kaspersky واجهوا المستقبل بأمان

XDR مقابل SIEM
مقابل SOAR

هل تعبت بينما تفكر في الكثير من الاختصارات؟ دعنا نعرف ما الذي يحدث وراء هذه الحروف الصغيرة...

المقدمة

SIEM وSOAR وMDR وEDR وEPP وXDR... هل تشعر بالحيرة والضياع وسط هذا الكم من اختصارات الأمن الإلكتروني؟ نتفهم ذلك، ولهذا السبب مضينا قدمًا ووفرنا هذا الدليل المفيد لشرح الفروق بين ثلاثة من الأدوات الكبيرة: SIEM وSOAR وXDR. ما القصة وراء هذه الاختصارات؟ كيف طورت الصناعة هذه المصطلحات المربكة والمتداخلة؟ هل تعني أي شيء مميز، أم أنها مجرد حيل تسويقية؟ ما أوجه الشبه والاختلاف؟ هل يمكن أن تكمل بعضها البعض أم أنها تتنافس مع بعضها البعض؟
تعال وانضم إلينا في هذا الحوار! دعنا نلتقط مفاتيح المعرفة، ونخوض داخل غابة الاختصارات والمصطلحات، ونصل إلى ساحة مفتوحة من الفهم الواضح!

SIEM

إدارة معلومات الأمان والأحداث (SIEM) هي مجموعة من الأدوات والخدمات التي تجمع بين إدارة أحداث الأمان (SEM) وإدارة معلومات الأمان (SIM) في منصة واحدة. وتجمع إدارة معلومات الأمان والأحداث (SIEM) بيانات السجل وتجمعها وتحللها وتخزنها عبر البنية التحتية لتقنية المعلومات لحالات الاستخدام المختلفة، بما في ذلك الحوكمة والامتثال ومطابقة الارتباط المستندة إلى القواعد للأنشطة المشبوهة.

كيف تعمل إدارة معلومات الأمان والأحداث (SIEM)؟

تم تطوير خدمات إدارة معلومات الأمان والأحداث (SIEM) الأولى في عام 2005، وكان الغرض الأصلي هو تجميع السجلات والأحداث وتخزينها عبر البنية التحتية لتقنية المعلومات في المؤسسة - بما في ذلك نقاط النهاية والتطبيقات وأجهزة الشبكة - لأغراض إعداد تقارير الامتثال. وتدير إدارة معلومات الأمان والأحداث (SIEM) الارتباطات على مجموعة البيانات هذه، وتبحث عن أي أنماط أو أحداث قد تشير إلى سلوك مشبوه، وتنشئ تنبيهًا لمركز عمليات الأمن (SOC). وسرعان ما رأى محللو الأمان إمكانية استخدام هذه التنبيهات ليس فقط لأغراض الامتثال والحوكمة، لكن لتحديد ووقف تقدم أي نشاط ضار في النظام البيئي بشكل أكثر استباقية.

قيود إدارة معلومات الأمان والأحداث (SIEM)

كانت المشكلة هي أن خدمات قيود إدارة معلومات الأمان والأحداث (SIEM) لم تكن مصممة لغرض محدد وهو اكتشاف الحوادث والاستجابة لها. وهذا ما جعل العمل معها صعبًا بعض الشيء، وذلك لعدة أسباب:

- لديك عدد كبير جدًا من التنبيهات - يجب تصفية مجموعة البيانات الضخمة التي توفرها إدارة معلومات الأمان والأحداث (SIEM) وتعالجها وتحللها يدويًا، وهو أمر غير مناسب لمحللي الأمان الذين يحاولون منع الهجمات في مشهد التهديدات سريع الخطى.

- لا يوجد سياق - للتعامل مع الهجمات الجديدة والمعقدة والمتطورة، يحتاج محللو الأمان إلى صورة سياقية ومتسقة لمشهد التهديد الخاص بالمؤسسة، بدلاً من تدفقات البيانات المنفصلة التي توفرها إدارة معلومات الأمان والأحداث (SIEM).

