kaspersky BRING ON THE FUTURE

XDR vs. SIEM vs. SOAR

Zu viele Akronyme verwirren Sie? Finden wir heraus, was sich hinter diesen Buchstabenkombinationen verbirgt...

Einleitung

SIEM, SOAR, MDR, EDR, EPP, XDR... fühlen Sie sich verwirrt, verloren im Dschungel der Akronyme der Cybersicherheit? Das ist verständlich — deshalb haben wir diesen hilfreichen Leitfaden erstellt, um die Unterschiede zwischen drei der großen Systeme herauszuarbeiten: SIEM, SOAR und XDR. Was verbirgt sich hinter diesen Akronymen? Wie kommt es, dass die Branche diese verwirrenden, sich überschneidenden Begriffe entwickelt hat? Haben sie überhaupt eine eindeutige Bedeutung, oder sind sie nur ein Marketing-Gag? Was sind die Gemeinsamkeiten und Unterschiede? Können sie sich gegenseitig ergänzen oder stehen sie in Konkurrenz zueinander?

Begleiten Sie uns auf dieser Suche! Lasst uns unsere Macheten des Wissens in die Hand nehmen, uns durch den Wald der Akronyme und des Jargons hacken und auf eine offene Lichtung des klaren Verständnisses kommen!

SIEM

Sicherheitsinformations- und Ereignisverwaltung (SIEM) ist eine Reihe von Tools und Diensten, die Sicherheitsereignisverwaltung (SEM) und Sicherheitsinformationsverwaltung (SIM) in einer einzigen Plattform vereinen. SIEM sammelt, aggregiert, analysiert und speichert Protokolldaten aus der gesamten IT-Infrastruktur für verschiedene Anwendungsfälle, einschließlich Governance und Compliance, und regelbasierten Korrelationsabgleich für verdächtige Aktivitäten.

Wie funktioniert SIEM?

Die ersten SIEM-Dienste wurden bereits 2005 entwickelt. Ihr ursprünglicher Zweck war die Sammlung und Speicherung von Protokollen und Ereignissen aus der gesamten IT-Infrastruktur eines Unternehmens — einschließlich Endpunkten, Anwendungen und Netzwerkgeräten — zu Zwecken der Compliance-Berichterstattung. Das SIEM führt Korrelationen mit diesem Datensatz durch, sucht nach Mustern oder Ereignissen, die auf verdächtiges Verhalten hindeuten könnten, und generiert einen Alarm für das Security Operations Center (SOC). Sicherheitsanalysten erkannten bald die Möglichkeit, diese Warnungen nicht nur für Compliance- und Governance-Zwecke zu nutzen, sondern auch, um den Fortschritt bösartiger Aktivitäten im Ökosystem proaktiv zu erkennen und zu stoppen.

Einschränkungen von SIEM

Das Problem bestand darin, dass SIEM-Dienste nicht speziell für die Erkennung von und Reaktion auf Zwischenfälle konzipiert waren. Das machte die Arbeit mit ihnen aus mehreren Gründen etwas schwierig:

- Zu viele Warnungen — Der riesige Datensatz, der vom SIEM bereitgestellt wird, muss manuell gefiltert, verarbeitet und analysiert werden, was für Sicherheitsanalysten, die versuchen, Angriffe in einer schnelllebigen Bedrohungslandschaft zu verhindern, nicht sehr praktisch ist.

- Kein Kontext — Um neuen, komplexen und ausgeklügelten Angriffen begegnen zu können, benötigen Sicherheitsanalysten ein kontextbezogenes, kohärentes Bild der Bedrohungslandschaft des Unternehmens und nicht die unzusammenhängenden Datenströme, die das SIEM liefert.

- Zu passiv — Das Blockieren verdächtiger Prozesse, die Quarantäne von Dateien und andere Reaktionsmöglichkeiten gehören nicht zu SIEMs Aufgabenbereich, denn es ist im Grunde ein passives, analytisches Tool.

Sicherheitsexperten haben versucht, diese Probleme zu lösen, indem sie zusätzliche Tools auf das SIEM aufsetzten oder neue Generationen mit Plugins für maschinelles Lernen und Verhaltensanalysen entwickelten. Aber die Nachfrage nach einem Werkzeug, das bessere Qualitätswarnungen liefert und schnellere, automatisierte Prozesse ermöglicht, blieb bestehen.

