المؤشرات التي ستخزنها؟

شرح متطلبات منصة استخبارات التهديدات

عامل رئيسي قد يؤثر على اختيارك هو مستوى التفاصيل الاستخباراتية التي تحتاج لتخزينها، إضافةً إلى اهتمامك بمشاركة نتائجك.

- **المؤشرات الشائعة:**

معظم المنصات مصممة خصيصًا للتعامل مع المؤشرات القياسية مثل عناوينIP ، تجزئات (بصمة) الملفات (Hashes)، الروابط(URLs) ، وأسماء الملفات. إذا كانت هذه احتياجاتك الرئيسية، فإن معظم الحلول المتاحة ستلبي متطلباتك الأساسية. وبالتالي، يمكنك اتخاذ قرارك بناءً على التكامل مع أدوات أخرى.

- **التحليل المعمق:**

إذا كان عملك يتطلب تحليلًا شاملاً يشمل أسماء الحقول التعسفية أو البيانات غير التقليدية، فبعض المنصات ستكون أكثر ملاءمة.

عوامل اختيار المنصة المناسبة:

1. حدد **الحقول والبيانات** التي تحتاج إلى تخزينها.
2. تأكد من اختيار منصة تدعم سير العمل المتوقع وتلبية احتياجاتك.
3. إذا كان حجم المؤشرات كبيرًا، تحقق من قدرة المنصة على التعامل مع هذا الحجم.
4. إذا كان **مشاركة البيانات** جزءًا من العمليات، ابحث عن المنصات التي تسهل ذلك.

الخلاصة

اختيار منصة استخبارات التهديدات يعتمد على احتياجاتك في التحليل والتخزين والمشاركة. المنصات القوية توفر تكاملًا سهلاً، معالجة كميات كبيرة من البيانات، ومرونة في التعامل مع الحقول المخصصة والوظائف الإضافية.

تخزين ومشاركة استخبارات التهديدات بطريقة آمنة: المؤشرات المنزوعة الخطورة

الحذر عند التعامل مع مؤشرات الاختراق!

- **عناوين IP** والروابط غالبًا ما تصبح "نشطة" بمجرد إدخالها.
- العديد من الأدوات والمقالات تقوم بـ"نزع خطورة" هذه المؤشرات.
- يسمح ذلك بإدراجها بأمان في التقارير، ملفاتExcel ، تطبيقات مثلSlack ، وغيرها، دون أن تتحول إلى روابط نشطة أو يتم تحميلها تلقائيًا!

Indicator المؤشر	Details التفاصيل
hxxp://satkas.waw[.]pl/rainloop/forecast	TrailBlazer C2
vm-srv-1.gel.ulaval[.]ca	GoldMax C2
156[.]96[.]46[.]116	TA Infrastructure
188[.]34[.]185[.]85	TA Infrastructure

شرح تخزين ومشاركة استخبارات التهديدات بطريقة آمنة

تفصيل مهم يتعلق بمنصات استخبارات التهديدات هو استخدام المؤشرات المنزوعة الخطورة (De-fanged Indicators).

- **المشكلة المحتملة:**

بعض الحلول تقوم بتحويل الروابط وعناوين IP إلى روابط نشطة تلقائيًا. إذا لم يتم الحذر، قد يؤدي ذلك إلى النقر عليها دون قصد، مما يعرّض الفريق لخطر الإصابة بالبرمجيات الضارة.

- **الحل:**

يتم استخدام **الأقواس المربعة** بدلًا من النقاط في الروابط وعناوين IP لجعلها غير قابلة للنقر. على سبيل المثال:

  - الرابط الأصلي: http://malicious-site.com
  - الرابط منزوع الخطورة: hxxp://malicious-site[.]com

ويمكن أيضًا استبدال بروتوكول مثل "http" بـ "hxxp"لتحقيق الهدف نفسه.

أهمية المؤشرات المنزوعة الخطورة

- **السلامة:**

تقلل من احتمالية تحميل الروابط أو فتحها عن طريق الخطأ.

- **التقارير والمشاركة:**

تسهل تضمين المؤشرات في المستندات أو الاتصالات اليومية بأمان.

أمثلة عملية

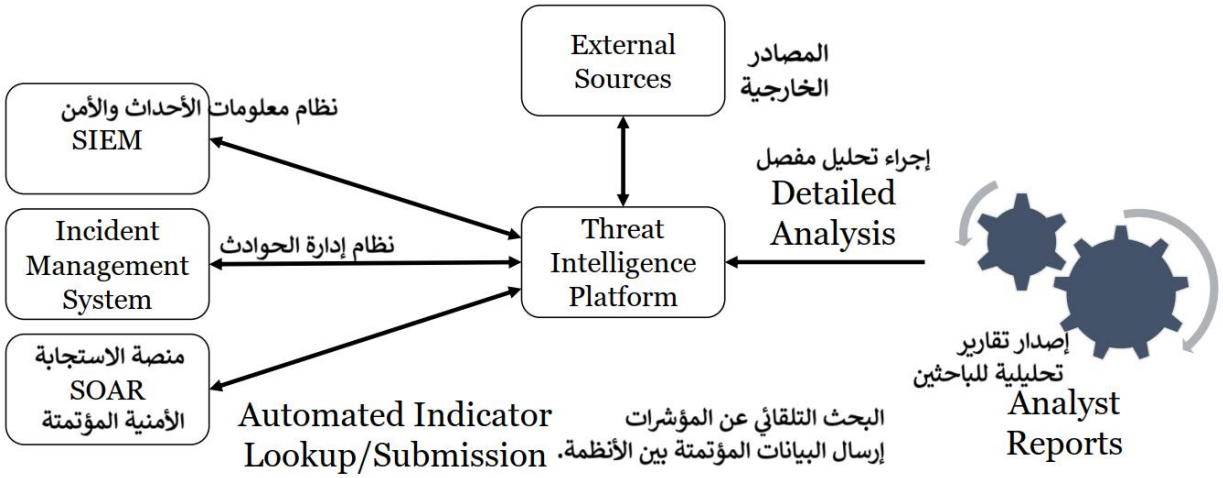
تُظهر المؤشرات المنزوعة الخطورة في الشريحة مثالًا لكيفية تمرير بيانات مؤشرات الاختراق بأمان، مثل تلك المتعلقة بهجمات **Stellar Particle**في أواخر عام 2021.

الخلاصة

استخدام المؤشرات المنزوعة الخطورة هو إجراء بسيط ولكنه فعال للغاية للحفاظ على الأمان عند تخزين أو مشاركة بيانات استخبارات التهديدات داخل الفرق.

[1] Early Bird Catches the Wormhole: Observations from the StellarParticle Campaign – CrowdStrike Blog: **مدونة كراود سترايك - StellarParticle العصفور الباكر يمسك بالثقب الدودي: ملاحظات من حملة**
https://www.crowdstrike.com/blog/observations-from-the-stellarparticle-campaign/

سير عمل منصة استخبارات التهديدات(TIP Workflow)



سير عمل منصة استخبارات التهديدات(TIP Workflow)

عند النظر إلى منصة استخبارات التهديدات (TIP) بعقلية الأنظمة، يمكننا ملاحظة أن معظم المدخلات والمخرجات تتعلق بمؤشرات ومعلومات التهديدات، سواء كانت تُرسل إلى المنصة من أدوات الأمان أو عبر استعلامات يتم إرسالها إليها.

ملاحظات هامة:

1. **مصادر المعلومات الخارجية:**

يمكن أن تأخذ منصة استخبارات التهديدات بياناتها من خارج المؤسسة. هناك العديد من الموردين ومجموعات الصناعة التي تقدم تغذيات تحتوي على مؤشرات تمثل مصادر خارجية موثوقة لمعلومات التهديدات.

2. **أهمية تبادل المعلومات:**

كما يُقال، "المشاركة تعني الاهتمام"، وينطبق ذلك على معلومات التهديدات أيضًا. فكلما زادت مصادر البيانات التي تمتلكها، وخاصة إذا كانت مخصصة لقطاعك وبيئتك، زادت احتمالية كشف المهاجمين داخل شبكتك.

الاستفادة منTIP

- **إدخال المؤشرات:** جمع البيانات من أدوات الأمان الداخلية أو المصادر الخارجية.
- **تحليل المؤشرات:** التحقق من موثوقيتها وتكاملها مع بقية منظومة الأمن السيبراني.
- **تبادل المعلومات:** تعزيز أمان المؤسسة عبر التعاون مع مصادر أخرى موثوقة لتبادل مؤشرات التهديد.

الخلاصة

تُمثل منصة استخبارات التهديدات عنصرًا أساسيًا في أنظمة الأمان السيبراني. بدمج مصادر متعددة من المعلومات، وتنسيق الجهود لتحليلها، يمكن تحسين قدرة المؤسسة على اكتشاف التهديدات ومنعها قبل أن تتسبب في أي ضرر.

منتجات منصات استخبارات التهديدات (Threat Intelligence Platform Products)

المنصات المجانية المستضافة ذاتيًا:

1. **MISP (Malware Information Sharing Platform):**

منصة مفتوحة المصدر تُستخدم لمشاركة معلومات البرمجيات الخبيثة. يتم استخدامها في المعامل ضمن هذا الفصل الدراسي.

2. **OpenCTI:**

خيار حديث وواعد، يقدم إمكانيات متطورة لإدارة استخبارات التهديدات.

المنصات التجارية:

CrowdStrike Falcon X	**ThreatConnect**	**LogRhythm TLM**	**Palo Alto XSOAR TIM**
Recorded Future	**IBM X-Force Exchange**	**Anomali ThreatStream**	

شرح المنتجات

تتضمن هذه الشريحة خيارات متعددة من منتجات استخبارات التهديدات. يمكن الاعتماد على حلول مفتوحة المصدر مثل **MISP**و**OpenCTI**، أو اختيار أنظمة سحابية متقدمة تقدمها شركات مثل **ThreatConnect**و**AlienVault OTX**.

اختيار المنصة المناسبة:

- يعتمد الاختيار على **عمق التحليل** الذي تحتاجه، ومدى **تكامل** المنصة مع أنظمة الأمان الحالية لديك.
- يجب أن تدرك أن منصة استخبارات التهديدات لا تُنتج المعلومات الاستخباراتية نيابة عنك. بل هي أداة تُستخدم **لتخزين واستعلام** المعلومات والاستخبارات التي قمت بجمعها أو الحصول عليها.

ملاحظات هامة:

- إذا كنت تبحث عن مزود تقارير استخباراتية جاهزة، فهذا منتج مختلف تمامًا يتمثل في التقارير المكتوبة من قبل محللي تلك الشركات.
- **منصات استخبارات التهديدات** تُستخدم لتنظيم وتخزين وتحليل استخباراتك الخاصة، وليس لتوليدها بشكل مستقل.

الخلاصة

توفر هذه المنصات خيارات متعددة لتناسب مختلف الاحتياجات، من الحلول المجانية الموجهة للأبحاث والتجارب إلى الأنظمة التجارية المتقدمة المخصصة للمؤسسات.

[1] https://www.misp-project.org/
[2] https://www.opencti.io/en/

مصادر تغذية استخبارات التهديدات(Threat Intel Feeds)

الهدف: الحصول على معلومات تلقائية، ذات صلة، ومحدثة باستمرار: • الاستفادة من الوصول إلى مصادر التهديدات المغلقة ومفتوحة المصدر. • تصنيف المعلومات بناءً على محتوياتها. • لا تكتفِ بالأخذ فقط؛ شارك المعرفة أيضًا! **قياس فعالية مصادر التغذية:** • **"عندما يتم تنبيه بناءً على تغذية س، كم مرة يكون التنبيه صحيحًا؟"** • **"ما مدى سرعة وصول البيانات إلى المصدر؟"** • الموازنة بين **الدقة** و**الشمولية**.	**الانضمام إلى مراكز مشاركة وتحليل المعلومات ISACs)و:(ISAOs** تعتبر مراكز **ISAC**و **ISAO**مصدرًا موثوقًا للمعلومات عالية القيمة المتعلقة بالتهديدات، وتتضمن: • **H-ISAC:**المجال الصحة. • **MS-ISAC:**للمؤسسات متعددةالولايات. • **EI-ISAC:**للبنية التحتية الانتخابية. • **W-ISAC:**لأنظمة المياه. • **FS-ISAC:**للخدمات المالية. • **A-ISAC:**للطيران. • **IT-ISAC:**لتقنية المعلومات. • **REN-ISAC:**لشبكات التعليم والبحث. • **Retail and Hospitality ISAC:** للبيع بالتجزئة والضيافة. • **MTS-ISAC:**لأنظمة النقل البحري. • **DNG-ISAC:**للغاز الطبيعي المتدفق. • **ONG-ISAC:**للنفط والغاز الطبيعي. • **S-ISAC:**للمعلومات المتعلقة بالفضاء.

تفاصيل حول مصادر تغذية التهديدات

وظيفتها:

مصادر تغذية التهديدات هي طريقة شائعة لملء منصة استخبارات التهديدات. رغم وجود العديد من المصادر المجانية والتجارية، إلا أنه لا يمكن تقديم توصية شاملة لكل فرق أمن المعلومات، حيث تختلف الاحتياجات حسب: **الصناعة - أنواع التهديدات - الأدوات المستخدمة**

عوامل تقييم مصادر التغذية:

1. **الصلة:**
   - هل تغطي المصدر تهديدات مرتبطة بمجالك؟
2. **المحتويات:**
   - ما هي البيانات المقدمة؟ هل تشمل القيم التجزئية (البصمة) (Hashes) ، الروابط (URLs)، أسماء النطاقات(Domain Names) ، أو أكثر؟
   - تأكد من معرفة نوع البيانات المتوفرة وكيفية الوصول إليها بسرعة.
3. **السرعة:**
   - ما الزمن المستغرق بين ظهور التهديد في الأخبار ووصوله إلى المصدر ليتم استخدامه في أدوات التحليل الخاصة بك؟
4. **الدقة مقابل الشمولية:**
   - هل تفضل تغذية تشمل أي شيء قد يكون خطيرًا؟ أم فقط التهديدات المؤكدة بنسبة 100%؟

- الاعتماد على المصدر الأقل شمولية قد يؤدي إلى **نتائج سلبية خاطئة (False Negatives)**، وهي أسوأ من التنبيهات الإيجابية الخاطئة.(False Positives)
- افهم فلسفة المصدر: هل يفضل الدقة أم الحذر المفرط؟

الخطوة الأولى:

- إذا لم تكن قد انضممت إلى إحدى مراكز **ISACs**أو **ISAOs**، فابدأ الآن للحصول على معلومات مخصصة وموثوقة تتعلق بمجالك.
- كما هو موضح، هذه المنظمات توفر قيمة كبيرة للمساعدة في تحسين فعالية تحليل التهديدات.

منصةMISP

دورها في هذه الدورة:

في هذه الدورة، سيتم استخدام **MISP**كمثال على منصات استخبارات التهديدات. تم اختيار MISP لأنها أصبحت المعيار الفعلي لمنصات استخبارات التهديدات المجانية والمفتوحة المصدر، واكتسبت شهرة كبيرة بين المؤسسات الكبرى خلال السنوات الأخيرة. بالإضافة إلى ذلك، توفر تكاملاً مدمجًا مع **TheHive**، الذي يُستخدم كإدارة أحداث الحوادث(IMS) ، مما يوفر فكرة ممتازة عن مستوى التكامل المطلوب بين أدوات مركز عمليات الأمن.(SOC)

MISPليست مجرد منصة مجانية، بل أداة متكاملة لإدارة استخبارات التهديدات تنافس العديد من الخيارات التجارية. يتسم فريق تطويرها بجهود رائعة في التحديث المستمر وإضافة ميزات جديدة بناءً على مدخلات المجتمع.

أبرز الميزات الرئيسية لـ:MISP

1. **تخزين فعال لمؤشرات التهديدات:(IoC)**
   - تخزين المعلومات التقنية وغير التقنية المتعلقة بالبرمجيات الخبيثة، الحوادث، المهاجمين، والاستخبارات.
2. **الربط التلقائي بين البيانات:**
   - كشف العلاقات بين السمات والمؤشرات المرتبطة بالبرمجيات الخبيثة أو الحملات الهجومية.
   - دعم الربط المتقدم مثل **Fuzzy Hashing**و.**CIDR Block Matching**[11]
3. **نموذج بيانات مرن:**
   - القدرة على التعبير عن الكائنات المعقدة وربطها لتوضيح الاستخبارات، الحوادث، أو العناصر ذات الصلة.
4. **وظائف المشاركة المدمجة:**
   - مزامنة الأحداث والسمات تلقائيًا بين مختلف منصات.MISP
   - خيارات مشاركة مرنة تلبي سياسات المشاركة لكل مؤسسة.
5. **واجهة مستخدم بديهية:**
   - إنشاء، تحديث، والتعاون في الأحداث والمؤشرات بسهولة.
   - التنقل السلس بين الأحداث والارتباطات المرتبطة بها.
6. **تخزين البيانات بطريقة منظمة:**
   - دعم شامل لمؤشرات الأمن السيبراني ومؤشرات الاحتيال في القطاعات المالية.
7. **التصدير والاستيراد:**

---

[11] كتلة (Classless Inter-Domain Routing) CIDR هي طريقة لتجميع عناوين IP ضمن نطاقات فرعية ذات أحجام مختلفة. بدلاً من تقسيم عناوين IPإلى فئات ثابتة، تسمح CIDR بتقسيمها بشكل أكثر مرونة وفقًا لاحتياجات الشبكة. كل كتلة CIDR تمثل مجموعة من عناوين.IP
الكشف عن التهديدات: تستخدم كتل CIDR لتحديد شبكات معروفة بكونها مضيفة للتهديدات. إذا تم رصد حركة مرور متجهة إلى أو قادمة من إحدى هذه الكتل، فإن ذلك يعتبر مؤشرًا محتملًا على نشاط ضار.
حماية الشبكات: يمكن استخدام كتل CIDR لإنشاء قواعد جدار ناري لمنع حركة المرور من أو إلى شبكات معينة.
تحليل السلوك: تساعد مطابقة كتل CIDR في تحليل سلوك المهاجمين وتحديد الأهداف المحتملة.
تبادل المعلومات الاستخباراتية: يتم استخدام كتل CIDR بشكل شائع في تبادل المعلومات الاستخباراتية حول التهديدات بين مختلف المؤسسات والشركات.

