WHITEPAPER

Die 10 wichtigsten Funktionen einer erstklassigen SOAR-Lösung

Mithilfe von Automatisierung intelligenter arbeiten und schneller auf Bedrohungen reagieren

splunk>
turn data into doing™

Der Sicherheitsbetrieb muss sich weiterentwickeln

Wenn Sie eine Gruppe von Sicherheitsanalysten nach den größten Cybersicherheitsherausforderungen fragen, werden Sie einige der folgenden Themen wahrscheinlich immer wieder hören:

- Ein Mangel an qualifiziertem Nachwuchs im Bereich Cyber Security
- Eine hohe Anzahl von Sicherheitswarnmeldungen
- Zu viele einzelne Security-Produkte, die verwaltet werden müssen
- Mangelnde Interoperabilität zwischen diesen Produkten
- Die Unfähigkeit, den Sicherheitsbetrieb im Laufe der Zeit zu skalieren
- Steigende Kosten, schrumpfende Budgets
- Zunehmende Komplexität von Malware
- Langsame Erkennung von und Reaktion auf Bedrohungen

Angesichts dieser Herausforderungen ist es nicht überraschend, dass sich Sicherheitsteams ständig überfordert fühlen.

Viele Teams setzen als Abhilfemaßnahme auf SOAR-Tools (Security Orchestration, Automation and Response). Eine SOAR-Lösung kann Sicherheitsaktionen (wie Untersuchungen, Triage, Reaktion) über verschiedene Security-Produkte im Portfolio eines Teams orchestrieren und wiederkehrende Security-Aufgaben, die zuvor manuell verwaltet wurden, automatisieren.

Aber nicht alle SOAR-Tools sind gleich. Eine erstklassige SOAR-Lösung bietet eine Reihe von Funktionen, die die Art und Weise, wie Sie Ihren Sicherheitsbetrieb gestalten, völlig revolutionieren kann. Solche Fähigkeiten ermöglichen Ihnen:

- durch die Automatisierung manueller und wiederkehrender Aufgaben smarter zu arbeiten.
- schneller zu reagieren und die Wartezeit durch die automatisierte Erkennung, Untersuchung und Reaktion zu verkürzen.
- Ihre Verteidigung durch die Integration bestehender Sicherheitsinfrastruktur zu stärken, damit jeder Teil dieser Infrastruktur aktiv am Schutz Ihres Unternehmens mitwirkt.

Erstklassige SOAR-Tools weisen 10 Kernfunktionen auf, die es Ihnen ermöglichen, diese Ergebnisse zu erzielen.

Die wichtigsten Funktionen einer erstklassigen SOAR-Lösung	
Orchestrierung	Die maschinengestützte Koordination komplexer Arbeitsabläufe über verschiedene Sicherheits-Tools hinweg sollte die Effizienz und Geschwindigkeit Ihres Sicherheitsbetriebs erhöhen.
Automatisierung	Die maschinengestützte Ausführung von ansonsten manuellen, voneinander abhängigen Sicherheitsaktionen unter Verwendung von „Playbooks“ sollte es Ihnen ermöglichen, diese Aktionen in Sekunden statt in Stunden auszuführen.
Event- und Alarm-Management	Die Event- und Alarmmanagementfunktion eines SOAR-Tools sollte eingehende Sicherheitsereignisse und Warnungen in eine Warteschlange aufnehmen und priorisieren, um Ihre Analysten bei der effizienteren Triage zu unterstützen.
Ticket-Management	Eine Ticket-Management-Komponente sollte einen breiteren und funktionsübergreifenden Lebenszyklus (von der Erstellung bis zur Lösung) eines Sicherheitsfalls steuern.
Zusammenarbeit	Eine eingebaute Chat- und Kommentarfunktion kann die Kommunikation innerhalb des Sicherheitsteams erleichtern und das Beheben von Sicherheitsereignissen beschleunigen.
Metriken und Berichte	Metriken und Berichte sind entscheidend, um die Wirksamkeit des SOAR-Tools zu verstehen und zu erkennen, wo Verbesserungen zur Steigerung des ROI vorgenommen werden können.
Mobilität	Die Steuerung des SOAR-Tools von mobilen Geräten der Analysten aus ermöglicht schnellere Reaktionszeiten und eine einfache Triage der Warnmeldungen – egal wo sich Ihre Analysten gerade befinden.
Skalierbarkeit	Ein SOAR-Tool sollte mit Ihrem Unternehmen wachsen, denn während ein Unternehmen im Laufe der Zeit immer mehr Anwendungsfälle hinzufügt, muss die Plattform immer größere Verarbeitungslasten bewältigen.
Offenheit und Erweiterbarkeit	Ein SOAR-Tool sollte die Einbeziehung neuer Sicherheitsszenarien, neuer Produkte, neuer Aktionen und neuer Playbooks problemlos unterstützen.
Community-Unterstützung	Ein SOAR-Tool muss ein ausgeprägtes Community-Modell unterstützen und das Teilen von Integrationen und Playbooks auf einfache Weise ermöglichen.