SOAR

SOAR-Tools (Security Orchestration & Automated Response) kamen 2015 auf den Markt, um einige der oben erwähnten Mängel in SIEM-Systemen zu beheben. SOAR-Plattformen nehmen Daten aus einer Vielzahl von Quellen in der gesamten Infrastruktur auf, darunter Managementsysteme und Bedrohungsdatenplattformen, und bieten Prioritätsanalysen. Sicherheitsteams können dann mehrstufige, lösungsübergreifende automatisierte Reaktionen auf eingehende Bedrohungen konfigurieren, indem sie die SOAR-Plattform mit einem API-verbundenen Ökosystem von Sicherheitstools verbinden.

Wie funktioniert SOAR?

Diesmal ist der Name sogar recht hilfreich! Hier erfahren Sie, warum:
SOAR-Tools automatisieren. Diese Tools sind zwar oft am besten für ihre Fähigkeit bekannt, Prozesse zur Reaktion auf Vorfälle zu automatisieren, können aber auch eine breite Palette von Arbeitsabläufen automatisieren, einschließlich Schwachstellen-Scans, Protokollanalysen, Benutzerzugriffsverwaltung, Bedrohungsauswertung und vieles mehr.

Dabei handelt es sich um vorkonfigurierte Regeln, die durch bestimmte Ereignisse ausgelöst werden und dem System mitteilen, welche Schritte als nächstes in einem bestimmten Arbeitsablauf unternommen werden sollen. Die meisten SOAR-Lösungen werden mit Hunderten von einsatzbereiten Playbooks geliefert, die die häufigsten Aufgaben von SOC-Teams abdecken. Teams können dann ihre eigenen Playbooks konfigurieren, um andere, spezifischere, sich wiederholende Prozesse zu automatisieren.

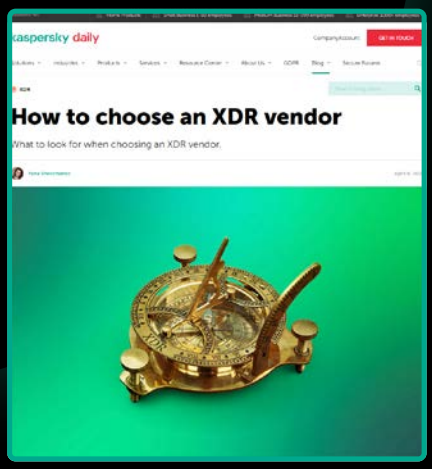
Dann orchestrieren sie. Während sich die Automatisierung auf die maschinengesteuerte Ausführung einzelner Aufgaben innerhalb eines einzelnen Arbeitsablaufs bezieht, bedeutet Orchestrierung die Koordinierung mehrerer unterschiedlicher Tools und Prozesse in einem größeren Arbeitsablauf, wobei alle relevanten Daten in einer einzigen Plattform für konsolidierte, umsetzbare Informationen zusammengefasst werden.

Der Zusammenhang zwischen SIEM und SOAR

Normalerweise wird ein SIEM zusammen mit SOAR-Tools in einer Art Assistenten-Manager-Beziehung eingesetzt: Das SIEM sammelt alle Protokolle, korreliert sie, um Warnungen zu finden, und leitet diese Informationen an das SOAR weiter, das dann die Reaktionsmaßnahmen einleiten kann.

Wie wählt man einen XDR-Anbieter aus?

Viele Anbieter von Cybersicherheitslösungen sind mit ihren eigenen Lösungen auf den XDR-Zug aufgesprungen. Wie können Sie wissen, ob Sie ein gutes Produkt erhalten? Erfahren Sie mehr in unserem Leitfaden: https://www.kaspersky.de/blog/choosing-xdr-vendor/28440/



Einschränkungen von SOAR

Klingt doch alles ganz toll, oder? Das Problem ist, dass die Pflege einer gut konfigurierten SOAR-Plattform, die mit Partner-Tools integriert werden kann, den kontinuierlichen Einsatz eines hochqualifizierten, ausgereiften SOC erfordert — eine Ressource, über die viele Unternehmen angesichts der aktuellen Qualifikationslücke im Bereich Cybersicherheit derzeit nicht verfügen.

Ohne eine solche qualifizierte, wachsame Wartung können SOAR-Analysten am Ende zu viele Warnmeldungen mit niedriger Priorität, Fehlalarme und einen allgemein inkohärenten Datensatz erhalten, der aus all den verschiedenen, isolierten Tools resultiert, die in die Plattform eingespeist werden — genau das, was sie eigentlich vermeiden wollten.

XDR

XDR ist eine vor Ort oder in der Cloud installierte Sicherheitslösung, die im Wesentlichen in zwei Kategorien unterteilt werden kann: nativ und hybrid. Das native XDR ist eine einheitliche Suite von Tools eines einzigen Anbieters, während das hybride XDR andere Lösungen von Drittanbietern in Ihr Ökosystem integriert. Der Begriff „XDR“ wurde erstmals 2018 verwendet, wobei das „X“ für „eXtended“ steht: XDR geht über die traditionellen Endpunkt-Erkennungs-, Reaktions- und Schutz-Tools (EDR und EPP) hinaus, indem es Daten aus mehreren Sicherheitsebenen, einschließlich E-Mail, Cloud und Netzwerk, sammelt und korreliert, um umfassenden Schutz für die gesamte IT-Infrastruktur zu bieten.