- **التصـــدير :**يـــدعم تنســـيقات مثـــل(IDS (Suricata, Snort, Bro ، النصـــوص العاديـــة، CSV، وJSON. و MISP XML و OpenIOC ويمكـــن دمجهـــا مـــع نظـــام منـــع التســـلل على مستوي الشبكة والمستخدم/المضيف وأدوات أخري.
- **الاســـتيراد :**اســـتيراد بالجملـــة، تقـــارير نصـــية، تنســـيقاتOpenIOC ، GFI Sandbox، ThreatConnect CSV، أو.MISP

8. **التكامل مع الأنظمة الأخرى:**
   - واجهـــة API مرنـــة مدمجـــة مـــع مكتبـــة **PyMISP**لإدارة الأحـــداث والســـمات وتحليـــل العينات الخبيثة.
9. **التصنيف والتصنيفات:**
   - تصـــنيف الأحـــداث باســـتخدام مخططـــات محليـــة أو عالميـــة مثـــل التـــي تُســـتخدم مـــن قبـــل **ENISA**أو .**Europol** وهي التي تستخدم بشكل افتراضي فى MISP
10. **مصطلحات الاستخبارات:**
    - ربـــط الأحـــداث مـــع الجهـــات المهـــددة، البرمجيـــات الخبيثـــة، وأطـــر مثـــل **MITRE ATT&CK**.
11. **وحدات التوسعة:**
    - إضافة خدمات جديدة أو استخدام الوحدات المتاحة مسبقًا.
12. **رصد المؤشرات:**
    - جمـــع ملاحظـــات مـــن المنظمـــات حـــول المؤشـــرات المشـــتركة، بمـــا فـــي ذلـــك دعـــم الســـلبيات الكاذبة أو انتهاء الصلاحية.
13. **دعم معيار:STIX**
    - تصدير البيانات بصيغة XML) **STIX**و(JSON، مع دعم صيغة .**STIX 2.0**
14. **الأمان المدمج:**
    - تشفير الإشعارات وتوقيعها باستخدام **PGP**أو .**S/MIME**

MISP ليســـت فقـــط أداة لإدارة المؤشـــرات، بـــل هـــي منصـــة متكاملـــة تســـاعد المؤسســـات علـــى **تخـــزين، تحليـــل، ومشـــاركة** اســـتخبارات التهديـــدات بفعاليـــة، ممـــا يجعلهـــا خيـــارًا متميـــزًا للعديـــد مـــن مراكـــز عمليـــات الأمن.

[1] https://www.misp-project.org/

مصطلحاتMISP

الأحداث:(Events)

- الأحداث هي الكيانات الرئيسية التي يتمحور حولها كل شيء في.MISP
- لكل تقرير تقوم بقراءته، أو برمجية خبيثة تقوم بتحليلها، أو حادث ترغب في تتبعه، يتم إنشاء حدث جديد.
- الأحداث لها أرقام تعريفية فريدة وتعمل كحاويات رئيسية تحتوي على مجموعة من السمات (Attributes).

السمات:(Attributes)

- السمات هي القطع الفردية من البيانات التي يتم تتبعها داخل الحدث.
- تشمل السمات البيانات التقليدية مثل مؤشرات التهديد(hash value، اسم الملف، URL، النطاق، IP)، بالإضافة إلى الروابط إلى مقالات خارجية، نصوص تفسيرية، أو حتى الملفات المرفقة نفسها.
- السمات المتطابقة عبر أحداث متعددة يتم إبرازها لتسهيل الربط والتوافق.
- لكل سمة نوع محدد مثل **md5**، **sha1**، **user-agent**، **email-subject**، أو **mime-type**، مما يوفر تصنيفًا دقيقًا.

ميزات التصنيف في:MISP

1. **Sightings(الرؤى):**
   - وسيلة لتتبع الإيجابيات الحقيقية أو الكاذبة لسمة معينة.
   - تساعد المحللين على تقييم فعالية المؤشرات.
2. **الوسوم:(Tags)**
   - وسيلة إضافية لإضافة سياق إلى الأحداث.
   - تُستخدم لتحديد نوع البيانات أو التصنيف المطلوب بسهولة.
3. **التصنيفات:(Taxonomies)**
   - مجموعات من الوسوم الجاهزة التي تُسهل تصنيف البيانات وفقًا لمعايير معينة.
   - تدعم التصنيفات المعايير القياسية مثل **ENISA**و.**MITRE ATT&CK**
4. **المجرات:(Galaxies)**
   - تضيف مجموعات من الجهات المهددة، الأدوات، أو عناصر الاستخبارات.
   - تساعد في تنظيم المعلومات المرتبطة بجهات التهديد أو الحملات الخبيثة.

استخدام المصطلحات:

- MISPلا يقتصر فقط على ما ستستخدمه في هذه الدورة، بل يقدم العديد من ميزات التصنيف الإضافية مثل **تتبع الرؤى(IOC Sighting Tracking)** ، **التصنيفات(Taxonomies)** ، و**المجرات.(Galaxies)**
- الهدف من هذه المصطلحات والميزات هو مساعدة محللي استخبارات التهديدات على **تصنيف** البيانات بدقة، **وربطها** بأنماط أو مجموعات نشاط يمكن تحليلها لاستنتاجات أعمق.

الخلاصة:

فهم هذه المصطلحات وتطبيقها بشكل صحيح يعزز من استخدام MISP كمنصة قوية لإدارة استخبارات التهديدات في مركز عمليات الأمن.

[1] Terminology from: https://www.circl.lu/assets/files/misp-training/luxembourg2018/misp-training.pdf

نظرة عامة على سير عملMISP

الاستخدام من قبل المحللين:

1. يقوم المحلل بإنشاء حدث جديد.
2. تُضاف جميع المؤشرات، الروابط، الملفات، والملاحظات كسمات.(Attributes)
3. يتم تطبيق الوسوم (Tags) والتصنيفات الأخرى) مثل المجرات.(Galaxies
4. يُراجع الحدث ويمكن نشره إلى مؤسسات أخرى إذا لزم الأمر.

الاستخدام التلقائي عبر أدوات مركز العمليات الأمنية:(SOC)

- تستخدم أدوات مثل **SIEM** و**SOAR** و**IMS** واجهة **API** للبحث عن سمات أو إضافتها إلى الأحداث.
- تقوم الخلاصات المشترك بها بتنزيل بيانات الأحداث الخارجية تلقائيًا.
- عند ظهور أي من المؤشرات في حركة المرور المباشرة، يتم توليد تنبيه.

تفاصيل سير العمل فيMISP

هناك طريقتان رئيسيتان لاستخدام:MISP

1. **التفاعل اليدوي:**

- يقوم المحلل بالتفاعل يدويًا معMISP ، بالبحث عن المؤشرات وإنشاء أحداث جديدة تحتوي على السمات والملاحظات.
- على سبيل المثال، عند اكتشاف حادثة جديدة، يمكن للمحلل إنشاء حدث جديد فيMISP ، وإضافة المؤشرات والمعلومات المتعلقة بالمصدر، وتطبيق الوسوم والتصنيفات المناسبة.

2. **التفاعل التلقائي عبر أدوات SOC:**

- يمكن لبعض الأدوات، مثل **TheHive**، إنشاء أحداث جديدة تلقائيًا في MISP وتعبئة السمات دون تدخل يدوي.
- عند إنشاء حادثة في **TheHive**، يمكن للأداة أن تتصل بـ MISP لإنشاء حدث جديد وإضافة المؤشرات والملاحظات تلقائيًا.

أهمية إضافة المؤشرات فيMISP

حتى إذا كان مركز العمليات الأمنية يحتوي على فريق منفصل لاستخبارات التهديدات، فمن المرجح أنك ستحتاج إلى إدخال المؤشرات في منصة استخبارات التهديدات مثلMISP.

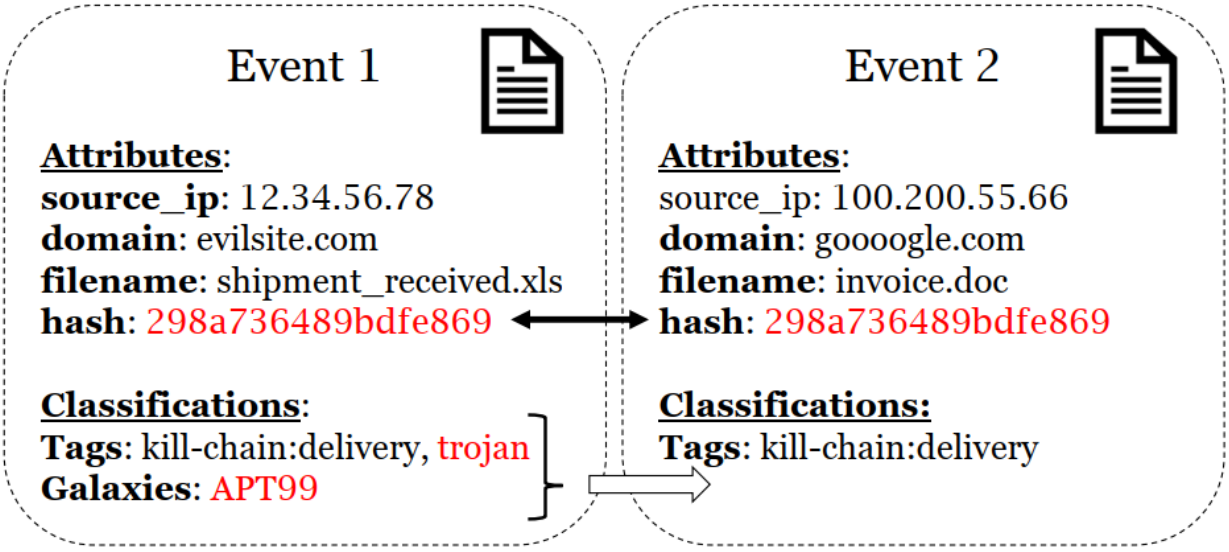
- يتطلب هذا إنشاء حدث جديد، وإضافة الوسوم المناسبة، واستيراد السمات من المقالات أو مصادر الاستخبارات.
- يتم تصنيف الاستخبارات وفقًا لمجموعات أدوات أو جهات تهديد عند الإمكان.

مثال عملي: إضافة حدث يدوي فيMISP

- **الخطوة الأولى :**قم بإنشاء حدث جديد.
- **الخطوة الثانية :**أضف المؤشرات مثل الروابط، الملفات، والعناوين.
- **الخطوة الثالثة :**قم بتطبيق الوسوم أو التصنيفات مثل المجرات.
- **الخطوة الرابعة :**راجع الحدث وتأكد من أن جميع البيانات مصنفة بدقة.

باستخدام هذه الخطوات، يمكن تحسين جمع وتحليل استخبارات التهديدات داخل مركز عمليات الأمن.

أحداث MISP موضحة



أحداث MISP موضحة

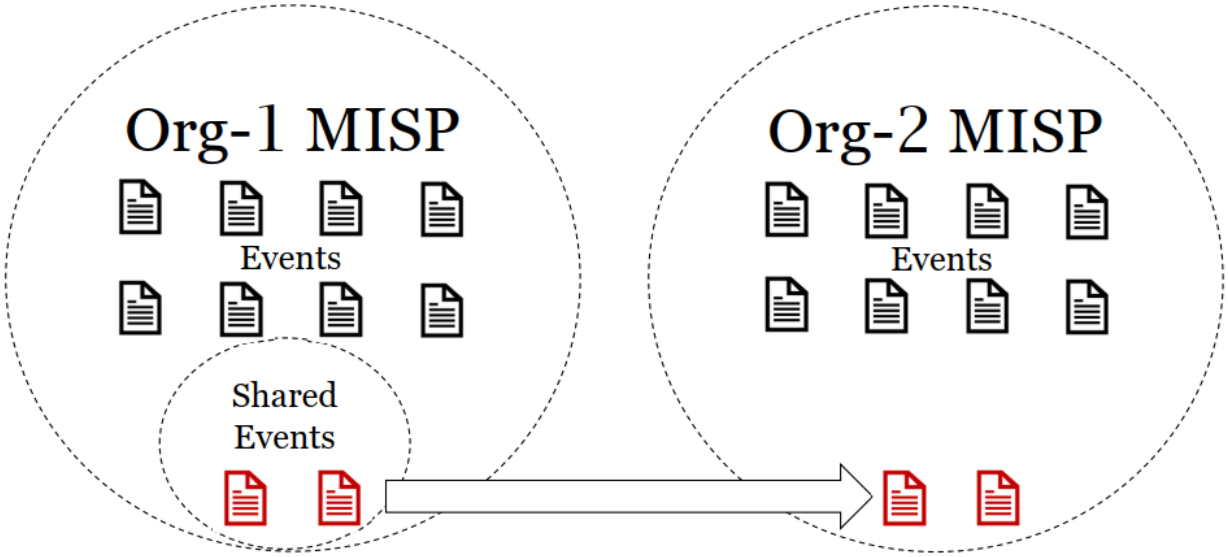
تُظهر هذه الشريحة حدثين يمكن أن يمثلوا روابط تم تلقيها عبر الهجوم الاحتيالي (التصيد). لكل منهما مجموعة من السمات والتصنيفات المرتبطة به. لكن هناك سمة واحدة، وهي **بصمة الملف (File Hash)**، والتي تتطابق بين الحدثين. باستخدام منصة مثل **MISP**، يمكننا التعرف بسهولة على هذه الحقيقة.

عند إدخال سمات الحدث الثاني في النظام، يجب على منصة استخبارات التهديدات أن تبرز أي أحداث أخرى تحتوي على نفس القيم للمؤشرات، مما يسمح لك بربط الحدثين الأول والثاني معًا واستنتاج أنهما من المحتمل أن يكونا جزءًا من نفس الحملة من نفس المهاجم، حتى وإن كانت أسماء الملفات والمصادر مختلفة.

لاحظ أن الحدث الأول قد تم تصنيفه بالفعل كـ **حصان طروادة (Trojan)** من **APT99**. عند إدخال العناصر للحدث الثاني، من المفترض أن يتعرف المحلل على أن هذه البصمة قد تم رؤيتها من قبل ولا يحتاج إلى تكرار العمل الذي تم القيام به لتحديد الحدث الثاني كـ **محاولة أخرى لتوصيل حصان طروادة**، حيث تم تصنيفه بالفعل أثناء الحدث الأول.

ستتمكن أيضًا من نسب البنية التحتية الملاحظة حديثًا (**goooogle.com**) إلى **APT99** مباشرةً بسبب النسبة السابقة.

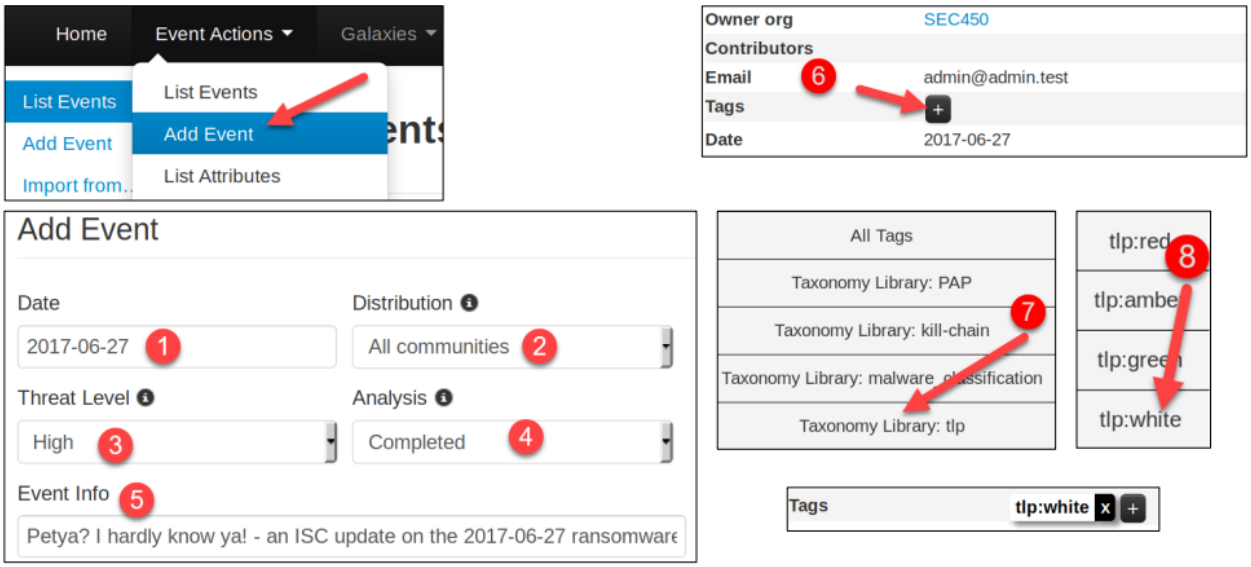
مشاركة MISP موضحة



مشاركة MISP موضحة

تم تصميم **MISP** لمشاركة الاستخبارات، حيث تُعد الاستخبارات المتعلقة بالتهديدات واحدة من العديد من الأنشطة التي تكون أفضل عندما يتم التعاون فيها مع الآخرين! يمكن لكل منظمة تشغل نسختها الخاصة من **MISP** تحديد الأحداث التي ترغب في مشاركتها، وربط نسختها من **MISP** مع الآخرين، مما يسمح بالمشاركة الثنائية للأحداث عبر عدة منظمات.

إنشاء حدث في MISP



إنشاء حدث في MISP

لنأخذ مثالاً على كيفية إنشاء حدث بسيط من منشور ISC في SANS حول **NotPetya**.

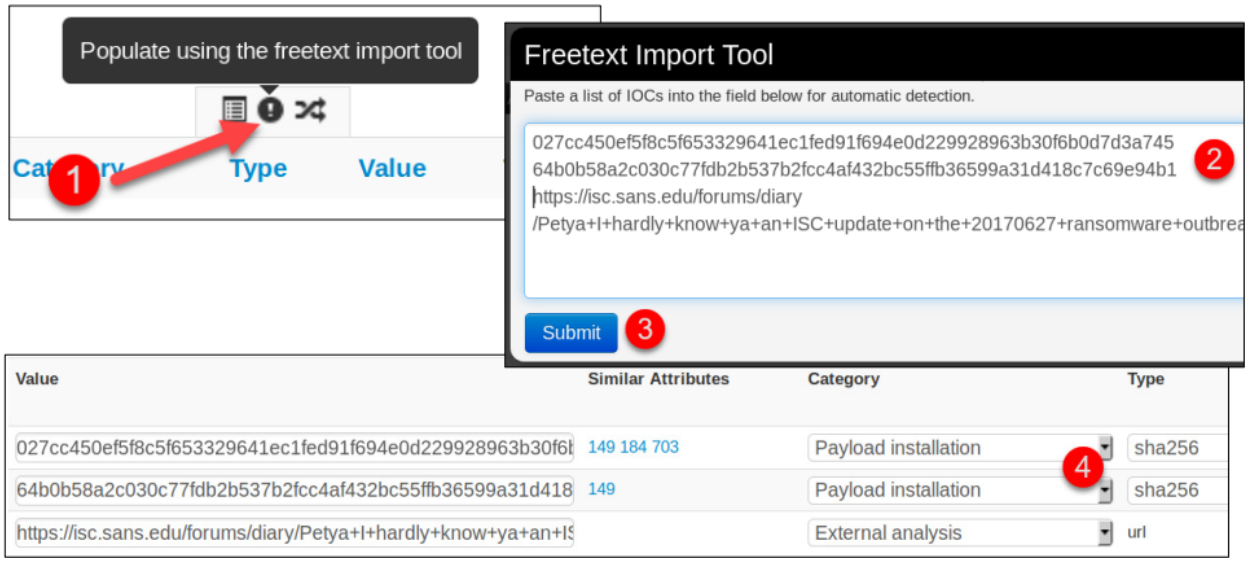
أولاً، نقوم بالنقر على **إجراءات الحدث Event Actions > إضافة حدث** Add Event ونملأ التفاصيل الخاصة بالحدث الذي أنشأناه.
تذكر أن تستخدم تاريخ الحدث، وليس التاريخ الحالي. بالنسبة للعنوان، نستخدم عنوان منشور المدونة نفسه، وهو التقليد المعتاد.