Im Folgenden betrachten wir jede dieser Funktionen etwas detaillierter:

Orchestrierung

Orchestrierung ist definiert als die maschinengestützte Koordination komplexer Arbeitsabläufe über verschiedene Security-Tools hinweg und stellt eine wesentliche Funktion eines SOAR-Tools dar.

Sicherheitsteams nutzen zur Reaktion auf einen Sicherheits-Incident eine Vielzahl verschiedener Security-Tools. Jedes Tool spielt dabei innerhalb eines zuvor definierten Arbeitsablaufs eine andere Rolle. Zum Beispiel wird VirusTotal angewiesen, die Reputation einer Datei zu prüfen, es wird die Firewall verwendet, um eine IP zu blockieren, und das Endpoint Security-Tool wird genutzt, um eine ausführbare Datei zu blockieren. Ohne Orchestrierung durch ein SOAR-Tool müsste das Sicherheitsteam diese Abläufe manuell koordinieren. Ein SOAR-Tool wird dagegen über seine API in alle eingesetzten Sicherheitstools integriert und koordiniert dann die Arbeitsabläufe dieser Tools, um Sicherheits-Incidents zu erkennen, zu untersuchen oder auf sie zu reagieren.

Bei der Evaluierung eines SOAR-Tools sollte die Orchestrierungsfunktion alle Aktivitäten, die sich auf ein bestimmtes Sicherheitsszenario beziehen, von Anfang bis Ende dirigieren und überwachen. Es sollte in der Lage sein, Sicherheitsdaten aus jeder Datenquelle und in jedem Format aufzunehmen. Es sollte ihm zudem möglich sein, Daten zu empfangen, die an die Plattform weitergeleitet werden, Datenquellen abzufragen und Daten in die Plattform aufzunehmen. Darüber hinaus sollte ein Orchestrator sicherstellen, dass die Ausgabedaten einer Aktion richtig geparst, normalisiert und strukturiert sind, damit diese Daten für zukünftige Aktionen genutzt werden können.

Automatisierung

Automatisierung ist definiert als die maschinengestützte Ausführung von ansonsten manuellen, voneinander abhängigen Sicherheitsaktionen unter Verwendung von „Playbooks“. Mit anderen Worten, es ist das Arbeitstier der meisten SOAR-Tools. Während der Orchestrator die Integration und Koordination zwischen den Sicherheits-Tools ermöglicht, führen Playbooks die voneinander abhängigen Aktionen der einzelnen Sicherheits-Tools automatisch in einer bestimmten Reihenfolge aus – ohne die Notwendigkeit menschlicher Interaktion.

