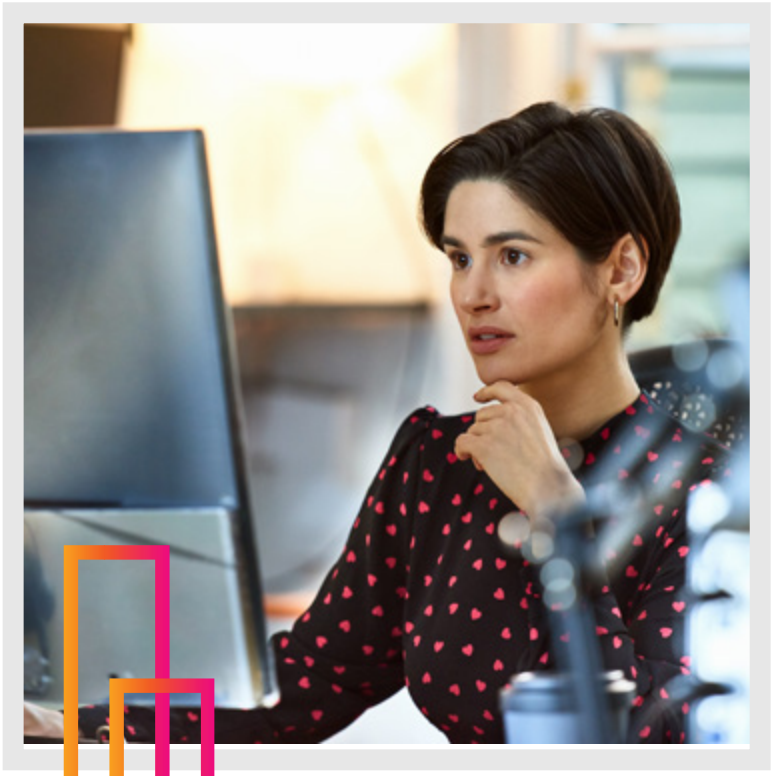
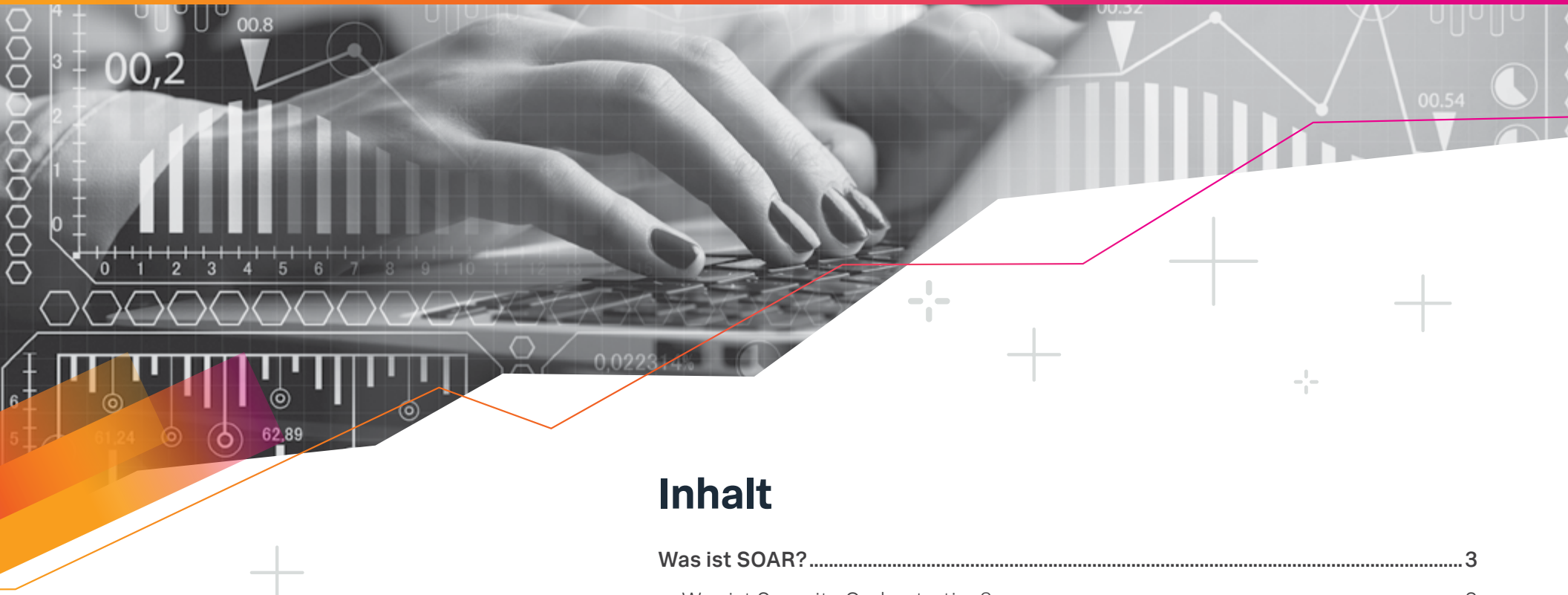
Leitfaden für SOAR-Käufer