الآن تم إنشاء الحدث الجديد. من قسم البيانات الوصفية، يمكننا الآن إضافة علامة **TLP:WHITE** لأن هذه المعلومات مفتوحة المصدر. اضغط على علامة **+** بجانب العلامات، اختر مكتبة التصنيف TLP ، ثم اختر **tlp:white**.
سيتم إضافة علامة باللون الأبيض إلى قسم العلامات في الحدث. يمكن التحكم في لون كل علامة في ملف التكوين **JSON** المستخدم لإعداد تصنيفات العلامات.

الآن نحتاج لإضافة سمات (Attributes) إلى الحدث...

[1]
https://isc.sans.edu/forums/diary/Petya+I+hardly+know+ya+an+ISC+update+on+the+20170627+ransomware+outbreak/22566/

إضافة سمات الحدث



إضافة سمات الحدث

من أفضل ميزات MISP هي سهولة إضافة معلومات متعددة بأنواع مختلفة. بما أن المقال يحتوي على عدة معلومات مفيدة بأنواع بيانات متنوعة، سنستخدم أداة الاستيراد النصي المجاني لإضافة السمات إلى الحدث.

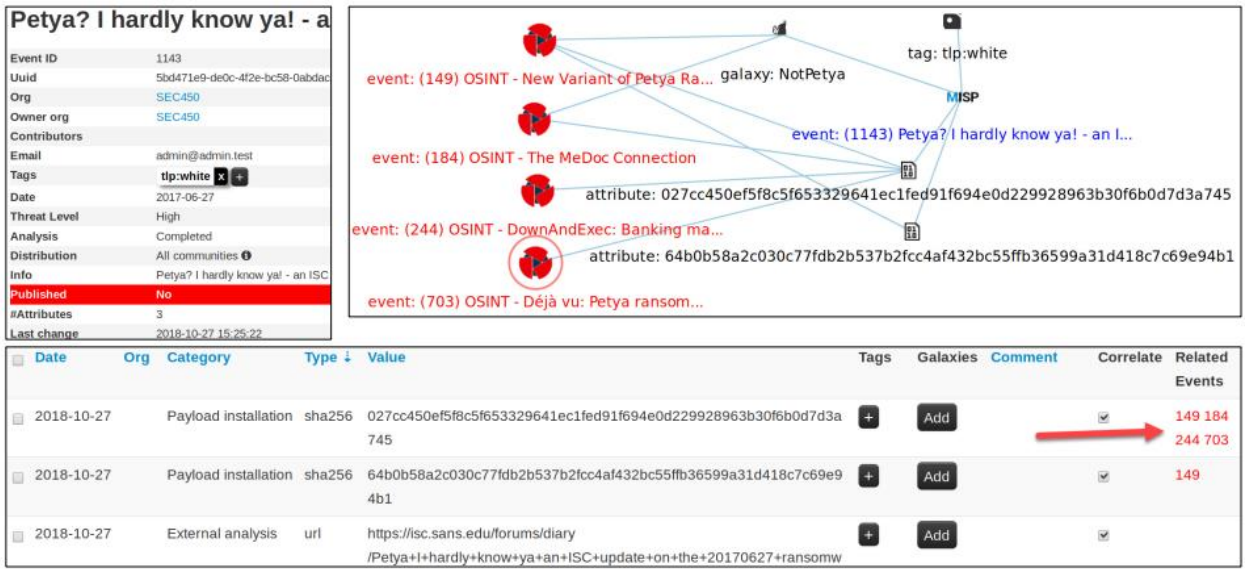
من خلال تحليل مقال **SANS ISC**(الذي تم الرجوع إليه في الأسفل)، هناك العديد من **الهاشات** المرتبطة بـ **NotPetya**التي نرغب في إدخالها في هذا الحدث. يمكن إدخال كل عنصر مهم في سطر منفصل ليتم اكتشاف النوع واستيراده تلقائيًا. بما أننا نرغب أيضًا في حفظ رابط إلى المقالة، يتم إدخاله في أداة الاستيراد النصي المجاني أيضًا (بسبب الطول، تم لف الرابط إلى سطر جديد). بعد إدخال العناصر، نضغط على زر **"إرسال."**

تُظهر الشاشة في الأسفل نتائج اكتشاف النوع بالإضافة إلى فئة السمة والنوع. في هذه المرحلة، نحتاج إلى تعديل الفئات لضمان توافقها مع ما تمثله كل مؤشرات. في هذه الحالة، الهاشات هي هاشات تثبيت الحمولة، والرابط هو التحليل الخارجي للحدث (وليس رابط القيادة والتحكم أو أي رابط ضار آخر). بمجرد التأكد من أن كل شيء صحيح، يمكننا الضغط على زر **"إرسال السمات "** (غير موضح في الصورة) لإتمام تقديم السمات.

المصدر:

https://isc.sans.edu/forums/diary/Petya+I+hardly+know+ya+an+ISC+update+on+the+20170627+ransomware+outbreak/22566/

مثال على ارتباط السمات

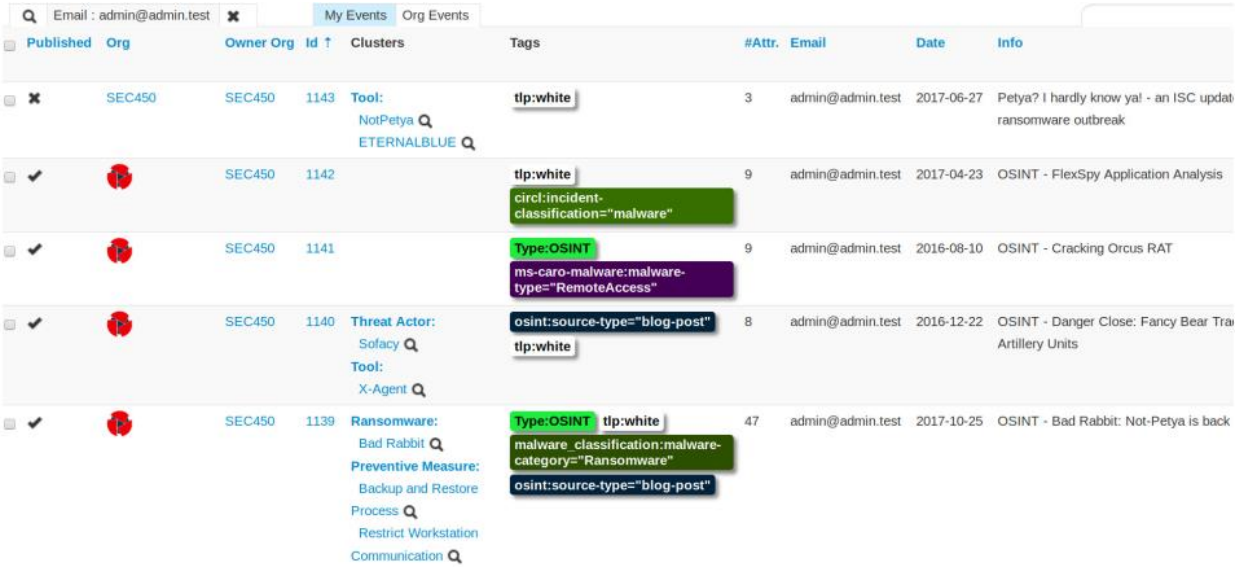


مثال على ارتباط السمات

تُظهر هذه الشريحة مثالاً بسيطًا تم إنشاؤه يدويًا لحدث يحتوي على سمتين—هما **الهاشات SHA256** لعينات **NotPetya**. يظهر مربع الميتاداتا في أعلى اليسار، وقائمة السمات في الأسفل، ومربع الرسم البياني للارتباط في أعلى اليمين. تتيح لنا قائمة السمات ملاحظة وعرض أي سمات مرتبطة بحدث معين، وفي هذه الحالة، كانت قيمتا الهاشات.

هنا تكمن قوة منصة استخبارات التهديدات — بالإضافة إلى جميع السمات التي تم إضافتها محليًا، تم إعداد هذا المثال من **MISP** لسحب بيانات مؤشرات التهديد من **CIRCL OSINT** (مؤشرات التهديد المفتوحة المصدر). يؤدي ذلك إلى تنزيل مئات الأحداث من **MISP** مع سماتها ذات الصلة تلقائيًا. في عرض الرسم البياني للارتباط، وكذلك في عرض السمات، يمكننا أن نرى أن الهاشات المدخلة يدويًا من الحدث #370 كانت موجودة أيضًا في العديد من الأحداث الأخرى من المصدر الخارجي (مرئية من خلال الأيقونة المختلفة في عرض الرسم البياني للارتباط). تم التعرف على هذه السمات التي تظهر عبر العديد من الأحداث تلقائيًا من خلال **MISP**، ومع هذه المعلومات، يمكننا الآن ربط هذا الحدث مع الأنشطة التي تم إدخالها سابقًا بواسطة طرف ثالث. للحصول على سياق إضافي، يمكننا الآن التبديل إلى أحداث **MISP** الأخرى ورؤية السياق حول الهاشات المدخلة من الأحداث 184، 149، 703، و244.

قائمة الأحداث



قائمة الأحداث

إليك لقطة شاشة من الصفحة الرئيسية للأحداث في **MISP**. يمكنك رؤية الحدث الذي تم إدخاله سابقًا عن **NotPetya**، بالإضافة إلى العديد من الأحداث الأخرى التي تم سحبها مسبقًا وتم تصنيفها من خلال المصادر الخارجية. تُظهر عمود "المنظمة" مصدر المعلومات، والذي في هذه الحالة كان **مؤشر التهديد المفتوح** .**CIRCL** يعرض عمود **التجمعات** أي تصنيفات "مجرة" تم تطبيقها، بينما تظهر العلامات أي تسميات من التصنيفات أو غيرها التي تم إرفاقها.

ملخص منصات استخبارات التهديدات

المؤشرات والاستخبارات المُدارة في منصة TIP

- يجب سحب المؤشرات أو إضافتها تلقائيًا من خلال تكامل API مع الأدوات الأخرى.
- تم إنشاء الأحداث يدويًا بناءً على تحليل الأحداث الفردية.

الحوادث المُدارة فيIMS/SIRP

- تصبح جميع التنبيهات عالية الدقة أو التنبيهات الأولية حالات.
- تتم إضافة الحالات إلى قائمة الانتظار وتعيينها للمحللين.
- أداة ستقضي معها الكثير من الوقت، اخترها بحكمة.
- من الناحية المثالية، يجب أن تتكامل مع أطر العمل التلقائية ومنصةTIP.

ملخص منصات استخبارات التهديدات

من خلال القسمين الأخيرين، تناولنا أداتين رئيسيتين تُستخدمان لتنظيم بيانات مركز العمليات الأمنية (SOC):**نظام إدارة الحوادث** ومنصة **استخبارات التهديدات** .تسمح هاتان الأداتان لمراكز العمليات الأمنية بمراقبة جميع الحوادث التي حدثت وربط تفاصيلها معًا للحصول على صورة شاملة للأشياء المتصلة. تتيح هذه القدرة لفرق الأمن الأزرق (Blue Teams) تحسين استخبارات التهديدات الخاصة بهم؛ ومع مرور الوقت، يجب أن يظهر لديك صورة عن نوع التهديدات التي تواجهها، والتكتيكات والتقنيات التي سيستخدمها المهاجمون، وأين يجب أن تركز إنفاقك الدفاعي لمواجهة الهجوم.

التمرين:

تمرين على هذا المقطع من الكتاب هو غرفة على موقع tryhackme فى الرابط التالي وهنا:

https://tryhackme.com/r/room/misp

خريطة الدورة التدريبية

- **القسم الأول :أدوات وعمليات فريق الدفاع(Blue Team)**
- **القسم الثاني** :فهم الشبكة الخاصة بك
- **القسم الثالث** :فهم المضيفين، السجلات، والملفات
- **القسم الرابع** :التقييم والتحليل
- **القسم الخامس** :التحسين المستمر، التحليلات، والأتمتة

أدوات وعمليات فريق الدفاع(Blue Team)

1. مرحباً بك في فريق الدفاع!
2. التمرين 1.0: إعداد الآلة الافتراضية
3. نظرة عامة على مركز العمليات الأمنية(SOC)
4. **مفاهيم الشبكة القابلة للدفاع**
5. الأحداث، التنبيهات، الشذوذ، والحوادث
6. أنظمة إدارة الحوادث
7. التمرين 1.1: نظام إدارة الحوادثTheHive
8. منصات استخبارات التهديدات
9. التمرين 1.2: منصة استخبارات التهديداتMISP
10. **إدارة الأمن والمعلومات (SIEM) والأتمتة**
11. اعرف عدوك
12. ملخص القسم الأول
13. التمرين 1.3: إدارة الأمن والمعلومات باستخدام Elastic Stack

SIEM والأتمتة

في هذه الوحدة

- دور SIEM في الكشف
- تدفق البيانات إلىSIEM
- ما هو الاستخدام؟
- دور SOAR في الاستجابة
- كيف يحسن SOAR فريق الأمن الأزرق

SIEMوالأتمتة

في هذه الوحدة، نستعرض أداتين حاسمتين إضافيتين لعمليات الأمن.

الأولى هي **SIEM**(إدارة معلومات الأمان والأحداث)، وهي المستودع المركزي لجميع السجلات والطريقة الأساسية للبحث والتنبيه والتقارير.

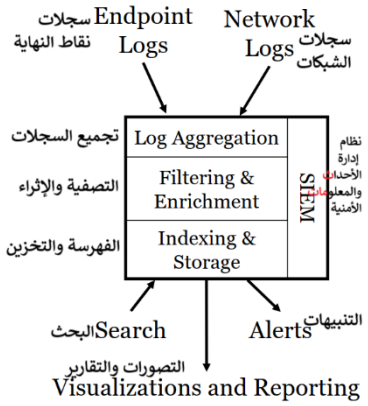
الثانية هي **الأتمتة** أو، إذا كان لديك أداة مخصصة لذلك، **SOAR**(تنسيق الأمان، الأتمتة، واستجابة الحوادث). قد يبدو جهاز SIEM معقدًا في البداية، لذا سيكون الهدف هو تبسيط تشغيله إلى الوظائف الأساسية والنظر إليه من منظور النظام بشكل عام. سنناقش أيضًا حالات الاستخدام لـ SIEM وكيف يمكن للأتمتة مساعدتنا في تنفيذها، بالإضافة إلى العديد من المهام التشغيلية الأخرى الشائعة.

وظيفةSIEM

مهامSIEM :

- **استقبال** جميع بيانات السجلات
- تحليل البيانات بشكل صحيح
- تصفية الأحداث غير المرغوب فيها
- إثراء الأحداث المفيدة ببيانات إضافية
- فهرسة السجلات في قاعدة البيانات
- البحث السريع
- إنشاء التصورات ولوحات التحكم
- التحليل والربط من أجل التنبيه

أحد أهم أدوات مركز عمليات الأمن(SOC)



وظيفةSIEM

علـــى أعلـــى مســـتوى، الهـــدف الأساســـي مـــن **SIEM**هـــو أن يكـــون تجمعًـــا مركزيًـــا للســـجلات يمكننـــا اســـتخدامه بطـــرق مختلفـــة لتمييـــز الظـــروف المريبـــة واكتشـــاف الهجمـــات أو مشـــكلات الامتثـــال. لتحقيـــق ذلـــك، يجـــب أولاً إرســـال جميـــع الســـجلات فـــي البيئـــة إلـــىSIEM ، ثـــم تحليلهـــا وتخزينهـــا. إذا تـــم تنســـيق كـــل ذلـــك بشـــكل صـــحيح، نريـــد أيضًـــا القـــدرة علـــى تصـــفية العناصـــر ذات الاهتمـــام باســـتخدام لغـــة بحـــث مرنـــة، وتصـــوير بيانـــات الســـجلات، وإثـــراء الحقـــول داخـــل ســـجلاتنا لمنحهـــا مزيـــدًا مـــن الســـياق. بالإضـــافة إلـــى ذلـــك، يجـــب أن يتضـــمن SIEM محـــرك تنبيـــه يعمـــل عنـــدما تصـــل الســـجلات ذات الاهتمـــام، كمـــا يجـــب أن يمنح مركز عمليات الأمن القدرة على إنشاء تقارير دورية يمكن توزيعها على أصحاب المصلحة.

تُظهـــر هـــذه الشـــريحة العـــرض العـــام مـــن مســـتوى النظـــام لـــ **SIEM.** فـــي النهايـــة، المـــدخلات إلـــى النظـــام هـــي الســـجلات (وربمـــا معلومـــات أخـــرى مثـــل **NetFlow**إذا كـــان SIEM يدعمـــه)، والمخرجـــات مـــن **SIEM** هـــي التصـــورات، والتنبيهـــات، والتقـــارير، ونتـــائج البحـــث. بالنســـبة لـــ **SIEM**، أكبـــر أجـــزاء اللغـــز هـــي العمليـــات الداخليـــة المطلوبـــة **لتحليـــل، إثـــراء، تصـــفية، وإدارة** العـــدد الهائـــل مـــن الســـجلات التـــي عـــادةً مـــا يـــتم جمعها بواسطة هذه الأجهزة.