Die meisten Sicherheitsanalysten verbringen ihren Arbeitstag mit zu vielen sich wiederholenden und eintönigen Sicherheitsaufgaben oder -aktionen. Diese Aktionen werden vom Team manuell ausgeführt. Die Automatisierung ermöglicht es dem Sicherheitsteam durch den Einsatz von Playbooks, diese Aktionen, die zuvor in mehreren Minuten oder gar Stunden manuell ausgeführt wurden, gebündelt und innerhalb von Sekunden auszuführen. Beispielsweise sollten Untersuchungen von Phishing-Vorfällen, die möglicherweise den Einsatz mehrerer Aktionen mit vier bis fünf verschiedenen Sicherheits-Tools erfordern und bei manueller Durchführung etwa 40 Minuten in Anspruch nehmen, mit einem automatisierten Playbook in weniger als einer Minute erledigt sein. Auf diese Weise können SOAR-Tools die mittlere Erkennungszeit (Mean Time To Detect bzw. MTTD) und die mittlere Reaktionszeit (Mean Time To Respond bzw. MTTR) drastisch reduzieren.

Die Playbooks sollten leicht zu erstellen und zu ändern sein. Im Automatisierungs-Editor eines SOAR-Tools kodiert ein Analyst oder Manager seine Prozesse zu Automatisierungs-Playbooks. Der Editor sollte die Bearbeitung sowohl des Quellcodes als auch der visuellen Darstellung ermöglichen. Dies ermöglicht es allen Mitgliedern des Sicherheitsteams, unabhängig von ihren Präferenzen oder Programmierkenntnissen umfassende und anspruchsvolle Playbooks zu erstellen. Beim Erstellen eines Playbooks in einem visuellen Editor sollte der resultierende Playbook-Quellcode in Echtzeit generiert werden und für den Autor zugänglich sein – mit reibungslosem Umschalten und Bearbeiten zwischen dem visuellen und dem Quellcode-Editor.

Der Editor für visuelle Playbooks sollte intuitiv und benutzerfreundlich sein und die sprichwörtliche leere Leinwand für visuelle Playbooks darstellen. Durch die Nutzung von Blöcken und anderen Formen zur Darstellung wichtiger Schritte im Playbook sollte ein Benutzer in der Lage sein, ein Playbook zu erstellen, das die Ausführung von Aktionen als schrittweise, gruppierte oder gemischte Abfolge ermöglicht. Jede Form sollte dabei für verschiedene Ausführungen von Aktionen, Plattform-API-Aufrufen, bedingten Anweisungen (if/then), Aufforderungen zur menschlichen Interaktion und Aufteilungsanweisungen stehen. Durch Klicken auf jede Form können Sie die Aktion oder den Parameter manuell eingeben oder aus einer Liste auswählen. Außerdem sollten neue Informationen, die sich aus vorangegangenen Ausführungen von Aktionen ergeben, als Input oder Parameter für nachgelagerte Aktionen oder Entscheidungsblöcke zur Verfügung stehen.

Event- und Alarm-Management

Unmittelbar nach der Dateneingabe sollte eine Event- und Alarm-Managementfunktion in einem SOAR-Tool eingehende Ereignisse in eine Warteschlange aufnehmen und priorisieren. Auf diese Weise können Warnmeldungen schnell erfasst und effizient bearbeitet werden, ohne dass eine umfangreiche Suche oder ein Wechsel zwischen verschiedenen Kontexten erforderlich ist. Ereignisse und Alarme sollten einen Statusindikator (z. B. neu, offen oder geschlossen), einen Schweregradindikator und einen farbkodierten Empfindlichkeitsindikator enthalten, um eine schnelle Informationserfassung zu gewährleisten.

Die technischen Attribute eines Sicherheitsereignisses oder eines Alarms sollten so organisiert sein, dass ein

schnelles Verständnis des Sicherheitsszenarios möglich ist. Dazu gehört eine organisierte Anzeige von Daten wie IPs, Domains, Dateihashes, Benutzernamen und E-Mail-Adressen. Ein Sicherheitsanalyst sollte in der Lage sein, anhand dieser Daten nahtlos Aktionen zur Untersuchung, Eindämmung oder Reaktion (oder ein Bündel von Aktionen, d. h. Playbooks) zu ergreifen.