Security Orchestration, Automation and Response beschaffen: Grundlagen und Kriterien der Entscheidung



splunk>
turn data into doing®



Inhalt

Jetzt ist der ideale Zeitpunkt, in eine SOAR-Lösung (Security Orchestration, Automation and Response) zu investieren. Sicherheitsteams können längst nicht mehr in Handarbeit auf Vorfälle reagieren. Das müssen sie auch nicht. Heute können sie smarter arbeiten, statt härter – indem sie wiederkehrende Aufgaben automatisieren. Damit steigen Produktivität und Präzision der Security-Fachkräfte, und das Unternehmen ist insgesamt besser geschützt.

Viel zu oft ächzen die Sicherheitsteams noch unter der Last monotoner Routinearbeit. Davon gibt es in der Security mehr als genug, vor allem auf Tier-1-Ebene. Obendrein fehlt in den SOCs (Security Operations Centers) weltweit über eine Million Fachleute mit dem nötigen Wissen und Know-how. Und es gibt noch weitere Hindernisse. Dazu gehören u. a. diese:

- **Zu viele Warnmeldungen:** Die Security-Fachleute werden von Hunderten, wenn nicht Tausenden von Sicherheitswarnungen überschwemmt – was dann zu einem Rückstand bei der Bearbeitung von Sicherheitsvorfällen führt und die gefürchtete Alarmmüdigkeit im Gefolge hat.
- **Zu viele einzelne Silo-Produkte:** Von den Teams wird erwartet, dass sie mit einem Haufen disparater Sicherheitstools ohne jede Interoperabilität jonglieren. Wenn die Tools aber nicht zusammenspielen, sind Sicherheitslücken unvermeidlich. Angreifer können (und werden) sie ausnutzen.
- **Qualifikationsdefizite:** Ein SOC zu besetzen, ist keine leichte Aufgabe. Qualifizierte Fachleute sind Mangelware, und die Fluktuation ist extrem hoch. Oft sind die Zeit und die Ressourcen, die Firmen in die Fortbildung und den Aufbau von institutionellem Wissen stecken, am Ende umsonst.
- **Prozessdefizite:** Die meisten Sicherheitsteams versäumen es, Arbeitsabläufe und Standardvorgehensweisen (Standard Operating Procedures/SOPs) für die einzelnen Arten von Security-Events festzulegen. Ohne diese operative Disziplin können die Verantwortlichen aber nicht schnell und bestimmt handeln, wenn sie auf einen Angriff reagieren sollen.
- **Mangelnde Geschwindigkeit:** Angreifer können in aller Ruhe Daten exfiltrieren, wenn die MTTD (Mean Time to Detect) zu lang ist. Die typische menschliche Reaktionszeit bei einem Alarm liegt irgendwo zwischen Minuten und Wochen oder gar Monaten. Bei ernsthaften Bedrohungen bedeuten sogar Minuten schon eine zu lange Verweildauer.

Angesichts dessen fällt es den Teams immer schwerer, Bedrohungen zu erkennen und darauf zu reagieren. Unternehmen brauchen eine Lösung, die leistungsstark, flexibel und schnell ist – eine Lösung mit Automatisierung.

Mithilfe von SOAR können Sicherheitsfachleute auf jede Bedrohung reagieren, egal wie groß, egal wie klein. Eine solide SOAR-Lösung schreibt Workflows als automatisierte Playbooks und kann Aktionsabfolgen – von der kontrollierten Explosion von Dateien bis zur Quarantäne ganzer Geräte – in der gesamten Sicherheitsinfrastruktur des Unternehmens binnen Sekunden ausführen, also unvergleichlich viel schneller als von Menschenhand.