ميزاتSIEM

الميزات التي يجب البحث عنها:

لغة استعلام سهلة ومعبرة أنواع متعددة من التصورات واجهة مستخدم مصممة بشكل جيد خيارات تنبيه مرنة يجب أن يسهل تحليل البيانات، بغض النظر عن تنسيق السجل أنواع متعددة من إثراء السجلات وإمكانية الربط	واجهة برمجة التطبيقات (API) لدمج الأدوات من طرف ثالث وثائق جيدة ودعم من البائع وكيل تسجيل عالي الأداء لجمع البيانات توافق مع تنسيقات متعددة للسجلات أداء عالي في الإدخال والفهرسة تحديثات متكررة ونظام "تطبيقات" مرن

ميزاتSIEM

على الرغم من وجود العديد من خيارات **SIEM** المتاحة في السوق، إلا أن بعضها يعتبر أكثر متعة في الاستخدام من البعض الآخر. فيما يلي بعض النقاط الرئيسية التي يجب البحث عنها للحصول على **SIEM** جيد.

النقاط المميزة هي ما يجدها العديد من الأشخاص الأكثر أهمية للسعادة طويلة المدى مع منتج .**SIEM**في النهاية، ما يجب أن يكون لديك هو القدرة على استقبال السجلات في **SIEM**باستخدام مجموعة واسعة من التنسيقات، وتحديد خوارزمية تحليل بسهولة، والقدرة على البحث والتصور والتنبيه حول محتويات تلك السجلات دون الرغبة في سحب شعرك. أفضل الأنظمة تجعل من السهل البحث المرن عبر محتويات السجلات بسرعة فائقة، وتدعم العديد من أنواع التصورات وظروف التنبيه التي تجعل من السهل تحديد الأنشطة الخبيثة بسرعة ودون عناء.

منتجاتSIEM

منتجاتSIEM

فيما يلي بعض الخيارات التي قد تجدها في سوق أنظمة **SIEM.**

تُعد الشركات الكبرى الأكثر شيوعًا، مثل **Splunk**، **QRadar**، **LogRhythm**، و**ArcSight**، من الحلول المهيمنة على الجانب الأيسر، وهي موجودة منذ سنوات عديدة. ومع ذلك، يجب أن تكون على دراية بوجود العديد من الحلول البديلة الأقل شهرة واللاعبين المتخصصين الذين يستهدفون أسواق مقدمي الخدمات الأمنية المُدارة والشركات الصغيرة والمتوسطة الحجم.

اختيار الحل الأمثل

عند اختيار حل **SIEM**، تأكد من الحصول على تجربة عملية مباشرة مع المنتج لتقييم مدى ملاءمته لاحتياجاتك. قم بتجربة عمليات مثل استيعاب السجلات، إعداد الوكلاء، تنفيذ عمليات البحث والتصور، إنشاء تنبيهات نموذجية، والتحقق من القدرات الأخرى. في حين أن الميزات قد تبدو متشابهة على الورق، إلا أن التنفيذ الفعلي يمكن أن يختلف بشكل كبير، وكما يُقال: "التفاصيل هي مفتاح النجاح."

كما هو الحال دائمًا، تعامل مع وعود البائعين بحذر. معظم البائعين لن يذكروا نقاط الضعف في منتجاتهم، لذلك تأكد من سؤالهم عن مقارنة منتجاتهم بالمنتجات المنافسة. استفسر أيضًا عن الشكاوى التي يتلقونها من عملائهم الحاليين أو الميزات التي يتمنون تحسينها.

حالات استخدامSIEM

ما هي حالة استخدامSIEM ؟

- تجيب عن السؤال: "ما الذي يفعله SIEM من أجلنا؟."
- نوع من المخرجات: تقرير، تنبيه، لوحة معلومات، وما إلى ذلك.
- عنصر قابل للتنفيذ يوثقه **SIEM**، مثل:
  - محاولة تسجيل دخول بالقوة الغاشمة.
  - حجم مريب من حركة رفع البيانات من مستخدم.
  - تنزيل يحتمل أن يكون ضارًا.
  - إضافة مستخدم إلى مجموعة المسؤولين.
  - تقديم بيانات اعتماد إلى موقع تصيد احتيالي.

شرح حالات استخدامSIEM

تعتمد فرق الدفاع (Blue Team) على حالات الاستخدام لتعريف ما يريدون من نظام **SIEM** (والأدوات الأخرى) القيام به. على سبيل المثال، قد تكون هناك قاعدة تحليلية مثل: "إذا حدث تسجيل دخول فاشل أكثر من 10 مرات، أرسل تنبيهًا". لكن هذه القاعدة ليست حالة الاستخدام الكاملة، بل جزء منها فقط.

حالة الاستخدام هي نهج أكثر تنظيمًا لتوثيق ما نريد أن يتعرف عليه **SIEM**. إنها تشمل:

- **الشرط نفسه** (مثل تسجيل الدخول الفاشل).
- **السبب وراء الشرط**.
- **الاستجابة المتوقعة**.
- **الاتصال بمتطلبات العمل أو الامتثال**.

أمثلة على حالات الاستخدام

ربما تكون قد سمعت عن أمثلة شائعة لحالات الاستخدام، مثل تسجيل الدخول بالقوة الغاشمة أو التنزيلات الضارة. ولكن التوثيق الكامل لكيفية اكتشاف هذا السلوك وما هي العمليات التي يجب أن تتبع هو جزء لا يتجزأ من حالة الاستخدام.

بينما لا توجد قواعد صارمة وواضحة لما يجب توثيقه، هناك بعض الممارسات المثلى التي سنناقشها في الأقسام التالية.

للمزيد حول حالات الاستخدام الشائعة

لمطاردة مختبري الاختراق: أهم حالات استخدام:SIEM

رابط الفيديو

صياغة واختبار حالة استخدام جديدة

الخطوات الأساسية:

1. تحديد واضح للحالة المراد اكتشافها.
2. تحديد مصادر البيانات التي يمكنها الكشف عن هذه الحالة.
3. اختبار الحالة للتأكد من التعرف الصحيح على الإيجابيات الحقيقية.
4. اختبار الحالة لضمان عدم التعرف على الإيجابيات الخاطئة باستخدام البيانات التاريخية.
5. توثيق التفاصيل في قاعدة بيانات حالات الاستخدام.

إجراء إعادة اختبار دوري:

- **التحقق اليدوي.**
- **اختبارات فريق البنفسجي Purple Team.**
- **أدوات التحقق الأمني المستمر.**

شرح صياغة واختبار حالة استخدام جديدة

عند صياغة حالة استخدام جديدة، يبدأ الأمر بتحديد دقيق للحالة التي تسعى لاكتشافها. بمجرد فهمك لهذه الحالة، حدد مصادر البيانات (سواء كانت بيانات من نقاط نهاية أو من الشبكة) التي تحتوي على الحقول اللازمة للتعرف على الحالة.

الخطوات التفصيلية:

1. **إنشاء التحليل:** استخدم الأداة المناسبة لصياغة تحليل يعتمد على تلك الشروط.
2. **اختبار الهجوم المحاكى:** تأكد من أن التحليل يمكنه التعرف بشكل صحيح على هجوم محاكى.
3. **تحليل البيانات التاريخية:** شغل التحليل على البيانات التاريخية لضمان عدم توليد إنذارات إيجابية خاطئة بشكل غير متوقع.
   (هذه الخطوة مهمة لضمان عدم امتلاء قائمة الإنذارات بأحداث غير هامة).
4. **توثيق الحالة:** إذا أثبت التحليل نجاحه في التعرف على الحالة المطلوبة دون توليد إنذارات كاذبة، يتم توثيق الحالة بكامل تفاصيلها في قاعدة بيانات حالات الاستخدام.

إعادة اختبار الحالة بانتظام

تذكر أن اختبار حالة الاستخدام ليس حدثًا لمرة واحدة. قد تؤثر تغيرات التكوين البيئي أو تحديثات البرامج على كفاءة التحليل.

طرق التحقق الدوري:

- **التحقق اليدوي :**اختبار يدوي للتأكد من استمرار كفاءة الحالة.
- **اختبارات فريق:Purple Team** دمج الاختبارات في التقييمات التي يجريها الفريق لمراجعة الدفاعات.
- **أدوات التحقق الأمني المستمر:** استخدام أدوات تجارية للتحقق الأمني تتيح لك أتمتة التحقق المستمر من الوضع الأمني وكفاءة التحليل.

تطوير حالات الاستخدام

حقول التوثيق في حالة الاستخدام:

• **الاسم** • **الوصف** • **بيان المشكلة** • **الأهداف** • **المتطلبات** • **مصدر البيانات الأساسي** • **مصادر البيانات الثانوية** • **المنطق التحليلي**	• **المراجع** • **الخطوات المقترحة للتحليل** • **خطوات تقليل الإيجابيات الخاطئة** • **الفئات والأطر المرتبطة:** o MITRE ATT&CK / Kill Chain o VERIS • دعم الامتثال/التدقيق • مجموعات التهديدات/إسناد التهديدات

شرح تطوير حالات الاستخدام

أهمية التوثيق الجيد:

توفر المعلومات المذكورة أعلاه لكل قاعدة أو حالة استخدام العديد من الفوائد التي تؤثر إيجابًا على العمليات اليومية لمركز عمليات الأمن.(SOC)

1. **توجيه المحللين:**
   - يساعد التوثيق الجيد المحللين الذين قد لا يكونون على دراية بتنبيه معين على فهم:
     - **ما الذي يجب فعله عند تفعيل القاعدة.**
     - **سبب وجود القاعدة.**
     - **كيفية تحليل الإنذار وتقليل الإيجابيات الخاطئة.**
   - بدون هذا التوجيه، سيضطر المحللون، سواء كانوا جددًا أو ذوي خبرة، إلى التخمين حول الهدف من القاعدة، مما يؤدي إلى استجابات غير متسقة.
2. **تتبع التغطية:**
   - يعتبر التوثيق أداةً حيويةً لتقييم التغطية التي توفرها أدواتك ومصادر البيانات المختلفة.
   - يتيح الإجابة على أسئلة مثل:
     - **"ما الأداة التي تقدم الجزء الأكبر من قدرتنا على الاكتشاف؟"**
     - **"هل لدينا تغطية مناسبة عبر جميع مراحل سلسلة القتل أو تقنيات MITRE ATT&CK؟"**

الإطار العام للتحليل والتغطية

الأطر المرتبطة بحالات الاستخدام:

- **MITRE ATT&CK وKill Chain:** أدوات رئيسية لفهم تقنيات وأساليب المهاجمين ورصد التغطية في مختلف مراحل الهجوم.
- **VERIS:** إطار عمل لتصنيف وتحليل حوادث الأمان.
- **التدقيق والامتثال:** يعزز التوثيق دعم الامتثال للمعايير مثل PCI DSS أو GDPR ويضمن استعدادك لعمليات التدقيق.

التوثيق المنظم يساعدك على:

- تحسين أداء فريق العمل.
- ضمان تغطية شاملة ضد التهديدات.
- تقليل الإيجابيات الخاطئة وتحسين كفاءة التحليل.

قواعد بيانات حالات الاستخدام

تتبع جميع معلومات حالات الاستخدام عن كثب:

- **خيارات التتبع:**
  - أنظمة التذاكر
  - جداولExcel
  - منصاتWiki
  - ملفات نصية
- **تتبع الاتساق مع:**
  - متطلبات الأعمال والامتثال.
  - أطر العمل مثلMITRE ATT&CK.
- التعديلات التي تمت على التحليلات مع مرور الوقت.

فوائد التتبع:

- مساعدة المحللين على فهم:
  - كيفية عمل كل اكتشاف والنظرية الكامنة وراءه.
  - كيفية تفسير البيانات والاستجابة لها.
  - مصادر البيانات المستخدمة.

شرح قواعد بيانات حالات الاستخدام

إدارة حالات الاستخدام:

لضمان تتبع جميع حالات الاستخدام التي تم إنشاؤها بمرور الوقت وتنظيمها بشكل فعال، يلزم إنشاء قاعدة بيانات مخصصة لهذه الحالات. يمكن تنفيذ قاعدة البيانات بطرق متعددة، منها:

- **أنظمة التذاكر :**لدمجها بسهولة مع تدفقات العمل اليومية.
- **جداول :Excel** كحل بسيط وسهل الاستخدام.
- **برامج :Wiki** لتوفير مرجع شامل وقابل للتحديث.
- **ملفات نصية أو قواعد بيانات :**لتلبية الاحتياجات التقنية المحددة.

اختيار الطريقة المناسبة:

- يعتمد الاختيار على الأدوات التي يستخدمها فريقك بالفعل.
- المهم هو أن تكون البيانات التي يتم تتبعها موحدة بين الفرق لضمان الكفاءة والاتساق.
- استخدام برمجيات مرنة وقابلة للتخصيص يمكن أن يعزز من سهولة إدارة الحالات وتوفير رؤية شاملة للتغييرات والقياسات المتعلقة بها على مر الزمن.

مصادر وموارد لتحسين إدارة الحالات

المرجع: دون موردوك

- **كتابه "Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases":**[12]
  - دليل شامل مليء بالتفاصيل الدقيقة المتعلقة بإنشاء حالات الاستخدام وأفضل الممارسات.

[12] يمكنك تحميل الكتاب من هنا: https://drive.google.com/file/d/1ZF8cVfw1NKlOhWUrvVztB1-Fm-iwnrWm/view?usp=sharing

- يقدم موردوك نصائح مبنية على خبرة واسعة في إدارة فرقBlue Team ، مما يجعله مصدرًا قيمًا للمبتدئين والمحترفين.

نهج بسيط باستخدام:Excel

- قدم **ريان فولوك** طريقة مبسطة لإدارة حالات الاستخدام باستخدام Excel في حديثه بعنوان *"Simplified SIEM Use Case Development"*خلال مؤتمر.DerbyCon 2015
- هذا النهج يمثل خيارًا مناسبًا للفرق التي تفضل البساطة والمرونة في تتبع حالات الاستخدام.

الخلاصة:

تتبع حالات الاستخدام بفعالية يعد أساسًا لضمان استجابة أمنية موثوقة ومبنية على بيانات دقيقة. سواء كنت تستخدم أنظمة معقدة أو حلولًا بسيطة، فإن الأهم هو توحيد المعلومات وتحديثها باستمرار لتحقيق أقصى استفادة من قدرات فريقك وأدواته.

[1] Don Murdoch – Blue Team Handbook Volume 2: https://www.amazon.com/Blue-TeamHandbookcondensed-Operations/dp/1726273989/

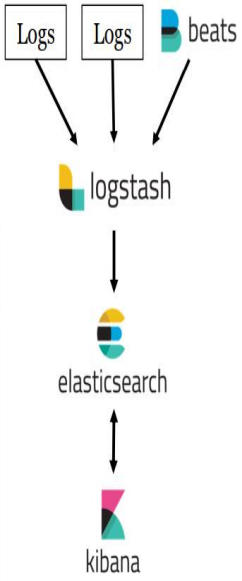
[2] Don Murdoch/SANS Security Operations Summit, 2018 – SecOps, SIEM, and Security Architecture Use Case Development:

https://isc.sans.edu/forums/diary/Petya+I+hardly+know+ya+an+ISC+update+on+the+20170627+ransomware+outbreak/22566/

[3] Ryan Voloch – Simplified SIEM Use Case Development: https://www.youtube.com/watch?v=JvYlOPvMyeA

مختبرSIEM

في جهازك الافتراضي الخاص بالمقرر: حزمةElastic Stack



- يتم استيراد السجلات عبر.Logstash
- تُخزّن السجلات في قاعدة بيانات.Elasticsearch
- يتم البحث عنها وعرضها عبر.Kibana

مختبرSIEM

نظرة عامة علىElastic Stack

في هذا المقرر، سنستخدم **Elastic Stack**كأداة تعمل كـ .SIEM. لا يتطلب الأمر التعمق في كيفية عملها (توفر SANS دورة **SEC455**لمتخصصي(Elastic Stack ، ولكن يمكننا تلخيص فكرتها الأساسية كما يلي:

1. **جمع السجلات:**
   - تُجمع السجلات من مصادر متعددة باستخدام **syslog**أو وكلاء برمجية مثل .**Beats**
   - تُرسل السجلات بعد ذلك إلى أداة تجميع السجلات .**Logstash**
2. **معالجة السجلات:**
   - يقوم **Logstash**بتحليل السجلات، وتنقيحها، وإثرائها بمعلومات إضافية قبل إرسالها إلى **Elasticsearch**للتخزين.
3. **تخزين السجلات:**
   - تعمل **Elasticsearch**كقاعدة بيانات ضخمة، لكنها تختلف عن قواعد البيانات التقليدية التي تستخدم تنسيق الأعمدة والجداول.
   - فيElasticsearch ، يتم تخزين كل سجل كوثيقة بصيغة **JSON**ضمن ما يسمى **"الفهرس"**، وهو شبيه بالجداول في قواعد البيانات التقليدية.
4. **البحث والعرض:**
   - **Kibana**هي واجهة البحث والعرض الأمامية المبنية على الويب. سنستخدمها لاستعراض السجلات المخزنة في.Elasticsearch

المختبر الخاص بالمقرر

- لا حاجة للتعامل مباشرة مع أدوات مثل Beats أو Logstash أو Elasticsearch أثناء هذا المقرر.
- ستقتصر مهمتك على العمل مع Kibana.
- تم الإعداد مسبقًا لاستيراد السجلات إلى Elasticsearch في الجهاز الافتراضي الخاص بالمقرر.

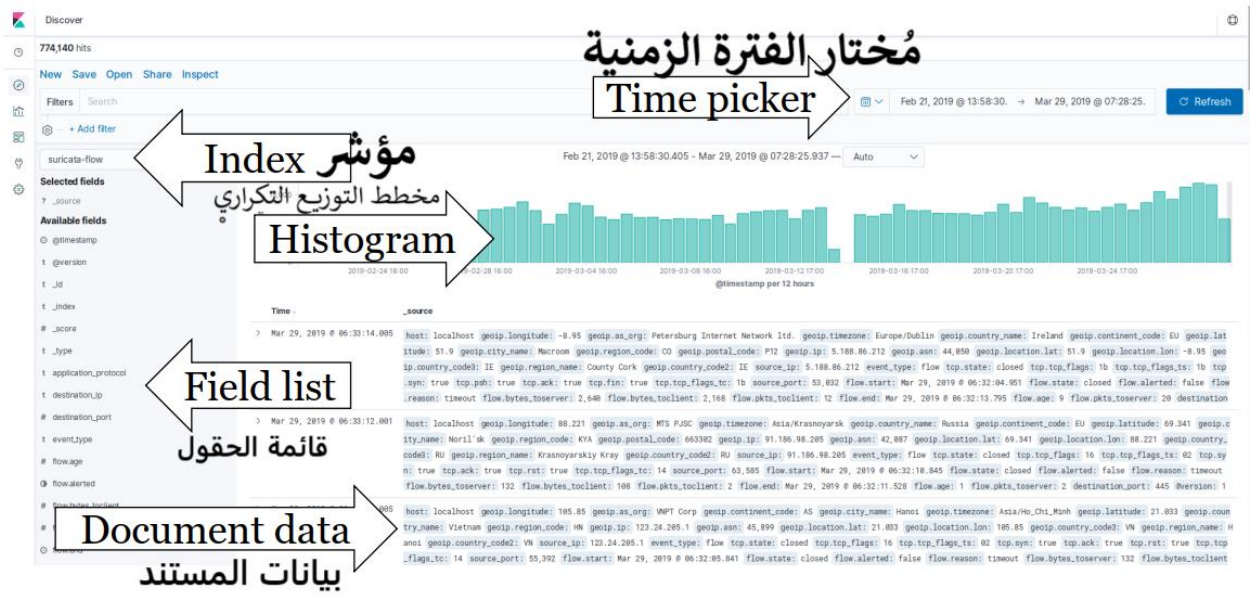
لماذا Elastic Stack ؟

تم اختيار Elastic Stack لأنه يوضح البنية الأساسية لأي نظام SIEM:

- جمع السجلات.
- معالجتها وإثراؤها.
- تخزينها بطريقة قابلة للبحث.
- عرضها باستخدام واجهات مرئية سهلة الاستخدام.