Und schließlich sollte das SOAR-Tool ein umfassendes Aktivitätsprotokoll zur Verfügung stellen, das eine Aufzeichnung aller Aktionen anzeigt, die zu einem Ereignis oder Alarm ausgeführt wurden, unabhängig davon, ob sie manuell oder über ein Playbook eingeleitet wurden. Für jede Aktion sollten die Ergebnisse angezeigt werden, einschließlich eines Indikators für den Erfolg oder Misserfolg der Aktion.

Ticket-Management

Sobald Alarme oder Ereignisse bestätigt und eskaliert wurden, sollte eine Ticket-Management-Komponente übernehmen und einen breiteren, funktionsübergreifenden Lebenszyklus von der Erstellung bis zur Lösung durchführen. Das SOAR-Tool erfasst mehrere Ereignisse und bestätigt, aggregiert und eskaliert sie anschließend zu einem einzelnen Fall. Die Benutzeroberfläche für das Ticket-Management sollte das Verknüpfen relevanter technischer Daten, z. B. die Quelldaten des Alarms und die Ergebnisse der Aktionen, mit dem Fall unterstützen. Die Benutzeroberfläche sollte darüber hinaus das Anhängen relevanter nicht-technischer Daten wie Kommentare, Memos, E-Mails, Screenshots, Aufzeichnungen oder anderer beliebiger Dateien mit Relevanz für den Fall unterstützen. Alle Änderungen an einem Fall sollten in einem Prüfpfad protokolliert werden und exportierbar sein. Des Weiteren sollte das automatische Anhängen von Informationen zu einem Fall aus einem Playbook heraus möglich sein.

Das Ticket-Management sollte zudem leicht auf die bestehenden Prozesse eines Unternehmens angepasst werden können. Viele Unternehmen haben Standardarbeitsanweisungen (Standing Operation Procedures oder SOPs) für die Reaktion bei Vorfällen entwickelt. Die Ticket-Management-Funktionalität sollte Anwendern die Möglichkeit bieten, ihrem Prozess entsprechend Phasen zu definieren und als Vorlage zu speichern. Anwender sollten die Möglichkeit haben, die SOP in mehrere Phasen zu unterteilen, wobei jede Phase eine oder mehrere Aufgaben beinhaltet und jeder Aufgabe ein Eigentümer zugewiesen werden kann. Die Benutzeroberfläche sollte einen Indikator sowohl für den Fortschritt als auch für den Status eines Vorfalls bieten.

Zusammenarbeit

Sicherheit ist ein Mannschaftssport. Sicherheitsanalysten müssen zusammenarbeiten, um auf Sicherheitsereignisse schnell reagieren zu können. Je besser Ihr Team vernetzt und synchronisiert ist, desto schneller und effektiver kann es das Unternehmen schützen.

Daher sollte ein branchenführendes SOAR-Tool integrierte Funktionen umfassen, um diese Zusammenarbeit zu erleichtern. Funktionen für die Zusammenarbeit wie der integrierte Chat und die Möglichkeit, Fällen Kommentare hinzuzufügen und diese zu teilen, sollten zusätzlich zu dem Untersuchungs- oder Reaktions-Workflow verfügbar sein, um eine kontextbezogene Zusammenarbeit zu ermöglichen. Dank der Echtzeit-Chatfunktion, der Kommentare sowie der Informationen zu den Ereignissen, Alarmen und Tickets können Sicherheitsanalysten einen Grad an Situationsbewusstsein erreichen, der die effiziente und schnelle Lösung von Sicherheitsvorfällen fördert.

Dadurch entsteht zudem ein einfacher Prüfpfad. Idealerweise sollte das Protokoll dieser Zusammenarbeit gemeinsam mit den relevanten Daten des Ereignisses und den aufgezeichneten Aktionen, die unternommen wurden, erfasst und organisiert werden können. Dies gestaltet sich jedoch nicht ganz einfach, wenn Ihre Kommunikation über ein externes Tool und damit von den Workflow-Informationen in Ihrem SOAR-Tool getrennt erfolgt.