- سلبية للغاية - حظر العمليات المشبوهة وعزل الملفات وإمكانيات الاستجابة الأخرى ليست من اختصاصها؛ وهي في الأساس أداة تحليلية سلبية.

حاول متخصصو الأمان حل هذه المشكلات من خلال وضع أدوات إضافية فوق إدارة معلومات الأمان والأحداث (SIEM)، أو تطوير أجيال جديدة باستخدام المكونات الإضافية للتعلم الآلي والتحليلات السلوكية. لكن ظل الطلب على أداة توفر تنبيهات ذات جودة أفضل وتسهيلات أسرع، قائمًا.

SOAR

ظهرت أدوات التنسيق الأمني والاستجابة الآلية (SOAR) في عام 2015 لحل بعض الأخطاء المذكورة أعلاه في أنظمة إدارة معلومات الأمان والأحداث (SIEM). تستوعب منصات التنسيق الأمني والاستجابة الآلية (SOAR) البيانات من مجموعة متنوعة من المصادر عبر البنية التحتية، بما في ذلك أنظمة الإدارة ومنصات معلومات التهديدات، وتوفر تحليل الأولويات. وتستطيع فرق الأمان بعد ذلك تكوين استجابات تلقائية متعددة المراحل ومتعددة الحلول للتهديدات الواردة، باستخدام دمج منصة التنسيق الأمني والاستجابة الآلية (SOAR) للنظام البيئي المتصل بواجهة برمجة التطبيقات لأدوات الأمان.

كيف يعمل التنسيق الأمني والاستجابة الآلية (SOAR)؟

هذه المرة، الاسم مفيد جدًا! وإليك السبب:
أتمتة أدوات التنسيق الأمني والاستجابة الآلية (SOAR). على الرغم من أن هذه الأدوات معروفة غالبًا بقدرتها على أتمتة عمليات الاستجابة للحوادث، إلا أنها يمكنها في الواقع أتمتة مجموعة واسعة من مهام سير العمل، بما في ذلك فحص الثغرات الأمنية، وتحليل السجل، وإدارة وصول المستخدم، وفرز التهديدات وغيرها.

تفعل ذلك باستخدام "كتب التشغيل" - مجموعات القواعد التي يتم تكوينها مسبقًا ويتم تشغيلها بواسطة أحداث معينة، والتي تخبر النظام بالخطوات التي يجب اتخاذها بعد ذلك في سير عمل محدد. ويصاحب معظم حلول التنسيق الأمني والاستجابة الآلية (SOAR) مئات من أدلة التشغيل الجاهزة للاستخدام، التي تغطي المهام الأكثر شيوعًا من التي تواجهها فرق مركز عمليات الأمن. وتستطيع الفرق بعد ذلك تكوين كتب التشغيل الخاصة بها لأتمتة العمليات المتكررة الأخرى الأكثر تحديدًا التي قد تكون لديهم.

ثم يتولون التنسيق. وبينما تشير الأتمتة إلى التنفيذ الآلي للمهام الفردية ضمن سير عمل واحد، فإن التنسيق يشير إلى تنسيق أدوات وعمليات متباينة متعددة في سير عمل أكبر، وجمع كل البيانات ذات الصلة في منصة واحدة للحصول على معلومات موحدة ويمكن اتخاذ إجراءات بناءً عليها.

العلاقة بين إدارة معلومات الأمان والأحداث (SIEM) والتنسيق الأمني والاستجابة الآلية (SOAR)

في العادة، يتم استخدام إدارة معلومات الأمان والأحداث (SIEM) جنبًا إلى جنب مع أدوات التنسيق الأمني والاستجابة الآلية (SOAR) في ما يشبه العلاقة بين المساعد والمدير: تجمع أداة إدارة معلومات الأمان والأحداث (SIEM) جميع السجلات، وتربطها للعثور على التنبيهات، وتقدم هذه المعلومات إلى أدوات التنسيق الأمني والاستجابة الآلية (SOAR)، التي يمكنها بعد ذلك أخذ زمام المبادرة في إجراءات الاستجابة.