توفر هذه النظرة خلفية لفهم بنية Kibana وكيفية استخدامه في التمارين العملية ضمن هذا المقرر.

البحث باستخدام :Kibana علامة تبويبDiscover



البحث باستخدام :Kibana علامة تبويبDiscover

إجراء البحث في علامةDiscover

للبحث داخل علامة **Discover**، اتبع الخطوات التالية:

1. **تحديد النطاق الزمني:**
   - استخدم محدد الوقت في الزاوية العلوية اليمنى لتحديد نطاق زمني يقيد نطاق السجلات التي يتم البحث فيها.
2. **اختيار الفهرس:**
   - يجب اختيار **نمط فهرس** لتحديد مجموعة السجلات التي سيتم البحث فيها.
   - عادةً، يكون لكل مصدر بيانات (مثل سجلاتWindows ، سجلات الجدران النارية، سجلات برامج مكافحة الفيروسات) فهرس خاص يحمل اسمًا يمكن اختياره من القائمة المنسدلة.
   - إذا كنت ترغب في البحث في جميع السجلات، اختر نمط الفهرس .*
3. **عرض الحقول المتاحة:**
   - بمجرد اختيار نمط الفهرس، ستظهر قائمة بجميع الحقول المتاحة على الجانب الأيسر من الصفحة.
   - بالنقر على أي من هذه الحقول، ستُعرض **أعلى 5 قيم** لهذا الحقل، بالإضافة إلى زر **إضافة** لعرض هذا الحقل كعمود.

- إذا لم تضف أي حقل كعمود، فسيتم عرض الوثيقة بالكامل مع إبراز أسماء الحقول بخط عريض.

4. **استعراض الوثائق:**

- يمكن توسيع أي وثيقة باستخدام المثلث الصغير الموجود على الجانب الأيسر، مما يعرض جميع الحقول داخل السجل الفردي.
- إذا تمت إضافة حقول محددة كأعمدة، فسيتم عرض البيانات من تلك الحقول فقط في قسم البيانات.

تحسين نتائج البحث باستخدام شريط البحث

- يوجد شريط البحث في الجزء العلوي من الصفحة ويمكن استخدامه لتحسين النتائج المعروضة.
- يمكنك إجراء عمليات بحث عن مصطلحات داخل أي حقل أو ضمن حقل محدد، ويمكنك استخدام الرموز البرية **(wildcards)**أو التعبيرات المنتظمة .**(regular expressions)**
- بمجرد تشغيل البحث، ستظهر الوثائق التي تتطابق مع الإطار الزمني ونمط الفهرس المختار فورًا في الرسم البياني الشريطي .**(histogram)**

تحديد نطاق زمني دقيق باستخدام الرسم البياني الشريطي

- إذا كنت ترغب في تحسين نطاق البحث الزمني بصريًا، يمكنك النقر على الرسم البياني الشريطي وتحديد جزء معين لتكبير فترة زمنية محددة تهمك.

ملخص

توفر علامة **Discover**في Kibana أدوات قوية لتحليل السجلات من خلال البحث داخل فهارس محددة وتصفية النتائج بناءً على الحقول أو الفترات الزمنية. تساعد هذه الميزة المحللين في استعراض المعلومات بشكل مبسط وفعال، مع إمكانية التخصيص الكامل للعرض.

أمثلة على لغة الاستعلام فيKibana

بحث مفتوح عن كلمة أو سلسلة نصية

- للبحث عن **"string"**في أي مكان :
  - string
- للبحث في الحقل **response**عن القيم التي تحتوي على :**"string"**
  - response:string

البحث عن القيم في الحقول الرقمية

- للبحث في الحقل **destination_port**عن القيم الأكبر من :**1024**
- destination_port > 1024

البحث عن تطابقات متعددة

- للبحث عن سجلات تطابق الشروط: الحقل **response**يحتوي على **"string"**والحقل **destination_port**يساوي :**80**
- response:string and destination_port:80

البحث عن أي من شرطين

- للبحث عن أحد الشرطين :
  - الحقل **response**يحتوي على **"string"**أو الحقل **destination_port** يساوي :**80**
  - response:string or destination_port:80
  - الحقل **response**يحتوي على القيمة **200**أو :**404**
  - response:(200 or 404)

نبذة عن الأمثلة

هذه الأمثلة تُظهر طرقًا شائعة للبحث عن البيانات داخل Kibana باستخدام لغة الاستعلام. ورغم أنها ليست قائمة شاملة، إلا أنها تغطي غالبية السيناريوهات المطلوبة في هذه الدورة.

تعريف الأتمتة والتنظيم

النقاط الرئيسية

- **الأتمتة** :تُنفذ مهمة محددة.
- **التنظيم** :يربط بين المهام المؤتمتة لتشكيل سير عمل متكامل.
- **الفكرة الأساسية"** :تشغيل كتاب الإرشادات الخاص بك تلقائيًا"!

الفوائد:

- توحيد المهام المرتبطة بالاستجابة (تطبيق كتب الإرشادات).
- تقليل وقت الاستجابة بشكل فوري.
- رفع القدرة على معالجة التنبيهات، مما يقلل من الإرهاق.
- تسريع عملية انضمام الموظفين الجدد.
- التركيز على المهام الأكثر أهمية.
- زيادة رضا المحللين بعد التخلص من الأعمال المتكررة.

شرح مفصل للأتمتة والتنظيم

الأتمتة أصبحت تقنية أساسية في السنوات الأخيرة، بل إنها أصبحت ضرورة للتعامل مع الكم الهائل من البيانات المطلوبة لتوفير دفاعات حديثة. تتلخص الأتمتة في تنفيذ المهام التي كانت تُجرى يدويًا بواسطة برامج أو نصوص برمجية.

أما التنظيم، فهو خطوة أكثر تقدمًا. التنظيم يجمع بين المهام المؤتمتة ويرتبها في سلسلة من الأحداث أو سير عمل يتضمن منطقًا شرطيًا. يمكن تشبيه ذلك بـ"كتب الإرشادات" المستخدمة في أنظمة إدارة الحوادث.(IMS)

أدوات **SOAR** (Security Orchestration, Automation, and Response) هي مثال مثالي على التنظيم، حيث يمكنها تنفيذ خطوات كان من الضروري أن يقوم بها المحللون يدويًا. من خلال الأتمتة والتنظيم، يتم تقليل الزمن المستغرق في تحليل الحوادث وتحقيق كفاءة أعلى في العمل، مما يترك المحللين يركزون على المهام التي تتطلب التفكير البشري العميق.

منصاتSOAR

المنتجات التجارية الموجهة للأمن السيبراني:

• **Swimlane** • **FortiSOAR** • **NetWitness Orchestrator** • **D3 XGEN SOAR**	• **Rapid7 Komand** • **Siemplify (acquired by Google)** • **Splunk SOAR** • **Palo Alto Cortex XSOAR**

أدوات أتمتة سير العمل المجانية (غير مخصصة للأمن):

• **Huginn** • **Airflow** • **المزيد**	• **IBM Node-RED** (nodered.org) • **StackStorm** • **n8n.io**

شرح لمنصاتSOAR

مع تزايد الطلب على الأتمتة، ظهرت فئة منتجات **SOAR**(التنظيم والأتمتة والاستجابة الأمنية) لتلبية هذه الحاجة. بينما ظهرت شركات جديدة في هذا المجال، سارعت فرق المنتجات الحالية إلى إضافة قدرات **SOAR**لمنتجاتها. بعض المنتجات الراسخة اعتمدت على أدوات من شركات **SOAR** أخرى من خلال **إعادة العلامة التجارية** أو الاستحواذ المباشر لتحقيق تقدم سريع.

لا شك أن السباق لتقديم ميزة الأتمتة أصبح واضحًا، ومنصات **SOAR**أثبتت أنها جزء أساسي من هذا الاتجاه. لماذا؟ لأنها ببساطة تقلل من الجوانب المتكررة وغير المفضلة في العمل وتجعلها سريعة وسهلة التنفيذ، مما يؤدي إلى رفع مستوى رضا المحللين!

على الرغم من قلة أدوات **SOAR**المجانية حتى الآن، هناك العديد من أدوات أتمتة سير العمل العامة المجانية التي تشبهها في وظيفتها. على سبيل المثال:

- **IBM Node-RED**: أداة برمجية تعتمد على التدفقات وهي مشابهة جدًا لمنصات **SOAR**، باستثناء أنها لا تحتوي على تكاملات محددة بأدوات الأمن.
- **Cortex**: أداة أتمتة مجانية مدمجة في **TheHive**، تُستخدم لإثراء البيانات القابلة للملاحظة بمعلومات إضافية بضغطة زر.

منصات **SOAR**هي المستقبل، حيث تساعد الفرق الأمنية على تحسين كفاءتها وتقليل الجهود غير الضرورية.

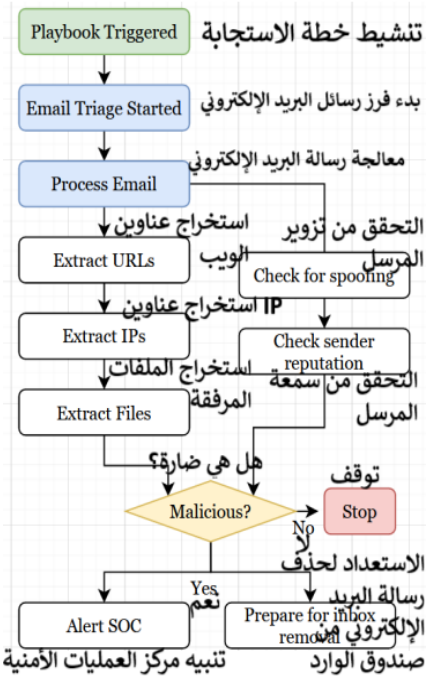
[1] nodered.org

[2] http://meirwah.github.io/awesome-workflow-engines/

القيمة المضافة لمنصاتSOAR

أمثلة على أتمتة المهام الأولية للتحقيق:

- **البريد العشوائي (Spam):** التحقق من السجلات لتحديد نطاق موجة البريد الإلكتروني.
- **استغلال الويب (Web-Exploit):** الحظر التلقائي للنطاقات.
- **الأوامر والتحكم (Command and Control):** إثراء بيانات النطاق باستخدام معلومات من **Virus Total**.
- **اكتشاف الفيروسات:** عزل الجهاز عن الشبكة.
- **التصيد الاحتيالي (Phishing):** فرض انتهاء صلاحية كلمة المرور للمستخدم.
- **الإثراء (Enrichment):** البحث عن DNS السلبي، عناوين IP، معلومات Whois أو GeoIP.
- **التصحيح (Remediation):** إنشاء وإرسال طلب إعادة بناء للنظام إلى مكتب الدعم الفني.



شرح القيمة المضافة لمنصاتSOAR

هناك العديد من السيناريوهات التي يمكن أن تُساهم فيها منصات **SOAR**بشكل كبير. عند مراجعة سيناريوهات العمل المعتادة (Playbooks) والخطوات المطلوبة للتحليل، يتبين أن الكثير من هذه الخطوات لا تتطلب تدخلاً بشريًا ويمكن تنفيذها تلقائيًا باستخدام استدعاء API[13]بسيط.

على أبسط مستوى، يمكن تنفيذ الإجراءات المذكورة أعلاه عن طريق استخراج المعلومات ذات الصلة من تنبيه (مثل مرسل البريد الإلكتروني، اسم النطاق، اسم جهاز الحاسوب، وغيرها)، ثم إجراء استدعاء API مناسب لأحد أدوات الأمان لديك.

تتيح منصات **SOAR**تنفيذ العديد من هذه الإجراءات الأولية بشكل متسلسل ومنسق داخل واجهة مستخدم رسومية (GUI) منخفضة أو خالية من الكود. كل خطوة في سير العمل تمثل مهمة يجب تنفيذها ويمكن أن تتضمن شروطًا منطقية على المخرجات لتحديد الخطوة التالية.

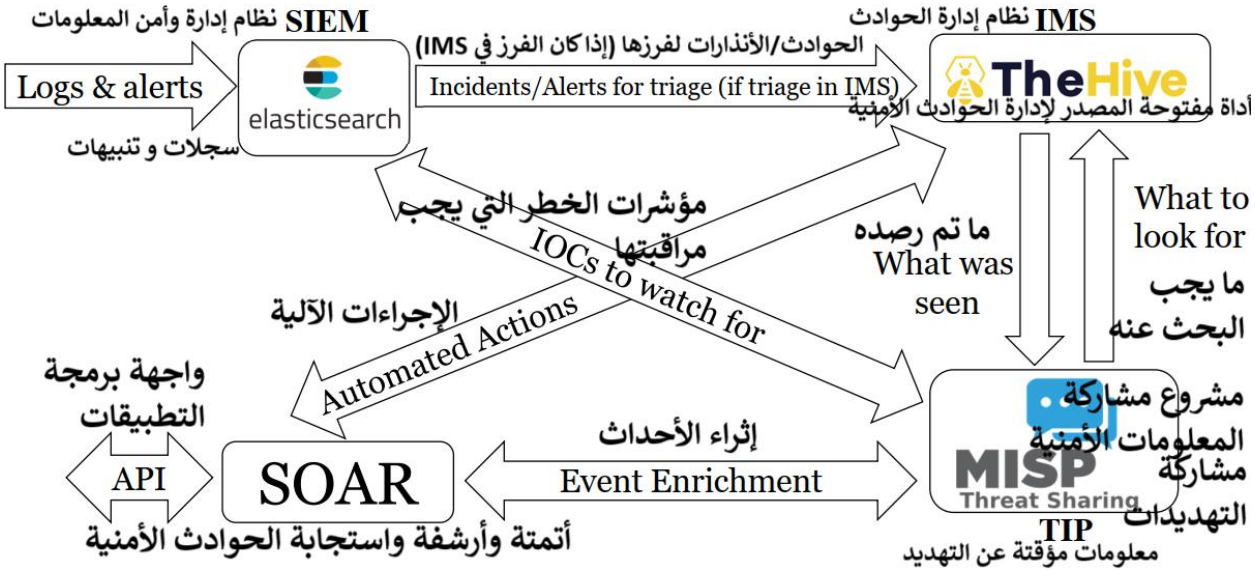
تعمل هذه الأدوات على تخفيض الحاجز اللازم للأتمتة، حيث أن العديد من المحللين ليسوا خبراء في البرمجة. بينما تتطلب كل خطوة إعداد المدخلات والمخرجات والمتغيرات الرئيسية، فإن التعليمات البرمجية المخصصة اللازمة لإتمام هذه المهام تكون أقل بفضل الإجراءات المسبقة الإعداد المدمجة في المنصة.

من خلال **SOAR**، يتم تسريع العمليات الأمنية، تحسين الكفاءة، وتقليل الجهود اليدوية المتكررة، مما يسمح للمحللين بالتركيز على التهديدات الأكثر أهمية .

---

[13] API هي اختصار لـ Application Programming Interface، وهي عبارة عن مجموعة من القواعد والروتينات والواجهات التي تسمح لتطبيقين مختلفين بالتواصل والتفاعل مع بعضهما البعض وتبادل البيانات. تخيلها كواجهة برمجة تتيح للمطورين بناء تطبيقات جديدة أو دمج وظائف تطبيقات موجودة بسهولة وفعالية.
مثال بسيط: عندما تستخدم تطبيق الطقس على هاتفك، فإن هذا التطبيق يتصل بـ API خدمة الطقس للحصول على البيانات الحالية والتنبؤات، ثم يعرضها لك بطريقة سهلة القراءة.
ببساطة، الـ API هي وسيط يتيح للتطبيقات المختلفة التحدث مع بعضها البعض.

تجميع أدوات مركز عمليات الأمن معًا



تجميع أدوات مركز عمليات الأمن معًا

على مدار الأقسام السابقة، ناقشنا العديد من الأدوات مثل:

- **IMS (SIRP)**
- **TIP**
- **SIEM**
- **SOAR**

الآن، بعد أن فهمنا دور كل أداة على حدة، تعرض هذه الشريحة نظرة عامة على المستوى العالي لكيفية تكامل جميع هذه الأدوات معًا لتشكيل صورة كاملة لعمليات الأمن السيبراني.

بالطبع، لا تتضمن هذه الصورة كل التفاصيل، وقد تكون هناك بعض الاختلافات البسيطة حسب البنية المستخدمة. الهدف الأساسي من هذا المخطط هو توضيح التفاعلات الرئيسية وتدفق البيانات بين كل نظام.

على هذا المستوى، من المهم فقط أن نفهم ما يقوم به كل أداة، ونوع المعلومات التي يجب تبادلها بين الأدوات لتمكينها من أداء وظائفها بشكل فعال، ويفضل أن يتم ذلك بطريقة مؤتمتة قدر الإمكان.

هذا التكامل بين الأدوات المختلفة يعزز كفاءة مركز عمليات الأمن ويساعد في بناء استراتيجية متماسكة للتعامل مع التهديدات الأمنية المتطورة.

معلومات أخرى: تخزين البيانات غير المهيكلة وقاعدة بيانات الأكواد

للبيانات غير المهيكلة وشبه المهيكلة:

لإدارة باقي المعلومات في مركز عمليات الأمن(SOC) ، تحتاج إلى مستودع عام لتخزين الوثائق غير المهيكلة أو شبه المهيكلة، مثل:

- مواد التوظيف.
- معلومات التدريب.
- العروض التقديمية التي يتم تطويرها داخل الفريق.

للأكواد والبيانات المهيكلة:

بالنسبة للأكواد والمعلومات التي تتطلب التحكم في الإصدارات عبر الزمن، فإن استخدام أدوات مثل Gitأو SharePoint شائع. هذه الأدوات توفر بيئة منظمة لحفظ الأكواد والملفات التي تحتاج إلى التتبع المستمر.