Metriken und Reportings

Ein Sicherheitsteam muss in der Lage sein, den Status seiner Sicherheitsoperationen auf einfache Weise zu messen und im Laufe der Zeit kontinuierliche Verbesserungen anzustreben. Daher sind solide Metriken und Berichte für jedes SOAR-Tool ein Muss. Sie helfen dem Sicherheitsteam, die Auswirkungen von Funktionen wie der Automatisierung auf die Produktivität zu verstehen und festzustellen, wo Verbesserungen vorgenommen werden können, um den ROI zu steigern.

Die Automatisierung wird zur Steigerung der Betriebseffizienz über mehrere Funktionen eines SOC (Security Operations Center) hinweg eingesetzt. Es ist von entscheidender Bedeutung, den quantitativen Leistungsgewinn und die Ressourceneinsparungen zu verstehen, die die Automatisierung bringt, und diese Informationen über ein Dashboard innerhalb des SOAR-Tools angezeigt zu bekommen. Beispiele für wichtige Leistungskennzahlen, die auf der SOAR-Plattform verfügbar sein sollten, sind die mittlere Lösungszeit (Mean Time To Resolve oder MTTR), die mittlere Wartezeit (Mean Dwell Time oder MDT), die durch die automatisierte Ausführung eingesparten Arbeitsstunden von Analysten, die Anzahl der durch die automatisierte Ausführung gewonnenen Vollzeitäquivalente (VZÄ), die durchschnittliche Zeitersparnis pro Playbook-Durchlauf, die Kostenersparnis (VZÄ-Kosten x gewonnene VZÄ), die Gesamtzahl der offenen Alarme, der pro Tag (Stunde, Woche, Monat) offenen und geschlossenen Alarme sowie die Leistung im Rahmen von Dienstleistungsvereinbarungen (Service Level Agreements oder SLAs).

All diese vorstehenden Informationen sollten sich leicht organisieren und in Berichten für die Geschäftsleitung

und die CISOs zusammenfassen lassen, um schnell den Gesamtstatus ihrer Sicherheitsoperationen (sowie die Verbesserungen, die das SOAR-Tool ermöglicht) zu verstehen.

Mobilität

SOAR-Plattformen sind darauf ausgelegt, die Reaktionszeiten zu beschleunigen. Um schnell reagieren zu können, müssen Sicherheitsanalysten erreichbar sein, wenn ein Vorfall oder eine Sicherheitsabfrage menschliches Eingreifen erfordert. Doch die Analysten sitzen nicht immer mit geöffnetem Laptop an ihrem Schreibtisch und sind nicht immer in der Lage, sofort auf Abfragen zu reagieren.

Deshalb ist es wichtig, dass eine SOAR-Plattform es dem Sicherheitsanalysten ermöglicht, in Sachen Plattform-Zugang, -Interaktivität und -Kontrolle bequem von einem mobilen Gerät aus zu agieren. Auf diese Weise können Sicherheitsanalysten auch von unterwegs Playbooks ausführen, Sicherheitsartefakte und Triage-Ereignisse ohne Laptop überprüfen, von ihrem mobilen Gerät aus auf Abfragen reagieren und immer erreichbar sein, unabhängig davon, ob sie gerade am Schreibtisch sitzen oder unterwegs sind.

Skalierbarkeit

Ein SOAR-Tool sollte mit Ihrem Unternehmen wachsen. Während Sie im Laufe der Zeit immer mehr Anwendungsfälle hinzufügen, muss die Plattform immer größere Verarbeitungslasten bewältigen.

Es ist wichtig, zu verstehen, wie sich die Automatisierungs-Engine sowohl vertikal als auch horizontal skalieren lässt. Es wird erwartet, dass ein Anwender mit der Zeit immer mehr Anwendungsfälle automatisiert. Mit jedem zusätzlichen Anwendungsfall entsteht für die Automatisierungs-Engine eine zusätzliche Verarbeitungslast. Die Automatisierungs-Engine sollte so konzipiert sein, dass eine vertikale Skalierung (z. B. eine Erhöhung der CPU- und RAM-Ressourcen) ebenso möglich ist wie eine horizontale Skalierung (z. B. eine Erhöhung der Server-Instanzen), um die Leistung zu erhöhen und den durch die Automatisierung generierten Return on Investment (ROI) zu schützen.