Es handelt sich also um eine einzige Plattform, die eine Reihe von Tools koordiniert und maschinelles Lernen und Automatisierung einsetzt, um Sicherheitsteams beim Schutz des gesamten Sicherheitsökosystems zu unterstützen... klingt ein bisschen wie SOAR, oder? Es gibt jedoch einige grundlegende Unterschiede. Sehen wir uns dies einmal näher an ...

XDR vs. SOAR: Was ist der Unterschied?

1. XDR-Lösungen sind in Endpunktdaten und -optimierung verankert — das bedeutet, dass die Erkennung von und Reaktion auf Vorfälle ein zentrales Konstruktionsmerkmal ist, was ihnen erweiterte Analysefunktionen verleiht, die SOAR-Tools in der Regel nicht haben. XDR-Tools sind Meister im Aufspüren unbekannter und Zero-Day-Bedrohungen und nutzen leistungsstarke künstliche Intelligenz, Algorithmen für maschinelles Lernen und Bedrohungsdaten, um ein Unternehmen über seine Grenzen hinaus zu schützen. Andererseits bieten SOAR-Tools ein viel breiteres Spektrum an Anwendungsfällen, da sie alle Prozesse in der gesamten Infrastruktur orchestrieren und automatisieren können — nicht nur die Reaktion auf Vorfälle.

2. XDR kann als etwas wie SOAR-lite betrachtet werden — eine optimierte Schnittstelle, die mit einem Klick automatische Antworten auf eingehende Bedrohungen und Warnungen bietet. Dies kann für eine Organisation, die nicht über die Ressourcen verfügt, um die Komplexität einer gut konfigurierten SOAR-Plattform aufrechtzuerhalten, sehr viel bequemer sein.

3. XDR ermöglicht eine reibungslose produktübergreifende Integration — ob mit den Tools eines einzelnen Anbieters oder mit Produkten von Drittanbietern, XDR zeichnet sich durch eine nahtlose Interoperabilität aus. SOAR-Tools haben oft das Problem, all die unterschiedlichen, isolierten Tools in ihrem Stack zu integrieren. XDR bricht diese Silos auf und ermöglicht so eine effiziente, ganzheitliche Reaktion auf Bedrohungen.

Wird XDR also SIEM und SOAR ersetzen?

Die Entscheidung darüber steht noch aus, da es sich bei XDR um eine relativ neue Technologie handelt, die ständig weiterentwickelt wird. Derzeit empfehlen die meisten Experten einen integrierten Ansatz, da jede Lösung Vorteile bietet, die die anderen ergänzen:

- SIEM — das SIEM kann auch außerhalb der Bedrohungserkennung eingesetzt werden, z. B. für die Protokollverwaltung, die Einhaltung von Vorschriften und die Analyse von Daten, die nicht mit Bedrohungen zusammenhängen.

- SOAR — die große Anpassungsfähigkeit von SOAR-Playbooks ist nützlich für die Orchestrierung und Automatisierung von Prozessen in der gesamten Infrastruktur des Unternehmens.

- XDR — Wenn es darum geht, Bedrohungen zu erkennen und auf sie zu reagieren, bieten die fortschrittlichen Analysen einer XDR-Lösung einen verbesserten Schutz, der seinesgleichen sucht.

Sie suchen eine erprobte und anpassungsfähige Lösung für Ihre Experten? Kaspersky Expert Security, XDR basiert auf einer cloud-nativen EDR-Lösung und bietet Ihrem Unternehmen eine verbesserte Sichtbarkeit und Funktionalität für die KI-basierte Erkennung und die automatische Reaktionslogik auf allen Endgeräten und im Netzwerk, was eine Vielzahl von Szenarien für die automatische Reaktion auf Vorfälle ermöglicht. Die in der Plattform integrierte fortschrittliche Technologie zur Erkennung und Analyse wird durch weltweit führende Bedrohungsdaten ergänzt. Die einheitliche Architektur von Kaspersky XDR ermöglicht eine zentrale Verwaltung über eine einzige Webkonsole. Hier erfahren Sie mehr: go.kaspersky.com/expert

www.kaspersky.de

© 2022 AO Kaspersky Lab.
Eingetragene Marken und Servicemarken
sind Eigentum ihrer jeweiligen Rechtsinhaber.