مفاتيح النجاح في تخزين المعرفة والأكواد:

1. **التعاون في الوقت الفعلي:** أدوات تسمح للفرق بتحرير المحتوى بشكل مشترك وسريع.
2. **بحث سهل وسريع:** إمكانية الوصول إلى المعلومات بسرعة من خلال البحث.
3. **التحكم في الإصدارات:** الاحتفاظ بسجل للتغييرات وإمكانية التعليق عليها.
4. **المزامنة التلقائية:** ضمان أن التحديثات تنعكس فورًا لجميع المستخدمين.
5. **سهولة الاستخدام:** أدوات بواجهة استخدام بسيطة ومباشرة لجعل الموظفين يرغبون في استخدامها.
6. **دعم النصوص الغنية والصور:** إدراج النصوص والصور بسهولة مع التنسيق المناسب.
7. **التنبيهات:** الإشعارات عند حدوث تغييرات على الوثائق.

اختيار الأدوات المناسبة:

- **OneNote:** أداة شائعة نظرًا لسهولتها ودعمها للتعاون الفوري أثناء الاجتماعات. كما أنها توفر هيكلة بسيطة للملاحظات مع صفحات جديدة لكل اجتماع أو فترة زمنية.
- **Markdown Wikis مثل(HackMD):** توازن جيد بين التنسيق وسهولة الاستخدام، مع دعم الكتابة التعاونية.
- **SharePointأو:GitHub** لإدارة الأكواد والمستندات التي تتطلب تحكمًا دقيقًا في الإصدارات.

أهمية البساطة:

الأداة المثالية هي التي تكون سهلة بما يكفي لتحفيز الفريق على استخدامها باستمرار. إذا كانت معقدة أو مثقلة بالقيود، فقد يتجنب الفريق إدخال المعلومات بانتظام، مما يعيق الهدف الأساسي من وجود قاعدة بيانات للمعرفة والأكواد.

ملخص نظام إدارة الأحداث والمعلومات الأمنية (SIEM) والأتمتة

المهام الأساسية لنظام:SIEM

1. **البحث، التصور، والتنبيه عن المعلومات المسجلة:**
   - يجب فهم البيانات المتاحة وكيفية قراءتها بفعالية.
2. **استخدام منصة معلومات التهديدات:(TIP)**
   - تُستخدم لتخزين معلومات التهديدات.
   - يعمل كل من SIEM ونظام إدارة الحوادث (IMS) على استعلام أو إضافة معلومات إلى القوائم.
3. **التعامل مع التنبيهات:**
   - تتحول التنبيهات إلى حوادث يتم تتبعها في نظام إدارة الحوادث أو منصة الاستجابة الأمنية.(SIRP)
   - يتم تعيين الحالات إلى المحللين الذين يتبعون أدلة التشغيل لتحليلها.
4. **دور SOAR في الأتمتة:**
   - يسهل عملية الأتمتة، مما يقلل من زمن الاستجابة.
   - يقوم بجمع السياقات على الفور وإثراء البيانات.

ملخص الأتمتة ونظام SIEM في مراكز عمليات الأمن:(SOC)

تناولت هذه الفقرة الأدوات المختلفة وكيفية تكاملها لجعل عمليات مركز الأمن (SOC) أكثر كفاءة. خلال هذا الفصل، سيتم استخدام هذه الأدوات لتنفيذ التحقيقات وتقديم رؤى ملهمة لتحسين العمليات.

إذا كنت تملك هذه الأدوات ولكنها غير مترابطة أو لا تتفاعل بالطريقة المثلى، فيجب التفكير في كيفية تحسين تدفق البيانات بينها لتعزيز سرعة الاستجابة وتحسين العمل اليومي!

خريطة الدورة التدريبية

- **القســـــم الأول :أدوات وعمليـــــات فريق الدفاع(Blue Team)**
- **القســـم الثـــاني** :فهـــم الشـــبكة الخاصة بك
- **القســـم الثالـــث** :فهـــم المضـــيفين، السجلات، والملفات
- **القسم الرابع** :التقييم والتحليل
- **القســـم الخـــامس** :التحســـين المستمر، التحليلات، والأتمتة

أدوات وعمليات فريق الدفاع(Blue Team)

1. مرحباً بك في فريق الدفاع!
2. التمرين 1.0: إعداد الآلة الافتراضية
3. نظرة عامة على مركز العمليات الأمنية(SOC)
4. **مفاهيم الشبكة القابلة للدفاع**
5. الأحداث، التنبيهات، الشذوذ، والحوادث
6. أنظمة إدارة الحوادث
7. التمرين 1.1: نظام إدارة الحوادثTheHive
8. منصات استخبارات التهديدات
9. التمرين 1.2: منصة استخبارات التهديداتMISP
10. إدارة الأمن والمعلومات (SIEM) والأتمتة
11. **اعرف عدوك**
12. ملخص القسم الأول
13. التمرين 1.3: إدارة الأمن والمعلومات باستخدام Elastic Stack

في هذا الفصل

لإقامة دفاع قوي، يجب أن نفهم عدونا!

"إذا كنت تعرف عدوك وتعرف نفسك، فلن تخشى نتيجة مئة معركة. إذا كنت تعرف نفسك ولكن لا تعرف عدوك، فمع كل انتصار تحققه، ستعاني هزيمة. أما إذا كنت لا تعرف نفسك ولا عدوك، فستُهزم في كل معركة".

—صن تزو، *فن الحرب*

في هذا الفصل

قد تكون سمعت هذا الاقتباس مرارًا وتكرارًا، لكن هناك سبب وجيه لذلك - إنه صحيح تمامًا. النصيحة الخالدة التي قدمها صن تزو تنطبق مباشرة على الدفاع السيبراني. كما ناقشنا في مجال استخبارات التهديدات، يجب أن نفهم المهاجم إذا أردنا إيقافه.

سيتناول هذا الفصل بعمق من هو العدو، وأسباب هجومه، وأساليبه التي يواجهها مركز عمليات الأمن (SOC) على مر الزمن.

من يهاجمنا؟

مجموعات مدعومة من الحكومات

- تتضمن قوائم الاتهام الدول التالية: روسيا، الصين، الولايات المتحدة، المملكة المتحدة، إيران، كوريا الشمالية، فيتنام، فرنسا، الهند، إسرائيل، سوريا والمزيد.

برامج الفدية والجريمة المنظمة

- REvil
- Conti
- DarkSide
- CLOP
- Netwalker
- Magecart

من يهاجمنا؟

هناك العديد من المجموعات المختلفة التي تقف وراء موجة الهجمات السيبرانية. من بين أبرز الجهات التي سنناقشها أولاً :**المجموعات المدعومة من الحكومات** و**الجريمة المنظمة**.

المجموعات المدعومة من الحكومات

رغم أنها ليست الأكثر عددًا في الهجمات، إلا أن الدول تُعد الأكثر قدرةً، والأكثر تخفّيًا، والأشد ضررًا. قائمة الدول المتهمة بشن الهجمات تتزايد باستمرار، وأدواتها وتقنياتها الجديدة تبهر المراقبين بشكل دائم. تشتهر هذه المجموعات باستخدام الثغرات غير المعروفة (***Zero-Days***[14]) والجذور الخفية (***Rootkits***[15]) وأسلوب الهجمات عالية التعقيد التي غالبًا ما تُغير التصورات حول ما هو ممكن في الدفاعات.
لحظة فارقة في تتبع الهجمات كانت في تقرير APT1 [16]عام 2012، ومنذ ذلك الحين استمر مقدمو الخدمات الأمنية في نشر تفاصيل الحوادث وربطها بالمجموعات الهجومية التابعة لهذه الدول.

برامج الفدية والجريمة المنظمة

شهدت السنوات الأخيرة، خاصة منذ بداية الجائحة، تحولًا كبيرًا في الجرائم الإلكترونية نحو **برامج الفدية** وأساليب الابتزاز المزدوج. في هذا الأسلوب، تقوم المجموعة بحجز بيانات الشركة وطلب

---

[14] هجوم "يوم الصفر (Zero-day) "هو هجوم سيبراني يستغل ثغرة أمنية في برنامج أو نظام تشغيل لم يتم اكتشافها أو إصلاحها بعد من قبل المطورين .بمعنى آخر، هي ثغرة جديدة تمامًا لا يوجد لها تصحيح متاح.

[15] الجذور الخفية **(Rootkit)** هي برنامج خبيث مصمم للاختباء داخل نظام التشغيل، مما يمنحه مستوى عالٍ من الامتيازات والوصول إلى النظام. تخيلها كباب خلفي يسيطر على جهازك دون علمك.

[16] **APT1**هي مجموعة هجمات سيبرانية متقدمة ومستمرة (Advanced Persistent Threat) تم تحديدها على أنها وحدة 61398 التابعة لجيش التحرير الشعبي الصيني. تعتبر APT1 واحدة من أبرز مجموعات الهجمات السيبرانية التي تم الكشف عنها، وقد نفذت حملات تجسس إلكتروني واسعة النطاق ضد مجموعة متنوعة من الضحايا منذ عام 2006 على الأقل.

فديـــــة لفـــــك التشـــــفير، وتزيـــــد التهديـــــد بنشـــــر البيانـــــات إذا لـــــم يـــــتم دفـــــع الفديـــــة. تظهـــر هـــذه المجموعـــات وتختفـــي مـــع اعتقـــال أفرادهـــا وتشـــكيل مجموعـــات جديـــدة. علـــى ســـبيل المثـــال، أظهـــرت لقطـــات فيـــديو مـــن جهـــاز الأمـــن الفيـــدرالي الروســـي (FSB[17]) عمليـــة اعتقـــال لأعضـــاء يُـــزعم أنهـــم ينتمون إلى مجموعة REvil في 14 يناير 2022.

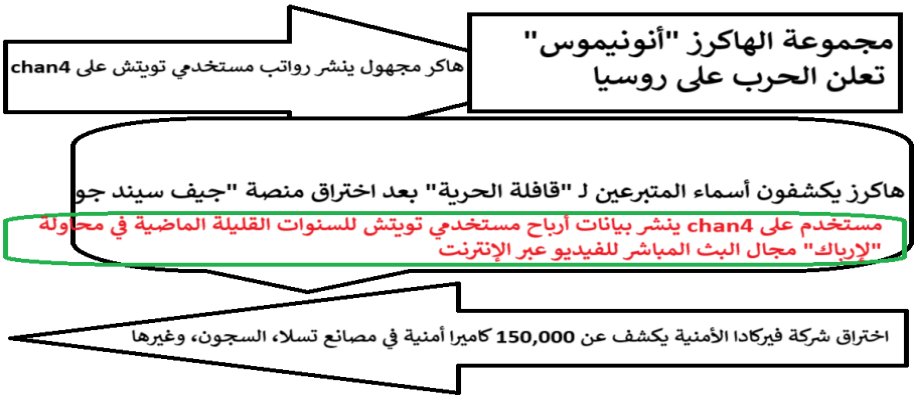
[1]: MITRE ATT&CK: Groups: https://attack.mitre.org/groups/
[2]: Reuters: Russia arrests REvil operators: https://www.reuters.com/technology/russia-arrests-dismantles-revil-hacking-group-us-request-report-2022-01-14/

[17] **خدمة الأمن الفدرالية الروسية (FSB)** هي الوكالة الأمنية الرئيسية في روسيا، وهي الوريث الرئيسي للجهاز السري السوفيتي السابق، الكي جي بي. تأسست الـ FSB في عام 1995 بعد تفكك الاتحاد السوفيتي، وتتولى مجموعة واسعة من المهام

الهاكتيڤيزم (الاختراق من أجل الأيديولوجيا)

الأهداف الشائعة:

- هجماتDDoS
- تغيير محتوى المواقع
- سرقة البيانات ونشرها
- نشر معلومات شخصية (Doxing)
- تدمير السمعة



الهاكتيڤيزم (أيديولوجية الاختراق)

من الجهة المقابلة، نجد مجموعات أو حتى أفراد أقل تنظيمًا يندرجون تحت مظلة **الهاكتيڤيزم** – الأشخاص الذين يسعون لإيصال رسالة أيديولوجية أو سياسية من خلال الاختراقات. **Anonymous** و **LulzSec** هما من أبرز المجموعات في هذه الفئة في الآونة الأخيرة. إذا كنت قد شاهدت المسلسل الأمريكي "Mr. Robot" (وهو شيء يجب أن تشاهده إذا كنت في هذه الدورة)، فهذه هي المجموعة التي يتمثل فيها."FSociety" تشتهر هذه المجموعات بهجمات واسعة النطاق بدوافع متنوعة. من الأمثلة على ذلك "OpRussia" التي قادتها مجموعة Anonymous خلال غزو روسيا لأوكرانيا في 2022، وهجمات أخرى مثل اختراق شركة **Verkada** في 2021 بسبب احتجاجات على المراقبة الجماعية. تقدم Verkada كاميرات مراقبة لعدد من المنظمات مثل **Cloudflare** و **Tesla** والمستشفيات والمدارس والسجون والمزيد.

تُعرف هذه المجموعات (وأحيانًا أفرادها فقط) بصعوبة تحديد هويتهم، وقد يشنون هجماتهم دون سابق إنذار.

أولئك الذين يحاولون تتبع المعلومات الاستخباراتية حول الهاكتيڤيزم غالبًا ما يضطرون إلى التسلل إلى أماكن تواجدهم على الويب المظلم[18]، الدردشات المشفرة أو المنتديات، وغيرها من الأماكن الصعبة الوصول إليها. إذا كنت محظوظًا، قد تكون خططهم متاحة أو في الحالات الأكثر تطرفًا يتم الإعلان عنها علنًا على وسائل التواصل الاجتماعي. لهذا السبب، من الجيد أن يكون هناك شخص يراقب هذه الأماكن إذا كنت تتوقع أن تواجه هجمات أيديولوجية على مؤسستك.

[1]: OpRussia Video on YouTube: https://www.youtube.com/watch?v=kcb2yudJ29c
[2]: Verkada Hack - The Verge: https://www.theverge.com/2021/3/19/22339625/tillie-kottmann-swiss-hacker-verkada-charged-usgovernment-verkada

---

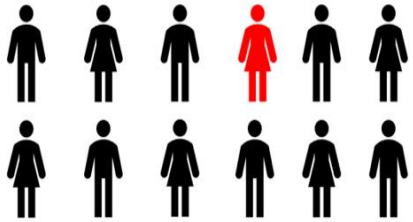
[18] الويب المظلم، أو الدارك ويب، هو جزء من الإنترنت لا يمكن الوصول إليه عبر محركات البحث التقليدية مثل جوجل .هو عبارة عن شبكة من المواقع والخدمات التي تعمل على إخفاء هوية المستخدمين، مما يجعلها مكانًا مثاليًا لأنشطة غير قانونية.

من يهاجمنا؟ القراصنة المأجورون والمهاجمون الداخليون

القراصنة المأجورون:

- بيع الوصول إلى المنظمات المخترقة
- "الفدية كخدمة"
- "الاستغلال كخدمة"
- قد يتعاونون مع مجموعات من أي نوع

المهاجمون الداخليون:



- جني الأموال
- سرقة الملكية الفكرية
- تدمير سمعة المنظمة

من يهاجمنا؟ القراصنة المأجورون والعاملون الداخليون الخبثاء

إلى جانب المجموعات التقليدية مثل الدول القومية والجريمة المنظمة، هناك أيضًا **القراصنة المأجورون** - وهم أفراد مستعدون لفعل أي شيء يُطلب منهم مقابل المال المناسب - وأخيرًا **العاملون الداخليون الخبثاء** .هذه الفئات الثلاث تمثل تهديدات تختلف كثيرًا عن الأنواع التي تمت مناقشتها سابقًا.

القراصنة المأجورون

ليسوا مجموعة محددة جيدًا بل هو مصطلح شامل يشير إلى الأفراد أو مشغلي الشبكات المصابة وغيرهم من المهاجمين الذين يعملون بأسلوب أشبه بـ "عمل تجاري بين القراصنة."

- قد يُدير هؤلاء القراصنة حملات تصيد كبرى لجمع بيانات الأجهزة المخترقة ثم بيعها لأعلى مزايد.
- توجد أيضًا مجموعات تقدم خدمات "الفدية كخدمة"، حيث يبيعون حلولاً جاهزة تمامًا لإدارة حملات الفدية.

العاملون الداخليون الخبثاء

هؤلاء هم الموظفون الذين يشعرون بالسخط أو يجدون أنفسهم في صراع مع الشركة، وقد يلجؤون إلى:

- تسريب معلومات سرية.
- سرقة الأموال.
- إحداث اضطرابات بعد مغادرتهم العمل.

مثـــال: حادثـــة بـــارزة تتعلـــق بموظـــف داخلـــي اســـتخدم كلمـــة مـــرور نظـــام SWIFT (لنقـــل الأمـــوال بـــين البنـــوك) لســـرقة مبلـــغ 1.8 مليـــار دولار مـــن بنـــك البنجـــاب الـــوطني فـــي الهنـــد، ممـــا تســـبب فـــي هجـــوم مـــدمر للغاية! تُعتبر مثل هذه الأحداث "أحداث البجعة السوداء"، حيث تكون نادرة وصعبة التوقع.

التعامل مع التهديدات الداخلية

لـــدينا برمجيـــات يمكنهـــا المســـاعدة فـــي مراقبـــة نشـــاط المـــوظفين وتنبيـــه مركـــز العمليـــات الأمنيـــة (SOC) إذا ظهر أي نشاط غير عادي. تشمل هذه الأدوات:

- **برامج منع فقدان البيانات.(DLP)**
- **تحليل سلوك المستخدم والكيانات.[19](UBA/UEBA)**

لكـــن، غالبًـــا مـــا تُعـــاني هـــذه الأدوات مـــن معـــدلات إنـــذارات كاذبـــة مرتفعـــة حتـــى يـــتم ضـــبطها بشـــكل صـــحيح لتناســـب البيئـــة. بالإضـــافة إلـــى ذلـــك، قـــد تكـــون لهـــا تبعـــات قانونيـــة تختلـــف حســـب الدولـــة، لـــذلك يُنصـــح بالتشاور مع المحامين قبل تنفيذها.

