WHITEPAPER

Die 10 wichtigsten Funktionen einer erstklassigen SOAR-Lösung

Mit Sicherheitsorchestrierung, Automatisierung und Reaktion schneller auf Bedrohungen reagieren

splunk> turn data into doing

Cybersicherheit entwickelt sich weiter

Wenn Sie Sicherheitsfachleute zu den Herausforderungen befragen, die ihnen bei ihrer Arbeit im Bereich Cybersecurity begegnen, können Sie davon ausgehen, dass sie sich bei einigen Themen alle einig sind. Dazu gehören u. a.:

- Fachkräftemangel im Bereich Cybersicherheit
- Ein große Anzahl an Sicherheitswarnungen
- Zu viele Punktlösungen, die kaum noch verwaltbar sind
- Mangelnde Integration zwischen diesen Produkten
- Unfähigkeit zur Skalierung von Sicherheitsprozessen
- Steigende Kosten und schrumpfende Budgets
- Immer ausgefeiltere Malware.
- Zu langsame Bedrohungserkennung und Reaktion.

Angesichts dieser Herausforderungen ist es kein Wunder, dass sich Sicherheitsteams ständig überfordert fühlen.

Viele Teams greifen zu SOAR-Tools (Sicherheitsorchestrierung, Automatisierung und Reaktion), um Abhilfe zu schaffen. Mit einer SOAR-Lösung lassen sich Sicherheitsaufgaben (wie z. B. Untersuchung, Sichtung und Reaktion) mit verschiedenen den Teams zur Verfügung stehenden Sicherheitsprodukten orchestrieren, während manuelle, wiederkehrende Sicherheitsaufgaben automatisiert werden können.

Allerdings sind nicht alle SOAR-Lösungen gleich aufgebaut. Eine erstklassige SOAR-Lösung bietet eine Reihe von Funktionen, die die Herangehensweise Ihres Teams an den Sicherheitsbetrieb komplett revolutionieren kann. Diese Funktionen ermöglichen Ihnen zum Beispiel:

- Intelligenteres Arbeiten durch die Automatisierung manueller und wiederkehrender Aufgaben
- Schnellere Reaktion und kürzere Verweildauer durch automatisierte Erkennung, Untersuchung und Reaktion
- Unterstützung Ihres Sicherheitsteams bei der Automatisierung von Sicherheitsprozessen, damit mehr Zeit für andere strategische Aktivitäten bleibt.

Im Folgenden sind die 10 wichtigsten Funktionen einer erstklassigen SOAR-Lösung aufgeführt, mit denen Ihr zuvor überfordertes Security-Team wieder die Kontrolle über den Sicherheitsbetrieb gewinnt.

Sehen wir uns diese Funktionen im Einzelnen an:

Die wichtigsten Funktionen einer erstklassigen SOAR-Lösung	
Orchestrierung	Dabei handelt es sich um die maschinengestützte Koordination einer Reihe von Sicherheitsmaßnahmen innerhalb eines komplexen IT-Ökosystems. Dies hilft sicherzustellen, dass alle Tools und Systeme aufeinander abgestimmt sind, während Aufgaben über alle Produkte und Workflows hinweg automatisiert werden.
Automatisierung	Die maschinengestützte Ausführung von Sicherheitsmaßnahmen mit der Möglichkeit, Bedrohungen programmgesteuert, ohne das Eingreifen des Menschen zu erkennen, zu untersuchen und zu beheben. Die Sicherheitsautomatisierung übernimmt einen Großteil der Arbeit der Analysten, sodass sie nicht mehr jede eingehende Benachrichtigung manuell beurteilen und behandeln müssen.
Management von Events und Warnmeldungen	Nachdem die Daten in einer SOAR-Lösung erfasst worden sind, sollten eingehende Warnmeldungen in eine Warteschlange gestellt und priorisiert werden. Anschließend sollten Untersuchungen unter Einsatz manueller oder automatisierter Maßnahmen durchgeführt werden, sodass für ein Maximum an Produktivität und Genauigkeit gesorgt ist.
Threat Intelligence / Bedrohungsinformationen	Sicherheitsteams sollten in der Lage sein, die neuesten Bedrohungsinformationen auszuwerten, ohne dabei ihre Ressourcen ausschöpfen zu müssen. Effektive Threat Intelligence sollten darüber hinaus Bewertungsoptionen beinhalten, um zu ermitteln, auf welche Quellen sich die Analysten bei den Bedrohungsinformationen konzentrieren sollten.
Ticket-Management und Zusammenarbeit	Beim Ticket-Management sollte ein umfassenderer funktionsübergreifender Blick auf den Lebenzyklus eines Vorfalls, von seiner Entstehung bis zu seiner Behebung, gerichtet werden. Es sollte die Möglichkeit geben, mehrere Warnmeldungen und/oder Events gemeinsam als einen einzigen Fall bestätigen, aggregieren und eskalieren zu können. Dies wiederum ermöglich eine effektive Zusammenarbeit und Kommunikation im gesamten Sicherheitsteam der Organisation, sodass die Behebung von sicherheitsrelevanten Ereignissen beschleunigt wird.