Offenheit und Erweiterbarkeit

Eine SOAR-Plattform sollte auf Offenheit und Erweiterbarkeit ausgelegt sein. Sie sollte die Einbeziehung neuer Sicherheitsszenarien, neuer Produkte, neuer Aktionen und neuer Playbooks problemlos unterstützen. Ohne diese Funktionalitäten kann eine SOAR-Plattform mit der Zeit ihren Wert verlieren.

Durch ein Ökosystem mit offener Integration, das einem gemeinsamen Standard- und Programmierungsmodell folgt, können Sicherheitsteams deutliche Vorteile erzielen. Neue Technologien können schnell in die Plattform integriert werden, ohne dass Änderungen am Kern der Plattform erforderlich sind oder negative Auswirkungen auf automatisierte Playbooks entstehen. So können Anwender zusätzliche Integrationen ohne Genehmigung oder Entwicklungszyklen des SOAR-Anbieters entwickeln. Sie können zum Beispiel ihre eigenen Integrationen programmieren, selbst Anwendungen entwickeln oder eine Early-Access-API von einem Anbieter nutzen.

Außerdem sollte ein SOAR-Tool flexible Bereitstellungsoptionen bieten und eine lokale, Cloud-basierte oder Hybrid-Implementierung unterstützen. Aufgrund der effizienteren Installation, Konfiguration, Implementierung und Skalierung bietet besonders eine Cloud-Bereitstellung mehr Agilität und eine schnellere Time-to-Value. Dazu kommt, dass Cloud-Software laufend und automatisch aktualisiert wird und daher keine manuelle Übertragung von Software-Updates notwendig ist.

Unterstützung durch die Community

Das Thema Cyber Security unterliegt ständigen Veränderungen. Entsprechend wichtig ist es, auf immer neue Bedrohungen reagieren zu können. Hierbei hilft eine Community aus Fachleuten, die zusammenarbeiten, um Playbooks, Best Practices und Strategien für den Umgang mit den neuesten Bedrohungen auszutauschen. Daher muss ein SOAR-Tool den Community-Ansatz unterstützen und die gemeinsame Nutzung von App-Integrationen und Playbooks auf einfache Weise ermöglichen.

Messen Sie die Installed Base einer Plattform, um das Kooperationspotenzial der zugehörigen Community zu ermitteln. Eine große und aktive User Community ermöglicht Ihnen den Austausch von Playbooks, Anwendungen oder das Brainstorming von Ideen für neue Automatisierungs-Use Cases. Darüber hinaus ist das Engagement eines Anbieters innerhalb der Community sowohl ein starker Indikator für dessen Bekenntnis zur Community, als auch zu guter Kollaboration. Um den Austausch von Ideen zu erleichtern, sollte der SOAR-Anbieter ein Kommunikations-Tool der Community, wie z. B. Slack, bereitstellen, das Gruppenchats und Direktnachrichten für technischen Support und Fragen ermöglicht. Weitere Kommunikations-Tools zum Teilen von Ideen sind die Github-Seiten der Community-User, auf denen Einzelpersonen ihre Arbeiten veröffentlichen, sowie ein zentrales Community-Repository, in dem sich Benutzerpräsentationen, Blogs, Community-Playbooks, Integrationen von Apps und allgemeine Dokumentationen befinden.

Kann ein SOAR-Tool Ihnen helfen, Ihre Sicherheitsoperationen zu verbessern? Finden Sie es heraus und erfahren Sie, wie **Splunks branchenführende SOAR-Technologie** die Effizienz und Effektivität Ihres Sicherheitsteams auf eine neue Stufe heben kann.

21-14104-Splunk-10 Essential Capabilities of a Best-of-Breed SOAR-WP-106_DE