مصادر إضافية:

1. خدمات الفدية كخدمة
2. التعامل مع التهديدات الداخلية :دروس من الهند

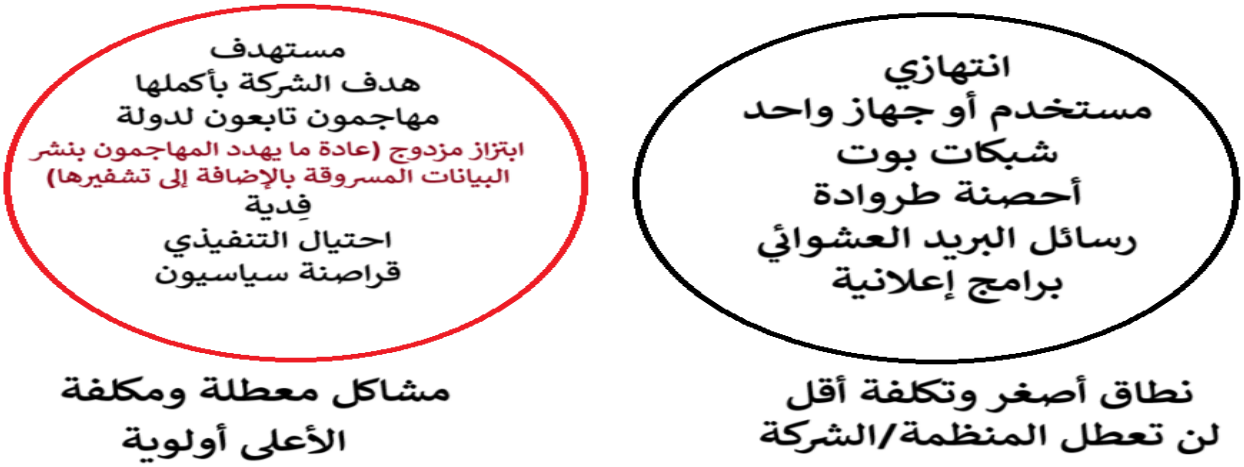
[19] **تحليل سلوك المستخدم والكيانات (UBA/UEBA)** هي تقنية تستخدم لتعزيز الكشف عن التهديدات والاحتيال. تعمل هذه التقنية من خلال مراقبة أنماط سلوك المستخدمين والأجهزة والكيانات الأخرى داخل شبكة المؤسسة، ومقارنتها بأنماط السلوك الطبيعية.

أمثلة على السلوكيات الشاذة التي يمكن أن تكشفها:UBA/UEBA

- **تسجيل الدخول من موقع جغرافي غير معتاد.**
- **الوصول إلى بيانات حساسة بشكل غير مصرح به.**
- **تنزيل برامج ضارة.**
- **زيادة غير طبيعية في نشاط الشبكة.**

تحليل سلوك المستخدم والكيانات هي تقنية قوية تساعد المؤسسات على حماية أنظمتها من التهديدات المتطورة. من خلال مراقبة سلوك المستخدمين والأجهزة بشكل مستمر، يمكن لـ UBA/UEBA الكشف عن الأنشطة الضارة بسرعة واتخاذ الإجراءات اللازمة لحماية البيانات والممتلكات الفكرية للمؤسسة.

تصنيف الهجمات إلى نوعين رئيسيين



الفروقات الرئيسية

- **المشكلات المُعطِّلة والمكلفة** :أعلى الأولويات نظرًا لتأثيرها الواسع والكبير على الشركة.
- **النطاق الأصغر والتكاليف الأقل** :تؤثر غالبًا على فرد أو جهاز واحد، ولا توقف عمل الشركة بالكامل.

تقسيم الهجمات إلى مجموعتين رئيسيتين

رغم أنه قد لا يكون هناك تمييز واضح دائمًا، ومن الصعب في بعض الأحيان تحديد طبيعة الهجوم، فإنه يجب عليك دائمًا التفكير في **الهدف المقصود ونطاق الهجوم**.

بوجه عام، يمكن تقسيم الهجمات إلى:

1. **الهجمات الصغيرة والمحدودة**
   - هذه الهجمات غالبًا ما تكون ضمن "ضوضاء الإنترنت" اليومية التي، رغم كونها مزعجة، من المحتمل أن تؤثر على مستخدم أو جهاز واحد فقط.
   - تتسم هذه الهجمات بتكتيكات عالية الحجم وغير مخصصة، وتكون **فرصية**، حيث يقبل المهاجمون أي ضحية يمكنهم خداعها.
2. **الهجمات الكبيرة التي تستهدف الشركة بأكملها**
   - هذه الهجمات قد تؤدي إلى:
     - توقف الإنتاج.
     - كشف كميات هائلة من البيانات.
     - إلحاق أضرار جسيمة.
     - تعريض الأفراد للخطر أو ما هو أسوأ.
   - غالبًا ما تنفذها دول قومية، نشطاء اختراق، وأحيانًا منظمات الجريمة المنظمة.

متى يصبح الهجوم خطيرًا؟

رغم أن التمييز بين النوعين قد لا يكون دقيقًا دائمًا، إلا أن أي مجموعة تهدف إلى **إيقاف شركتك للحصول على فدية** مقابل استعادة بياناتك، يجب أن تُعتبر تهديدًا من الدرجة الأولى.

- إذا رأيت أي هجوم يُحتمل أن يكون من هذا النوع، **غيّر موقفك فورًا إلى "هذا جدي، يجب أن نتحرك الآن."!**
- يجب أن تُقيّم باستمرار أي حادثة جارية لتحديد مدى خطورتها.

خلال الدورة التدريبية، سنناقش مختلف الجوانب المتعلقة بكيفية التصرف في كل من هذه السيناريوهات.

تعرف على عدوك: المهاجمون الانتهازيون

هدف المهاجم

- تحقيق اختراق واسع النطاق وغير موجه.

الإستراتيجية

- جمع أجهزة كمبيوتر مصابة والتحكم بها كجزء من شبكة الروبوتات.(Botnet)
- استغلال عدد الأجهزة المخترقة لتحقيق الأهداف المطلوبة.

التكتيكات

- رسائل البريد الإلكتروني الضارة والمزيفة.
- التنزيلات الضارة التلقائية عبر المواقع.(Web Drive-By Downloads)
- مسح واستغلال ثغرات الويب.
- هجمات الهندسة الاجتماعية المعتمدة على المتصفح.
- النوافذ المنبثقة ورسائل التحذير المزيفة مثل (FakeAV).

تعرف على عدوك: المهاجمون الانتهازيون

المهاجمون الانتهازيون هم مجموعات مثل بعض عناصر الجريمة المنظمة أو **المخترقين المأجورين** .لا يهتم هؤلاء المهاجمون بهوية ضحاياهم طالما أن مواردهم يمكن أن تخدم أهدافهم.

- يرسلون موجات واسعة من رسائل التصيد.
- ينشرون مجموعات استغلال عبر الإنترنت.
- يستخدمون هجمات الهندسة الاجتماعية القائمة على المتصفح لجمع أكبر عدد ممكن من الأفراد المخترقين.

كيف يتم استخدام الأجهزة المصابة؟

- أحيانًا يمكن بيع الوصول إلى جهاز مستخدم فريد إذا كان ينتمي إلى شركة يصعب اختراقها.
- أجهزة الروبوتات [20]ذات الأعداد الكبيرة تُستخدم في:
  - استضافة مواقع ضارة أو بنية تحتية لنظام أسماء النطاقات (DNS) لتوجيه المستخدمين إلى تلك المواقع.
  - إرسال رسائل البريد العشوائي.
  - شن هجمات حجب الخدمة الموزعة (DDoS) باستخدام عرض النطاق الترددي الجماعي للأجهزة.
  - وأكثر من ذلك.

---

[20] **شبكة البوتات: جيش من الأجهزة الخاضعة للسيطرة**

شبكة البوتات (Botnet) هي مجموعة ضخمة من الأجهزة المتصلة بالإنترنت والتي تم اختراقها ووضعها تحت سيطرة مهاجم واحد. تخيل أنك تمتلك جيشًا من الروبوتات، ولكن بدلًا من الروبوتات المادية، هذه الروبوتات هي أجهزة كمبيوتر. يمكن للمهاجم التحكم في هذه الأجهزة جميعًا وإصدار أوامر لتنفيذ مهام معينة. - ومن أشهر الهجمات التي تستخدم فيها هذه الأجهزة هي هجمات حجب الخدمة الموزعة (DDoS attacks)

عدوك: المهاجمون الموجهون التهديدات المتقدمة المستمرة (APTs)

هدف المهاجم

- استهداف أفراد أو منظمات بعينها.
- الحصول على معلومات محددة أو الوصول إلى أنظمة معينة.
- تعطيل أعمال شركتك بشكل متعمد.

الإستراتيجية

- شن هجمات مخصصة ومصممة خصيصًا لك ولمنظمتك.

التكتيكات

- **التصيد الاحتيالي الموجه :(Spear-phishing)** رسائل بريد إلكتروني مصممة لاستهداف أفراد معينين.
- **الهجمات عبر مواقع الاستهداف :(Watering Holes)** اختراق مواقع محددة لاصطياد ضحايا معينين.
- **الهجمات المادية أو الهندسة الاجتماعية :**مثل إدخال وسائط USB ضارة أو خداع الموظفين للوصول إلى النظام.
- **استغلال الجوانب الخدمية المستهدفة والثغرات غير المكتشفة :(Zero-Days)** الهجوم على خدمات أو أنظمة معينة.
- **الابتزاز المزدوج :**سرقة البيانات وتشويش الأنظمة لزيادة الضغط على الضحية.

تعرف على عدوك: المهاجمون الموجهون(APTs)

الهجمات الموجهة تمثل النوع الأخطر من تهديدات المهاجمين. هؤلاء الأفراد أو المجموعات يستهدفونك تحديدًا لاعتقادهم بامتلاكك شيئًا يستحق العناء. هذا الاستهداف يعني أنهم أكثر تصميمًا على اختراقك مقارنة بالمهاجمين الانتهازيين الذين قد يتراجعون عند الفشل الأول.

كيف تختلف هجماتهم؟

- يقومون بتخصيص الهجمات لتلائم موظفيك، بنية شبكتك، وبرامجك.
- يعتمدون على تكتيكات مثل:
  - **التصيد الاحتيالي الموجه :**رسائل بريد إلكتروني موجهة وذات مصداقية.
  - **الهندسة الاجتماعية :**استغلال العامل البشري للحصول على المعلومات.
  - **استغلال الثغرات المستهدفة :**تطوير هجمات مخصصة تتناسب مع البرامج التي تستخدمها.
  - **اختراق مواقع الويب أو سلسلة التوريد :**لضمان وصولهم إلى أهداف محددة.

هل تعرضت لهجوم موجه من قبل؟

- إذا لم تواجه هجومًا موجهًا سابقًا، راجع الحوادث التي تعاملت معها.
- هل بدت أي منها مصممة بعناية وغير عشوائية؟
- هل أشارت إلى أن المهاجم استغرق وقتًا طويلًا لتحضير الهجوم وتخصيصه لشركتك؟

هذه الأدلة قد تشير إلى أن الهجوم كان موجهًا. كما سنناقش لاحقًا، من المهم جدًا التمييز بين الهجوم الموجه وغيره لضبط استجابتك بشكل مناسب.

تسمية مجموعات الهجوم والمعايير المستخدمة

افهم الأمر:

لكل شركة أمان إلكتروني طريقتها الخاصة في تسمية مجموعات التهديدات.

- ستحتاج إلى تتبع أسماء متعددة للمجموعة ذاتها!

أنظمة التسمية حسب الشركة:

1. **مايكروسوفت:**
   - تستخدم أسماء العناصر الكيميائية للمجموعات التابعة لدول، والبراكين للمجموعات الإجرامية، والأشجار للأنشطة المتعلقة بالقطاع الخاص، و "DEV"للمجموعات غير المعروفة.
2. **مانديانت:(Mandiant)**
   - "APT"متبوعًا برقم للمجموعات التابعة للدول، مثل APT1 أو APT28.
   - "UNC"للمجموعات غير المصنفة، و "FIN"للمجموعات المالية، و "TEMP" للأعمال قيد التقدم أو غير المعروفة.
3. **كراودسترايك:(CrowdStrike)**
   - تستخدم صفة متبوعة باسم حيوان ذو دلالة جغرافية للمجموعات التابعة لدول.
   - "Panda"لجميع المجموعات ذات الصلة بالصين، و "Spider"للمجموعات غير المدعومة من الدول.
4. **كاسبرسكي:(Kaspersky)**
   - لا يوجد نمط رسمي؛ يعتمد الاسم على الباحث المسؤول عن التحليل.

التحديات وأثرها على المدافع

هذا التنوع يعني أنك إذا علمت أنك تعرضت لهجوم من APT28 ، فستحتاج إلى متابعة أي أخبار مرتبطة أيضًا بأسماء أخرى لهذه المجموعة مثل:

- **Fancy Bear - Sofacy – Strontium**

بمعنى آخر، عليك بذل الجهد لفهم الأسماء المستخدمة من قبل الشركات الأخرى وربطها ببعضها، إذا أمكن.

كيف يمكن التعامل مع هذا؟

- يجب أن تحتوي منصة استخبارات التهديدات (TIP) لديك على ميزات تمكنك من:
  - تجميع الأنشطة.
  - تصنيفها باستخدام علامات متعددة.

اقتباس فكاهي عن تسمية المجموعات:

"ما الفائدة في اسم؟ APTبأي اسم آخر سيبقى دائمًا تهديدًا مستمرًا".

- سايبر وليم شكسبير.

للمزيد من المعلومات:

- ما الذي يوجد في اسم مجموعة تهديد؟(SecurityWeek)
- تعريف التهديدات المتقدمة المستمرة (CrowdStrike) (APT)

دراسة حالة لهجوم انتهازي: ميراى(Mirai)

النقاط الرئيسية:

- تم نشر الشيفرة المصدرية لبرمجية **Mirai**بشكل علني، مما سمح للعديد باستخدامها لتشكيل جيوش من الأجهزة المصابة.
- ملايين الأجهزة مصابة الآن ببرمجيةMirai ، وغالبًا ما تكون أجهزة إنترنت الأشياء (IoT) الصغيرة هي الهدف.
  - تشمل هذه الأجهزة: أنظمة التخزين الشبكي(NAS) ، أجهزة تسجيل الفيديو الرقمية (DVRs)، الكاميرات، وأجهزة أخرى تحتوي على ثغرات أمنية أو تستخدم كلمات مرور افتراضية.
- يمكن للأجهزة التي تقع تحت سيطرة Mirai أن تُستخدم بشكل جماعي لتنفيذ:
  - **الفحص السريع والموزع.**
  - **محاولات استغلال واسعة النطاق** مثل استغلال ثغرة .**(log4j)**
  - **هجمات حجب الخدمة الموزعة.(DDoS)**
  - **إرسال البريد المزعج.(Spam)**
  - **الاحتيال.(Fraud)**

شرح الحالةMirai :

شبكة **Mirai botnet**تُعد مثالًا على البرمجيات الخبيثة الانتهازية التي ما زالت تُستخدم حتى اليوم.

- يتم استخدام هذه البرمجية بشكل مستمر لعمليات الفحص واسعة النطاق ومحاولات الاستغلال.
- على سبيل المثال، عند ظهور ثغرة **log4j**في أواخر عام 2021، بدأت الروبوتات التي تتحكم فيها Mirai فورًا بالبحث عنها واستغلالها عالميًا.

كيف تعمل؟

- تعتمد Mirai بشكل كبير على الأجهزة المصابة من نوع **إنترنت الأشياء(IoT[21])** ، مثل:
  - أجهزة التخزين الشبكي.(NAS)
  - أجهزة تسجيل الفيديو الرقمية.(DVRs)
  - الكاميرات، وغيرها.
- ورغم أن كل جهاز مصاب منفردًا قد لا يمتلك قدرات كبيرة، إلا أن العدد الهائل من الأجهزة المصابة يُنتج قوة ضخمة بفضل النطاق الترددي المجمع، مما يجعلها قادرة على إحداث أضرار جسيمة عند استهداف ثغرة أو هدف معين.

للمزيد من المعلومات:

لماذا تُعتبر Miraiتهديدًا مستمرًا لنظام إنترنت الأشياء (IoT) – Intel 471.

---

[21] إنترنت الأشياء (IoT)
إنترنت الأشياء (IoT) هو مصطلح يشير إلى شبكة من الأجهزة والأشياء اليومية التي تم تجهيزها بتقنيات تسمح لها بالاتصال بالإنترنت وتبادل البيانات مع بعضها البعض. تخيل عالمًا حيث كل شيء من ثلاجتك إلى سيارتك يمكن أن يتصل بالإنترنت ويجمع البيانات ويحلل المعلومات. هذا هو جوهر إنترنت الأشياء.

دراسة حالة هجوم برمجيات الفدية: الهجوم على خط أنابيب كولونيال(Colonial Pipeline)

النقاط الرئيسية:

- **29أبريل 2020 :**تمكّن المهاجمون من الوصول إلى الشبكة عبر كلمة مرور واحدة مسربة كانت صالحة لحساب VPN كان يجب إيقافه، مما أدى إلى سرقة 100 جيجابايت من البيانات.
- **7مايو :**بدأ الهجوم الفعلي وأدى إلى إغلاق خط الأنابيب، مما تسبب في اضطرابات بالرحلات الجوية، وزيادة غير مسبوقة بأسعار الوقود، ونقص كبير في الوقود على الساحل الشرقي للولايات المتحدة.
- **10مايو :**أصدرت FBI بيانًا يؤكد استخدام برمجية الفدية **DarkSide** في الهجوم.
- **12مايو :**استُأنفت خدمات خط الأنابيب.
- **7يونيو :**تمكنت فرقة عمل حكومية أمريكية من استعادة معظم فدية البيتكوين المدفوعة.

شرح الحالة: هجوم كولونيال

السياق العام:

شهدنا في الآونة الأخيرة العديد من الهجمات المدمرة التي استهدفت البنية التحتية الحيوية، وكان الهجوم على **خط أنابيب كولونيال** أحد أبرز الأمثلة في عام 2020، حيث تسبب في مشاكل كبيرة للبنية التحتية والطاقة في الولايات المتحدة. وعلى الرغم من أن طبيعة الهجوم لم تكن فريدة من نوعها، إلا أن اختيار الهدف وطبيعة الهجوم العلنية زاد من تأثيره بشكل كبير.

كيف وقع الهجوم؟

- وُجدت بيانات اعتماد مستخدم واحدة على الإنترنت المظلم (**Dark Web**) والتي كانت تعمل مع بوابة VPN الخاصة بالشركة.
- الحساب المستخدم كان قديمًا وكان يجب إلغاء تنشيطه لكنه ظل نشطًا، ولم يكن محميًا بمصادقة متعددة العوامل.(**MFA**)
- لم يُعرف إذا ما كانت كلمة المرور المسربة تخص الموظف مباشرةً أو مجرد تطابق صدفي حيث استخدم الشخص كلمة مرور مشابهة على حسابات أخرى.
- أدى هذا الاختراق الأولي إلى دخول المهاجمين إلى شبكة كولونيال بايبلاين، وتم سرقة 100 جيجابايت من البيانات لاستخدامها في الابتزاز.