Das Fazit? Auch Sie können von SOAR profitieren. Dieser Leitfaden für SOAR-Käufer geht mit Ihnen die wichtigsten Auswahlkriterien durch, damit Sie die Lösung finden, die für die Sicherheitsabläufe in Ihrem Unternehmen optimal ist. Und damit Ihre Security-Fachleute wieder Zeit für wichtigere Aufgaben finden (und vielleicht sogar für eine Pause).

Was ist SOAR?

Eine SOAR-Lösung nimmt dem Sicherheitsteam die alltäglichen Aufgaben ab, die sonst unnötig Zeit und Ressourcen binden. Mit SOAR können die Teams mehr Vorfälle bearbeiten, Probleme genauer untersuchen, Zeit für wichtigere Sicherheitsaufgaben gewinnen und die allgemeine Sicherheitslage des Unternehmens verbessern.

In den meisten Branchen ist Automatisierung längst etabliert, nur die Cybersicherheit gilt als Nachzügler. In den letzten Jahren hat sich jedoch ein deutlicher Wandel vollzogen. Die Leute aus der Praxis zeigen sich zunehmend interessiert, und die Menge der Anbieter, die ins SOAR-Segment einsteigen, wächst zusehends; die meisten davon schneiden ihre bestehenden Lösungen aus angrenzenden Gebieten einfach neu zu.

Das hat dazu geführt, dass die Begrifflichkeiten rund um SOAR etwas unscharf geworden sind, was wiederum einen Vergleich erschwert. Was wir also zuerst brauchen, sind klare Definitionen. Entscheidend sind die folgenden Kategorien:

Security Orchestration

Sicherheitsorchestrierung ist die maschinengestützte Koordinierung der Abfolge zusammenhängender Sicherheitsmaßnahmen in einer komplexen Infrastruktur.

Security Automation

Sicherheitsautomatisierung ist die maschinengestützte Ausführung von Sicherheitsmaßnahmen.

Security Response

Sicherheitsreaktion ist die richtlinienbasierte Koordination der Aktivitäten von Mensch und Maschine bei Ereignis-, Fall- und Incident-Workflows.

Was ist Security Orchestration?

Security Orchestration bzw. Sicherheitsorchestrierung ist die maschinengestützte Koordinierung der Abfolge zusammenhängender Sicherheitsmaßnahmen in einem komplexen IT-Ökosystem. Damit lassen sich die einzelnen Sicherheitstools so aufeinander abstimmen, dass sie konzertiert zusammenarbeiten. Zugleich werden Aufgaben automatisiert, und zwar produkt- und prozessübergreifend. Grundsätzlich ermöglicht die Orchestrierung den Sicherheitsteams die Automatisierung komplexer Prozesse über einzelne Punktlösungen hinweg, sodass Sicherheitspersonal, -prozesse und -tools maximalen Wert schaffen.

Sicherheitsorchestrierung kann …

- Workflows über die einzelnen Tools hinweg abgestimmt und automatisch koordinieren,
- bei Sicherheitsvorfällen durch Zusammenführung von Daten aus anderen Quellen zusätzlichen Kontext bereitstellen,
- eingehende, aussagekräftige Untersuchungen ermöglichen.

Was ist Security Automation?

Security Automation bzw. Sicherheitsautomatisierung ist die maschinengestützte Ausführung von Sicherheitsmaßnahmen, die Bedrohungen programmiert untersuchen, darauf regieren und sie sogar beseitigen, ohne dass menschliches Eingreifen erforderlich wäre. Den Security-Fachleuten nimmt die Automatisierung den größten Teil der Arbeit ab, sodass sie nicht mehr jede eingehende Warnung einzeln durchsuchen und manuell bearbeiten müssen bzw. jede Sicherheitsmaßnahme oder -aufgabe von Hand anstoßen und durchführen müssen.