Metriken und Berichte	Metriken und Berichte werden benötigt, um so gut wie alles zu verstehen und zu quantifizieren. Eine SOAR-Lösung ist da keine Ausnahme. Mithilfe von Metriken wird die Effektivität einer SOAR-Lösung gemessen, und es wird ermittelt, wo zur Steigerung des ROI Verbesserungen vorgenommen werden können.
Mobilität	Es ist wichtig, dass eine SOAR-Lösung Zugriffs-, Interaktivitäts- und Kontrollfunktionen bietet, auf die Analysten über ihre Mobilgeräte zugreifen können. Auf diese Weise können Analysten ganz ohne Laptop unterwegs Playbooks ausführen, Sicherheitsartefakte überprüfen, Events triagieren und mit einem Fingerzeig auf Mitteilungen reagieren sowie immer erreichbar sein, ganz gleich, wo sie gerade sind.
Skalierbarkeit	Eine SOAR-Lösung sollte gemeinsam mit Ihrer Organisation wachsen. Da im Laufe der Zeit immer mehr Anwendungsfälle hinzukommen, sollte die Plattform so konzipiert sein, dass sie vertikales Skalieren durch Aufstockung der Hardware-Ressourcen (z. B. CPU und RAM) und horizontales Skalieren durch mehr Serverinstanzen zur Unterstützung der Bereitstellung ermöglicht.
Offenheit und Erweiterbarkeit	Eine SOAR-Lösung sollte offen und erweiterbar sein. Sie sollte problemlos neue Sicherheits-szenarios, neue Produkte, neue Aktionen und neue Playbooks integrieren können.
Community-Unterstützung	Eine SOAR-Lösung sollte durch Nutzung eines offenen Ökosystems für die Entwicklung von Anwendungen ein Community-Modell unterstützen. Auf diese Weise lässt sich der Erfolg langfristig sichern, da ein Vendor Lock-in vermieden wird und Technologien problemlos ein- und ausgewechselt werden können, ohne dass sich dies negativ auf automatisierte Playbooks auswirkt.

Orchestrierung

Sicherheitsteams nutzen zur Reaktion auf einen Sicherheits-Incident eine Vielzahl verschiedener Security-Tools. Jedes dieser Tools spielt innerhalb eines definierten Workflows eine bestimmte Rolle. Beispielsweise können Sie VirusTotal anweisen, die Reputation einer Datei zu prüfen, die Firewall zu verwenden, um eine IP zu blockieren, und das Endpoint Security-Tool zu nutzen, um eine ausführbare Datei zu blockieren. Ohne Orchestrierung müsste das Sicherheitsteam diese Abläufe manuell koordinieren. Eine SOAR-Lösung wird dagegen über ihre API in alle eingesetzten Sicherheitstools integriert und koordiniert dann die Arbeitsabläufe dieser Tools, um Sicherheitsvorfälle zu erkennen, zu untersuchen oder auf sie zu reagieren. Wenn Sie sich Ihre Sicherheits-Tools beispielsweise als Sinfonieorchester vorstellen, ist Ihre SOAR-Lösung der Dirigent, der dafür sorgt, dass alle Instrumente synchron und harmonisch aufeinander abgestimmt spielen.

Bei der Evaluierung einer SOAR-Lösung sollte die Orchestrierungsfunktion alle Aktivitäten in Verbindung mit einem bestimmten Sicherheitsszenario von Anfang bis Ende anleiten und überwachen und darüber hinaus in der Lage sein, Daten aus allen Datenquellen und in beliebigem Format zu erfassen. Außerdem sollte bei der Orchestrierung dafür gesorgt werden, dass die nach einer Aktion ausgegebenen Daten ordnungsgemäß analysiert, normalisiert und strukturiert werden, sodass bei zukünftigen Aktionen darauf zurückgegriffen werden kann.