قيود التنسيق الأمني والاستجابة الآلية (SOAR)

كل شيء يبدو رائعًا للغاية، أليس كذلك؟ يتطلب الحفاظ على منصة جيدة التكوين للتنسيق الأمني والاستجابة الآلية (SOAR) التي تتكامل مع أدوات الشركاء جهدًا مستمرًا من مركز عمليات أمن (SOC) متطور ويتمتع بالمهارات العالية - وهو مصدر لا تمتلكه العديد من المؤسسات في الوقت الحالي، نظرًا للفجوة الحالية في مهارات الأمن الإلكتروني.

بدون عملية الصيانة الماهرة واليقظة هذه، يمكن أن ينتهي الأمر بتلقي محللي التنسيق الأمني والاستجابة الآلية (SOAR) لعدد كبير جدًا من التنبيهات ذات الأولوية المنخفضة، والنتائج الإيجابية الكاذبة، ومجموعة بيانات غير متماسكة بشكل عام نتيجة لجميع الأدوات المنعزلة المتنوعة التي تغذي المنصة - وهو بالضبط ما كانوا يحاولون تجنبه.

XDR

XDR هو حل أمني محلي أو قائم على السحابة، ويندرج ضمن فئتين على نطاق واسع: أصلي وهجين. ويمثل حل XDR الأصلي مجموعة موحدة من الأدوات من بائع واحد، بينما يدمج حل XDR الهجين حلول الجهات الخارجية الأخرى في نظامك البيئي. واُستخدم مصطلح "XDR" لأول مرة في عام 2018، حيث يشير الحرف "X" إلى "eXtended" التي تعني "موسع": و"يمتد" حل XDR إلى ما هو أبعد من أدوات اكتشاف نقطة النهاية التقليدية والاستجابة لها وحمايتها (EDR وEPP) من خلال جمع البيانات وربطها من طبقات أمان متعددة، بما في ذلك البريد الإلكتروني والسحابة والشبكة، لتوفير حماية شاملة عبر البنية التحتية لتقنية المعلومات بأكملها.

لذا، فهي منصة واحدة تنسق مجموعة من الأدوات، وتستخدم التعلم الآلي والأتمتة لمساعدة فرق الأمان على حماية النظام البيئي الأمني بأكمله... يبدو الأمر مشابهًا بعض الشيء للتنسيق الأمني والاستجابة الآلية (SOAR)، أليس كذلك؟ لكن هناك بعض الفروق الأساسية. دعنا نلقِ نظرة..

XDR مقابل SOAR: ما الفرق؟

1. ترتكز حلول XDR على بيانات نقطة النهاية وتحسينها - يعني هذا أن اكتشاف الحوادث والاستجابة لها تعد ميزة تصميم مركزية، مما يمنحها إمكانات تحليل متقدمة لا تمتلكها أدوات التنسيق الأمني والاستجابة الآلية (SOAR) عادةً. وتعتبر أدوات XDR بارعة في اكتشاف التهديدات غير المعروفة والفورية، والاستفادة من الذكاء الاصطناعي القوي وخوارزميات التعلم الآلي وذكاء التهديدات لحماية المؤسسة خارج حدودها. ومن ناحية أخرى، تستطيع أدوات التنسيق الأمني والاستجابة الآلية (SOAR) تقديم مجموعة متنوعة من حالات الاستخدام، حيث يمكنها تنسيق وأتمتة أي عمليات عبر البنية التحتية - وليس فقط الاستجابة للحوادث.