أحداث الهجوم:

- **7مايو 2020، الساعة 5 صباحًا :**اكتشف موظف مذكرة فدية على أحد أجهزة الحواسيب في غرفة التحكم.
- بحلول الساعة 6:10 صباحًا، تم إيقاف تشغيل خط الأنابيب بالكامل (يبلغ طوله 29,000 ميل، ويمتد من تكساس إلى الساحل الشرقي الأمريكي)، وهو أول توقف شامل في تاريخه الذي امتد 57 عامًا.
- استغرق فحص الخط بالكامل بحثًا عن أي أضرار مادية عدة أيام، واستُعيدت الخدمة في **12 مايو**.

التأثير:

- خلال الأيام القليلة للإغلاق:

- شهدت الولايات المتحدة نقصًا حادًا في الوقود، وبلغت الأسعار أعلى مستوياتها خلال ست سنوات.
- في بعض المناطق، مثل فيرجينيا وواشنطن العاصمة، نفد الوقود من **87%** من المحطات بحلول اليوم الرابع نتيجة الذعر في الشراء.
- تعرّضت الرحلات الجوية في مطارات متعددة للاضطراب بسبب نقص الوقود الناتج عن إغلاق خط الأنابيب.

الدروس المستفادة:

- يُظهر هذا الهجوم مدى الضرر الذي يمكن أن تُحدثه كلمة مرور واحدة مسربة.
- يوضح أهمية إيقاف الحسابات القديمة وتفعيل المصادقة متعددة العوامل لحماية الوصول إلى الأنظمة الحساسة.
- تسلط هذه الحالة الضوء على أهمية دور فرق الأمن السيبراني في حماية البنية التحتية الحيوية.

لحسن الحظ، انتهت هذه القصة بنتيجة إيجابية جزئية. تمكنت فرقة العمل الأمريكية لمكافحة الابتزاز الرقمي من استرداد **63.7بيتكوين** من أصل **75بيتكوين** دُفعت كفدية، أي ما يعادل **2.3مليون دولار** في ذلك الوقت.

كيف تم الاسترداد؟

- قدمت الحكومة الأمريكية إقرارًا يفيد بأن مكتب التحقيقات الفيدرالي (FBI) تمكن من الوصول إلى المفتاح الخاص للمحفظة الرقمية التي تم تحويل الفدية إليها.
- لم تُعلن التفاصيل الدقيقة لكيفية حصول مكتب التحقيقات على المفتاح الخاص، مما أثار العديد من التساؤلات حول طبيعة العملية.

المصادر:

- اختراق خط أنابيب كولونيال باستخدام كلمة مرور مسربة Bloomberg -
- استرداد الفدية المدفوعة للهاكرز NPR.org -
- تفاصيل استرداد أموال الفدية Thomson Reuters -

دروس إضافية:

- على الرغم من أن الهجمات السيبرانية يمكن أن تكون مدمرة للغاية، فإنها تُظهر أن التعاون بين الحكومات وفرق الأمن السيبراني يمكن أن يؤدي إلى استرداد بعض الأضرار.
- تبقى الأسئلة حول قدرة الجهات الرسمية على الوصول إلى المحافظ الرقمية، مما يسلط الضوء على أهمية فهم المزيد حول العملات المشفرة والأمن المرتبط بها.

إطلاق دليل :Conti تحليل مدى تطور مجموعات الفدية

السؤال: ما مدى تطور مجموعات الفدية هذه؟

الإجابة:

1. ليست متطورة بالقدر الذي قد تتوقعه، ولكن...
2. متطورة بما يكفي للنجاح أحيانًا، وهذا هو الأمر المهم!

كيف عرفنا ذلك؟

- في **سبتمبر 2021**، قام أحد الشركاء في مجموعة الفدية **Conti** بتسريب دليل العمليات الخاص بالمجموعة!
- الدليل المسرب احتوى على:
  - قائمة شاملة بالأدوات والأوامر خطوة بخطوة.
  - مجموعة من الأدوات والملفات اللازمة لتثبيت برامج الفدية وتشغيلها على شبكات الشركات المستهدفة.

إطلاق دليل :Conti تحليل التفاصيل

مدى التطور داخل الشبكة؟

في كثير من الحالات، الإجابة كانت" :**ليس متطورًا جدًا."**

ولكن كيف عرفنا ذلك؟

- في خطوة غير مسبوقة، كشف شريك غاضب عن أساليب العمل لمجموعة الفدية .**Conti**
- هذا التسريب منح المدافعين السيبرانيين رؤية نادرة إلى التكتيكات والتقنيات والإجراءات (**TTPs**)التي تستخدمها المجموعة.

ما الذي اكتشفناه؟

- لم تكن المجموعة تستخدم **ثغرات غير مكتشفة (Zero-days)** أو تقنيات متقدمة جدًا.
- غالبًا اعتمدت على:
  - **أوامر نظام مدمجة**.
  - أدوات اختبار اختراق متاحة مجانًا.
  - تقنيات مهاجمين معيارية لتجنب الكشف.

ما الدرس المستفاد للمدافعين؟

- **يمكننا إيقافهم!**
- الفهم الدقيق لهذه الأساليب يمنحنا فرصة أفضل للكشف عن هذه الهجمات وإيقافها قبل حدوث أضرار كبيرة.
- في الصفحة التالية، سنستعرض بعض التفاصيل المحددة وما يمكننا البحث عنه كمدافعين.

نتائج ترجمة كتاب Cisco Talos لخطط Conti التشغيلية: أبرز الاكتشافات

الأدوات المستخدمة:	الأساليب/الخطوات من التسريب:
ADFind: لتعداد Active Directory. **Seatbelt**: لتحليل إعدادات الأجهزة. **SharpView**: نسخة .NET من PowerView لتعداد الشبكات. **SharpChrome**: أداة لسرقة تسجيلات الدخول وملفات تعريف الارتباط من متصفح Chrome. **GMER**: لتعطيل برامج مكافحة الفيروسات وحلول حماية النقاط النهائية. **Armitage**: أداة مرتبطة بـ Metasploit. **Cobalt Strike**: للتحكم وإدارة الهجوم. **AnyDesk/Atera**: للحفاظ على الوصول الدائم. **SMBAutoBrute**: لهجمات التخمين العشوائي.	1. **البحث الأولي**: استخدام Google لجمع المعلومات عن المؤسسة وإيراداتها. 2. **أوامر وأنظمة سطر الأوامر**: تنفيذ أوامر ونصوص لاستكشاف برامج مكافحة الفيروسات، المجموعات، المستخدمين، ونطاق الشبكة. 3. **الوصول إلى بيانات الاعتماد**: استخدام أساليب مثل Kerberoasting ، أداة Mimikatz، الهجمات بالثغرات، التخمين العشوائي، وسرقة بيانات المتصفح. 4. **البحث عن مشاركات الشبكة**: باستخدام PowerShell. 5. **بحث الثقة والتفريغ**: باستخدام NItest و NTDS dump. 6. **التسريب**: تحميل البيانات باستخدام Mega.io وأداة rclone. 7. **الإعداد للتشفير**: وضع ملفات exe/bat على مشاركات وحدة التحكم بالمجال (DC). 8. **تعطيل مكافحة الفيروسات**: باستخدام PowerShell ، أداة GMER ، وغيرها، ثم تفعيل هجوم الفدية.

تحليل Cisco Talos لخطط Conti التشغيلية

كشفت مجموعة Talos التابعة لشركة Cisco عن تفاصيل مدهشة أثناء ترجمة وتحليل أساليب Contiالهجومية. كانت إحدى أبرز النقاط هي **مدى الدقة والتفصيل في هذه الخطط**، مما يجعل من الممكن حتى للمهاجمين الهواة تنفيذ هجمات فدية مدمرة، حيث أصبح "حاجز الدخول" لتنفيذ مثل هذه الهجمات أقل بكثير مقارنة بغيرها من الهجمات.

تم تلخيص بعض الأساليب والتقنيات والأدوات الرئيسية المستخدمة من قبل المهاجمين في الشريحة السابقة. على الرغم من أنه لا يمكننا التعمق في كل شيء هنا، فإن التعرف على أسماء هذه الأدوات أمر ضروري. إذا صادفت إحدى هذه الأدوات في تنبيه أمني، مثل **AnyDesk**، وتساءلت: **"لماذا يقوم شخص ما بتثبيتAnyDesk ؟"**، فأنت تعرف الآن أن عليك التحرك بسرعة!

ننصح بشدة بالبحث والتعلم عن أي شيء غير مألوف بالنسبة لك من هذه القائمة. كما ننصح بزيارة مدونة Cisco Talos والمقال المرتبط بها لمعرفة المزيد حول هذا التسريب المهم. هذه فرصة نادرة لفهم تقنيات المهاجمين وعلينا الاستفادة منها لتحسين دفاعاتنا.

[1] "Translated: Talos' insights from the recently leaked Conti ransomware playbook" – Cisco Talos: https://blog.talosintelligence.com/2021/09/Conti-leak-translation.html

دراسة حالة لهجوم مستهدف 3: هجوم SolarWinds في ديسمبر 2020

ملخص الحادث:

- **4سبتمبر 2019** :حصل المهاجمون على الوصول الأولي.
- **20فبراير 2020** :تم تجميع ونشر الباب الخلفي."Solarigate"
- **مارس 2020** :بدأ تحديد أهداف الهجوم.
- **مايو - ديسمبر 2020** :وصول مباشر إلى بيئات الضحايا.
- **12ديسمبر 2020** :اكتشاف الاختراق والإعلان عنه علنًا.

التكتيكات المستخدمة:

1. **هجوم معقد على سلسلة التوريد** :نُفذ من خلال مورد موثوق.
2. **باب خلفي متعدد المراحل** :مع تنشيط متأخر وآليات قيادة وتحكم مخفية بعناية.
3. **إجراءات أمن العمليات (OPSEC[22]) متميزة** :تضمنت مؤشرات اختراق فريدة(IOCs) ، مثل الملفات، النطاقات، وعناوين IP لكل ضحية.
4. **أول هجوم علني باستخدام "Golden SAML"** :لتحقيق اختراق إضافي في بيئات السحابة.

تفاصيل الهجوم

في ديسمبر 2020، أعلنت شركة SolarWinds عن خرق خطير طال برنامجها **Orion**، والذي تبين أنه جزء من هجوم معقد على سلسلة التوريد. نُسب الهجوم إلى مجموعة APT29 المعروفة أيضًا بـ Cozy Bear و UNC2452.نظرًا لانتشار منتج Orion الواسع، تمكن المهاجمون من استغلال هذا الخرق للوصول إلى جهات بارزة، بما في ذلك **Microsoft، Intel، NVIDIA، FireEye، والعديد من الوكالات الحكومية الأمريكية** .وتشير التقديرات إلى أن ما يصل إلى **18,000منظمة** قد حمّلت الإصدار الضار من.Orion

لماذا كان هذا الهجوم كارثيًا؟

1. **مصدر موثوق** :تم نشر البرمجيات الضارة من خلال مورد موثوق.
2. **إخفاء احترافي** :استخدم المهاجمون تقنيات متقدمة مثل خوارزميات توليد النطاقات (DGA[23]) ومؤشرات اختراق (IOCs) فريدة لكل ضحية، مما جعل اكتشافهم صعبًا للغاية.
3. **اختراق السحابة** :تمكن المهاجمون من سرقة مفاتيح توقيعSAML ، مما سمح لهم بتوقيع رموز SAMLالخاصة بهم. أدى ذلك إلى حصولهم على وصول إداري للعديد من المنصات السحابية والتطبيقات.

ماذا نتعلم من هذا الهجوم؟

مع التحول العالمي نحو آليات مصادقة **عدم الثقة (Zero-Trust)** والاعتماد المتزايد على إدارة الهوية، يعد هذا الهجوم بمثابة تحذير. يشير إلى أن الهجمات المستقبلية قد تستهدف نفس الثغرات أو آليات مشابهة. يجب على فرق الدفاع السيبراني أن تكون مستعدة وتعمل باستمرار على تحسين استراتيجيات الدفاع، حيث إن التهديدات تتطور بشكل أسرع من أي وقت مضى.

روابط ذات صلة:

- تحليل Microsoftلمرحلة التنشيط الثانية في هجوم SolarWinds
- مدونة FireEyeحول استغلال سلسلة توريد SolarWinds

---

[22] **إجراءات أمن العمليات (OPSEC)** هي مجموعة من الممارسات والإجراءات التي تهدف إلى حماية المعلومات الحساسة والحيوية من الوقوع في أيدي الأعداء أو المنافسين. بعبارة أخرى، هي عملية منظمة لتحديد المعلومات الحساسة وحمايتها من الاستغلال.

[23] **خوارزميات توليد المجالات :(DGA) سلاح سري في ترسانة المهاجمين السيبرانيين**

خوارزميات توليد المجالات (Domain Generation Algorithms) هي تقنية ذكية يستخدمها المهاجمون السيبرانيون لإخفاء اتصالاتهم مع برامج ضارة. تخيل أنك تريد التواصل مع شخص ما بشكل سري، فبدلاً من استخدام رقم هاتف ثابت، تقوم بتغيير رقمك بشكل مستمر. هذا هو بالضبط ما تفعله خوارزميات.DGA

ملخص: "اعرف عدوك"

النقاط الرئيسية:

- يتراوح المهاجمون بين **الحكومات، والجريمة المنظمة، والهواة.(script kiddies)**
- فكر في الخصم :**من الذي يهاجمني؟**
- فكر في الدوافع :**ماذا يريدون؟ هل من المحتمل أن يهاجمونا؟ هل لديهم القدرة على إحداث ضرر؟**
- فكر في مسارات الهجوم :**كيف سيحصلون على ما يريدون؟**
- فكر في الإجراءات الدفاعية :**كيف يمكن مراقبة وحماية الأنظمة ضد هذه التهديدات بناءً على طبيعة المجموعة؟**
- حافظ على هذه الاعتبارات خلال التحليل والاستجابة للتهديدات.
- سيتم تغطية التفاصيل الدقيقة في الأيام القادمة.

التفاصيل:

خلال مسيرتك المهنية في **أمن المعلومات**، ستواجه طيفًا واسعًا من الفاعلين المهددين (Threat Actors) في عملك اليومي. بعض هذه التهديدات ستكون سهلة الصدّ، بينما ستكشف تهديدات أخرى عن جوانب جديدة لم تعهدها من قبل، مما يجبرك على وضع خطط تفصيلية وحلول إبداعية للتعامل مع التهديدات.

خلال هذه الدورة، سنخوض في تفاصيل أكبر حول هذا الموضوع. ولكن في الوقت الحالي، من الضروري أن تسعى باستمرار إلى تحديد **نوع المجموعة** التي تقف وراء أي هجوم تواجهه، على الأقل التمييز بين **الهجمات الفرصية** و**الهجمات المستهدفة**.

كما يجب أن تأخذ بعين الاعتبار **دوافع المهاجمين**، ففهم هذه الدوافع سيساعدك على اتخاذ قرارات أفضل. لذلك، من المفيد قضاء وقت فراغك في قراءة التقارير حول هذه المجموعات لتكون على دراية بمشهد التهديدات المتغير، ومن قد يكون مستهدفًا لمنظمات مثل منظمتك.

سيساعدك هذا الفهم على بناء تصور واضح عن **التقنيات المستخدمة** من قِبل هذه المجموعات، وكيفية التصرف أثناء تنفيذ **خطط الاستجابة**، وهو ما سنتحدث عنه بمزيد من التفصيل لاحقًا في الدورة.

ملخص القسم الأول

النقاط الرئيسية:

- الهدف الأسمى الذي يجب أن تتذكره دائمًا هو: **"تقليل احتمالية التأثير المادي على مؤسستي بسبب حدث إلكتروني".**
- لتحقيق هذا الهدف، يجب أن تمتلك فهمًا عميقًا لـ:
  - **مهمتك** وكيفية ترتيب الأولويات لمواجهة الأحداث ذات التأثير الكبير.
  - **أنواع الأعداء** الذين ستواجههم، ودوافعهم، وتقنياتهم التكتيكية والإجرائية.(TTPs)
  - **أنواع البيانات** من الشبكة، ونقاط النهاية، والتطبيقات التي يمكنك استخدامها للكشف عن الهجمات ووقفها.
  - كيفية **تكامل الأدوات** معًا لدعم ردود الأفعال السريعة بشكل تلقائي.
  - تنفيذ **تحليل عالي الجودة** واستجابة سريعة للحوادث.
- سيركز بقية هذه الدورة على هذه النقاط بالتفصيل!

ملخص القسم الأول:

لقد وصلنا إلى نهاية القسم الأول. كما لاحظت، فإن أعضاء **الفريق الأزرق** يواجهون تحديًا معقدًا ومليئًا بالتحديات. ومع ذلك، بفضل **وفرة الأدوات** والإصرار، يمكننا التغلب على المهاجمين.

لتحقيق ذلك، سنحتاج إلى فهم شامل لأدواتنا، شبكاتنا، مضيفينا(Hosts) ، ودوافع أعدائنا. وخلال بقية هذه الدورة، سنستكشف هذه المواضيع بعمق أكبر مع التركيز على كيفية تعزيز الدفاعات ومواجهة التحديات!

التمرين على ELK Stack

التمرين على ال ELK Stack على موقع tryhackme.com

https://tryhackme.com/r/room/servidae

مرفق القاموس

English	عربي
Web	مواقع الويب
Phishing	التصيد الاحتيالي
Ext. Media	الوسائط الخارجية
Impersonation	انتحال الهوية
Improper Usage	سوء الاستخدام
Theft	السرقة
etc	إلخ
Perimeter network	شبكة محيطية
IOCs: Indicator of Compromise	مؤشرات الإختراق
Observables	عناصر قابلة للرصد
Case	حالة
Hashes	القيم المشفرة
Cyber Kill Chain	**سلسلة القتل الإلكتروني**
Delivery	*التوصيل*
Exploit	*الاستغلال*
Install	*التثبيت*
has been sighted	تمت مشاهدته
False Positive	*إيجابية كاذبة*
True Positive	*إيجابية حقيقية*
Delivery Vector	*متجه التسليم*
Feedback	**التغذية الراجعة**
informs	يغذي
intent	نية
capability	قدرة
opportunity	فرصة
Payload	الحمولة
Galaxy	مجرة
Brute force	القوة الغاشمة
Firewall	الجدار الناري
regular expressions	التعبيرات المنتظمة
black swan	أحداث البجعة السوداء
Spear-phishing	**التصيد الاحتيالي الموجه**
Watering Holes	**الهجمات عبر مواقع الاستهداف**