Automatisierung

Die Tage der meisten Analysten sind mit zu vielen sich wiederholenden und langweiligen Sicherheitsaufgaben und -aktionen gefüllt. Diese Aktionen führt das Team zudem manuell aus. Bei der Automatisierung mithilfe von Playbooks sollte das Sicherheitsteam bestimmte Aktionen aus diesem Bereich in Sekunden statt in Minuten oder Stunden – und zuweilen sogar Tagen oder Wochen – ausführen können. Phishing-Untersuchungen z. B., die u. U. mehrere Aktionen mit vier bis fünf verschiedenen Sicherheits-Tools erfordern und bei manueller Ausführung ca. 40 Minuten in Anspruch nehmen, sollten bei Verwendung eines automatisierten Playbooks weniger als eine Minute dauern. Auf diese Weise können SOAR-Tools die MTTD (Mean Time to Detect) und die MTTR (Mean-Time-To-Resolution) drastisch reduzieren.

Playbooks sollten leicht erstellt und modifiziert werden können. Im Automatisierungs-Editor innerhalb einer SOAR-Lösung kodifizieren Analysten oder Manager ihre Prozesse in Automatisierungs-Playbooks. Der Editor sollte sowohl das Editieren des Quellcodes als auch visuelles Editieren ermöglichen. Auf diese Weise können Sicherheitsteams unabhängig von ihren Vorlieben und Coding-Kenntnissen umfassende und ausgeklügelte Playbooks erstellen. Beim Erstellen eines Playbooks in einem visuellen Editor sollte der daraus resultierende Quellcode des Playbooks in Echtzeit

generiert werden und vom Verfasser aufgerufen werden können, indem er nahtlos zwischen dem visuellen und dem Quellcode-Editor hin und herwechselt und sie bearbeitet.

Management von Events und Warnmeldungen

Direkt nach der Datenerfassung sollte das Event- und Warnmeldungsmanagement eine Warteschlange erstellen und eingehende Events und Warnmeldungen priorisieren. Das bedeutet, dass Warnmeldungen schnell erfasst und effizient bearbeitet werden können, ohne dass erst aufwendig gesucht oder zwischen verschiedenen Kontexten hin und hergewechselt werden muss. Events und Warnmeldungen sollten eine Statusanzeige (z. B. neu, offen oder geschlossen), eine Schweregradanzeige und eine farbkodierte Sensibilitätsanzeige enthalten, damit die Informationen schnell verarbeitet werden können. Die technischen Attribute eines Security-Events oder einer Sicherheitswarnmeldung sollten so strukturiert werden, dass das Sicherheitsszenario schnell verstanden werden kann. Dazu gehört eine strukturierte Ansicht der Daten wie z. B. der IPs, Domänen, Datei-Hashes, Benutzernamen und E-Mail-Adressen. Ein Sicherheitsanalyst sollte in der Lage sein, nahtlos investigative, eindämmende oder reaktive Maßnahmen (oder eine Reihe von Aktionen, d. h. Playbooks) zu diesen Daten einzuleiten.

Schließlich sollte die SOAR-Lösung ein umfassendes Aktivitätsprotokoll bereitstellen, in dem ein Datensatz mit allen Aktionen enthalten ist, die zu einem Event oder einer Warnmeldung ausgeführt worden sind, ganz gleich, ob sie manuell oder mittels eines Playbooks initiiert worden sind. Zu jeder Aktion sollten die Ergebnisse angezeigt werden, einschließlich der Angabe, ob sie erfolgreich war oder nicht.

Threat Intelligence / Bedrohungsinformationen

Bedrohungsinformationen geben Analysten entscheidende Einblicke in die Aktionen des Angreifers, damit sie weiteren Schaden vom Unternehmen abwenden können. Unterschiedliche Arten von Informationen, nämlich strategische, technische und operative, werden aus externen und internen Quellen erfasst und konsolidiert. Nachdem die Informationen an einem zentralen Ort aggregiert wurden, werden die Daten im Zusammenhang mit ihrer Quelle und Zuverlässigkeit bewertet und analysiert, um zu ermitteln, welche Daten für rasche und wirksame Entscheidungen wichtig sind.

Viele Sicherheitsteams nutzen heutzutage Bedrohungsinformationen, um relevante Kontextinformationen zu erhalten, auf deren Grundlage Analysten sich ein genaues Bild von den Bedrohungen machen können. Allerdings wechseln sie dafür oftmals zwischen einer Reihe von Produktoberflächen hin und her, um die Verbindungen zwischen verschiedenen Informationen herzustellen. Selbst bei Nutzung von Bedrohungsdaten-Feeds kann eine unüberschaubare Menge an Indikatoren gesendet werden, denen man unmöglich manuell nachgehen kann. Durch den Einsatz von Orchestrierung und Automatisierung können Security-Teams sich auf einer einzigen Plattform rasch einen Überblick über alle aggregierten Informationen verschaffen und schnell fundierte Entscheidungen treffen, die sich so automatisieren lassen, dass kein menschliches Eingreifen mehr erforderlich ist.