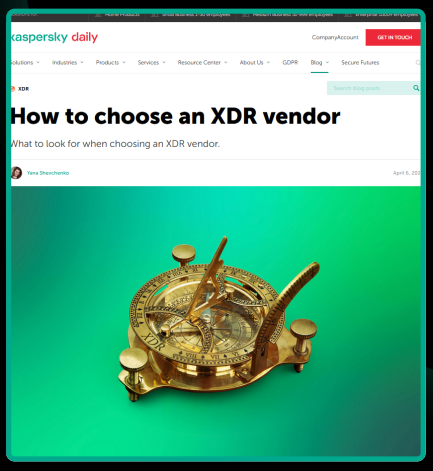
2. يمكن اعتبار XDR مثل حل تنسيق أمني واستجابة آلية خفيف، وهي واجهة مبسطة تقدم استجابات تلقائية بنقرة واحدة للتهديدات والتنبيهات الواردة. ويمكن أن يكون هذا أكثر ملاءمة للمؤسسة التي لا تمتلك المصادر اللازمة للحفاظ على تعقيد نظام التنسيق الأمني والاستجابة الآلية (SOAR) الذي يتمتع بتكوين جيد.

3. يتيح حل XDR الدمج السلس بين المنتجات - سواء عبر مجموعة أدوات لبائع واحد، أو منتجات الجهات الخارجية أيضًا، ويتفوق حل XDR في إمكانية التشغيل التفاعلي السلس. وتواجه أدوات التنسيق الأمني والاستجابة الآلية (SOAR) في الغالب صعوبة في محاولة دمج جميع الأدوات المنعزلة والمتباينة في مجموعتها؛ ويفكك حل XDR هذه المستودعات للاستجابة الفعالة والشاملة للتهديدات.

كيف تختار بائع حل XDR؟

لحق العديد من بائعي الأمن الإلكتروني بركب حل XDR لتقديم حلولهم الخاصة. كيف يمكنك معرفة ما إذا كنت تحصل على منتج لائق؟ تحقق من دليلنا المفيد:

https://www.kaspersky.com/blog/choosing-xdr-vendor/44063/



حسنًا، هل سيحل XDR محل SIEM وSOAR؟

لا تزال هيئة المحلفين غير متأكدة من هذا الأمر، لأن تقنية XDR تقنية جديدة نسبيًا يحدث تطوير مستمر لها. وفي الوقت الحالي، يوصي معظم الخبراء باتباع نهج متكامل، حيث يوفر كل حل مزايا تكمل الحلول الأخرى:

- SIEM — تتضمن إدارة معلومات الأمان والأحداث (SIEM) حالات استخدام خارج اكتشاف التهديدات، مثل إدارة السجل والامتثال وتحليل البيانات غير المتعلقة بالتهديدات.
- SOAR — تعد قابلية التخصيص الرائعة لكتب تشغيل التنسيق الأمني والاستجابة الآلية (SOAR) مفيدة لتنسيق العمليات وأتمتتها عبر البنية التحتية للمؤسسة.
- XDR - عندما يتعلق الأمر باكتشاف التهديدات والاستجابة لها، فإن التحليلات المتقدمة لحل XDR توفر حماية معززة لا مثيل لها.

هل تبحث عن حل مجرب ومختبر ويستطيع خبراؤك التكيف معه؟

يوفر Kaspersky Expert Security، وهو حل XDR مستند إلى حل EDR سحابي أصلي، لمؤسستك رؤية ووظائف محسنة للاكتشاف المستند إلى الذكاء الاصطناعي ومنطق الاستجابة التلقائية عبر جميع نقاط النهاية والشبكة، مما يسهل مجموعة واسعة من سيناريوهات الاستجابة التلقائية للحوادث. وتندمج التقنية المتقدمة المدمجة في المنصة للاكتشاف والتحليل من خلال معلومات التهديدات الرائدة عالميًا. وتوفر البنية الموحدة لحل Kaspersky XDR إدارة مركزية من وحدة تحكم واحدة على الويب. لمعرفة المزيد، يرجى زيارة go.kaspersky.com/expert.

me.kaspersky.com