Ticket-Management und Zusammenarbeit

Sobald Warnmeldungen oder Events bestätigt und eskaliert worden sind, sollten Ticket-Management-Komponenten greifen und einen breit angelegten, funktionsübergreifenden Lebenszyklus von der Erstellung bis zur Behebung in die Wege leiten. Das SOAR-Tool erfasst mehrere Events, bestätigt sie, fasst sie zusammen und eskaliert sie zu einem einzigen Fall. Die Ticket-Management-Oberfläche sollte die Einbindung relevanter technischer Daten, wie z. B. der Quelldaten und der Aktionsergebnisse, in den Fall unterstützen. Darüber hinaus sollte die Oberfläche die Einbindung relevanter, nicht technischer Daten, wie z. B. Hinweise, Memos, E-Mails, Screenshots, Aufnahmen oder sonstiger willkürlich ausgewählter, für den Fall relevanter Daten unterstützen. Jegliche Änderungen an einem Fall sollten in einem Audit-Trail protokolliert und exportiert werden können.

Das Ticket-Management sollte sich zudem problemlos den bestehenden Prozessen einer Organisation zuordnen lassen. Viele Organisationen haben Standardbetriebsverfahren (SOPs, Standard Operating Procedures) für die Reaktion auf Incidents entwickelt. Die Ticket-Management-Funktion sollte es den Benutzern ermöglichen, die einzelnen Prozesse in Phasen einzuteilen und als Vorlage zu speichern. Die Benutzer sollten in der Lage sein, die SOPs in mehrere Phasen mit jeweils einer oder mehreren Aufgaben zu untergliedern, von denen jede einem Besitzer zugewiesen werden kann. Die Oberfläche sollte sowohl den Fortschritt des Falls als auch den Fallstatus anzeigen können.

Eine erstklassige SOAR-Lösung sollte integrierte Funktionen für die Zusammenarbeit beinhalten. Funktionen für die Zusammenarbeit, wie z. B. eine integrierte Chat-

Funktion, sowie die Möglichkeit, Hinweise zu einem Fall einzubinden und freizugeben sollten in Verbindung mit dem Untersuchungs- und Response-Workflow ebenfalls zur Verfügung stehen, damit eine Zusammenarbeit nach Kontext möglich ist. Mithilfe einer Echtzeit-Chat-Funktion und Hinweisen zu Events, Warnmeldungen und Fallinformationen können Analysten sich einen Überblick über die jeweilige Situation verschaffen, um Sicherheitsvorfälle effizient und schnell beheben zu können. Auf diese Weise wird auch problemlos ein Audit-Trail erstellt. Am besten wird diese Zusammenarbeit gemeinsam mit den jeweiligen erfassten Event-Daten und -Aktionen erfasst und strukturiert. Das ist nicht ganz so einfach, wenn sich Ihre Kommunikation getrennt von den Workflow-Informationen in Ihrer SOAR-Lösung auf einem externen Tool befindet.

Metriken und Berichte

Ein Security-Team muss in der Lage sein, den Status seiner Sicherheitsprozesse problemlos zu messen und im Laufe der Zeit für eine kontinuierliche Verbesserung zu sorgen. Daher sind aussagekräftige Metriken und Berichte ein Muss. Durch sie versteht das Sicherheitsteam die Auswirkungen der Automatisierung und erfährt, wo zur Steigerung des ROI Verbesserungen vorgenommen werden können.

Die Automatisierung dient der Steigerung der Effizienz über mehrere Funktionen eines SOC (Security Operations Center) hinweg. Sie ist entscheidend, wenn es darum geht, den quantitativen Zuwachs der Leistung und die durch die Automatisierung ermöglichten Ressourceneinsparungen zu verstehen; außerdem werden diese Informationen auf einem Dashboard angezeigt.

Beispiele für wichtige Leistungsmetriken, die in einer SOAR-Lösung zur Verfügung stehen sollten, sind die MTTR (Mean Time To Resolve), die MDT (Mean Dwell Time), die durch die automatisierte Ausführung eingesparten Analystenstunden, die Anzahl der FTEs (Full-Time-Equivalents), die durch eine automatisierte Ausführung gewonnen werden, die durchschnittlich je Playbook-Ausführung eingesparte Zeit, das eingesparte Geld (FTE-Kosten x FTE-Gewinn), die Gesamtzahl der offenen Warnmeldungen, die pro Tag (Stunde, Woche, Monat) geöffneten und geschlossenen Warnmeldungen und die Leistung vor dem Hintergrund der Service Level Agreements (SLAs). All diese Informationen sollten für das gehobene Management und die CISOs strukturiert und in Berichten zusammengefasst werden, damit der Status ihrer Sicherheitsprozesse insgesamt sowie die Verbesserungen durch die SOAR-Lösung schnell verstanden werden können.

Mobilität

SOAR-Lösungen sind dazu vorgesehen, die Reaktionszeiten zu beschleunigen. Um schnelle Reaktionen zu erzielen, müssen Sicherheitsanalysten erreichbar sein, wenn ein Fall oder eine Sicherheitsanzeige das Eingreifen durch eine Person erfordert. Analysten sitzen jedoch nicht immer vor ihrem geöffneten Laptop am Schreibtisch, um sofort auf eine Anzeige zu reagieren.

Daher ist es so wichtig, Zugriffs-, Interaktivitäts- und Kontrollfunktionen über das Mobilgerät des Analysten zu bieten. Auf diese Weise können Analysten ganz ohne Laptop unterwegs Playbooks ausführen, Sicherheits-artefakte überprüfen, Events triagieren und fast wie nebenbei auf Anzeigen reagieren und immer erreichbar sein, ganz gleich, wo sie gerade sind.

Skalierbarkeit

Eine SOAR-Lösung sollte mit Ihnen und Ihrer Organisation wachsen. Während es unvermeidlich im Laufe der Zeit immer mehr Anwendungsfälle gibt, werden ständig weitere Verarbeitungsleistungen auf der Plattform hinterlegt.

Die Automatisierungs-Engine sollte so konzipiert sein, dass vertikales Skalieren (z. B. zur Steigerung der CPU- und RAM-Ressourcen) und horizontales Skalieren (z. B. zur Steigerung der Serverinstanzen) möglich ist, um die Leistung zu optimieren und den Automatisierungs-ROI zu schützen.

Offenheit und Erweiterbarkeit

Eine SOAR-Lösung sollte so konzipiert sein, dass sie offen und erweiterbar ist und dass sich problemlos neue Sicherheitsszenarios, neue Produkte, neue Maßnahmen und neue Playbooks integrieren lassen. Ist dies nicht der Fall, kann die SOAR-Lösung im Laufe der Zeit ihren Wert verlieren.

Mit einem offenen Ökosystem, das auf einem allgemeinen Standard und Programmiermodell basiert, können Sicherheitsteams von vielen Vorteilen profitieren. Neue Technologien lassen sich schnell in die Lösung integrieren, ohne dass die Kernplattform verändert werden muss und ohne dass automatisierte Playbooks davon negativ beeinflusst werden. Die Benutzer können weitere Integrationen entwickeln, ohne dass es dazu der Erlaubnis oder bestimmter Entwicklungszyklen seitens des SOAR-Anbieters bedarf. Beispielsweise können sie ihre eigenen Integrationen schreiben, selber Anwendungen entwickeln oder eine API für den Vorabzugriff über einen Anbieter schreiben.

Community-Unterstützung

Da sich das Thema Cyber Security ständig weiterentwickelt, müssen die jeweiligen Fachleute immer stärker zusammenarbeiten, um Playbooks, Best Practices und Strategien für den Umgang mit den neuesten Bedrohungen miteinander zu teilen. Eine SOAR-Lösung muss ein starkes Community-Modell unterstützen und die Freigabe von App-Integrationen und Playbooks erleichtern.

Das Messen der installierten Basis einer SOAR-Lösung ist ein guter Indikator für das Kooperationspotenzial der an sie angeschlossenen Community. Die meisten Benutzer profitieren am liebsten von den Erfahrungen anderer gleichgesinnter Benutzer. In einer großen Community aktiver Benutzer lassen sich Playbooks und Apps teilen und Ideen für neue Anwendungsfälle aus dem Bereich der Automatisierung entwickeln. Darüber hinaus ist die Engagement der Anbieter innerhalb der Community ein solider Indikator für ihr Commitment gegenüber der Community und zur Zusammenarbeit.

Kann eine SOAR-Lösung Sie bei der Optimierung Ihrer Sicherheitsprozesse unterstützen? Erfahren Sie, wie die branchenführende SOAR-Technologie von Splunk die Effizienz und Effektivität Ihres Sicherheitsteams optimieren kann.

splunk>

Weitere Informationen: www.splunk.de/asksales

www.splunk.de

22-23997-Splunk-10EssentialCapabilitiesofaBest-of-BreedSOAR-WP-108_GER