Security Automation kann …

- Bedrohungen in Ihrer Umgebung untersuchen,
- Potenzielle Bedrohungen gewichten und priorisieren – Security-Fachkräfte bekommen dazu klare Einzelschritte, Anweisungen und Entscheidungsworkflows, anhand derer sie Events untersuchen und bestimmen können, ob es sich um einen ernsthaften Vorfall handelt;
- eine Entscheidung herbeiführen, ob Abhilfemaßnahmen zu ergreifen sind,
- das Problem eingrenzen und beheben,
- die Untersuchung von Schwachstellen und das Patchen automatisieren.

Was ist Security Response?

Security Response bzw. Sicherheitsreaktion ist die richtlinienbasierte Koordination von menschlichen und automatisierten maschinellen Aktionen in Ereignis-, Fall- und Incident-Workflows. Die technischen Einzelheiten eines Sicherheitsereignisses bzw. einer Warnmeldung sollten so organisiert sein, dass Sicherheitsfachleute die vorliegenden Informationen möglichst rasch erfassen können; dann können sie das gesamte Ausmaß des Szenarios besser einschätzen und entsprechend reagieren. Kurz gesagt: Profis sollten in der Lage sein, anhand der bereitgestellten Daten übergangslos Ermittlungs-, Eindämmungs- und Reaktionsmaßnahmen zu ergreifen.

Sobald eine Warnmeldung bzw. ein Ereignis bestätigt und eskaliert ist, sollte eine eigene Komponente das Fallmanagement übernehmen und einen umfassenden, funktionsübergreifenden Zyklus steuern, der vom Anfang bis zu endgültigen Lösung reicht.

Security Response kann …

- mehrere Ereignisse bestätigen und sie als einen einzigen Fall eskalieren,
- Incidents bruchlos auf die bestehenden Prozesse des Unternehmens abbilden,
- Ermittlungs-, Eindämmungs- oder Reaktionsmaßnahmen anhand festgelegter technischer Daten starten,
- ein Handlungsprotokoll zur Verfügung stellen, das sämtliche Aktionen in Bezug auf ein Event oder eine Warnmeldung aufzeichnet,
- einen weit gefassten, funktionsübergreifenden Sicherheitszyklus vom Anfang bis zur Lösung steuern.

Die wichtigsten SOAR-Szenarien

Die folgenden Use Cases orientieren sich an bestehenden manuellen Workflows und betreffen Punkte, mit denen der IT-Betrieb oft zu kämpfen hat. Zu diesen Workflows gehört normalerweise eine Unmenge von manuellen Aufgaben, die eine Abstimmung diverser Punktlösungen erfordern.

Bevor Sie mit der SOAR-Evaluierung beginnen, sollten Sie potenzielle Use Cases definieren, die für Ihr Unternehmen typisch sind. Im besten Fall beziehen Sie dabei sowohl die Stakeholder aus den Security Operations als auch die Führungsebene mit ein. Die Identifizierung dieser Schlüsselanwendungsfälle ist – auch wenn sie nicht sofort implementiert werden – ganz entscheidend für eine erfolgreiche Sicherheitsstrategie.

Die folgende Auswahl von Use Cases behandelt die Bereiche Untersuchung, Anreicherung, Eindämmung und Behebung.

Alarm-Priorisierung	Die Alarm-Priorisierung (Alert Triage) prüft und priorisiert eingehende Warnmeldungen und kontextualisiert die Ereignisse. Hierzu gehören auch Methoden und Modelle, mit denen Fehlalarme von der weiteren Verarbeitung ausgeschlossen werden.
Vorfallreaktion	Die Vorfallreaktion (Incident Response) hängt von der Art des Vorfalls ab. So ist die Abwehr eines Phishing-Versuchs etwas völlig anderes als die Antwort auf einen erfolgreichen Ransomware-Angriff.
Bedrohungssuche	Durch Automatisierung der IOC-Suche (Indicators of Compromise) greifen die Teams automatisch und ohne ihre Ressourcen zu belasten auf die aktuellsten Bedrohungsinformationen zu. Möglich ist außerdem eine Gewichtung dieser Informationen, sodass sich der Input geordnet und pragmatisch verarbeiten lässt.
Schwachstellen-management	Die Automatisierung (und in der Folge die Standardisierung) des Zyklus zur Identifizierung, Klassifizierung, Behebung und Entschärfung von Schwachstellen führt zu mehr Effizienz und Konsistenz.
Netzwerkzugangskontrolle	SOAR kann dynamische NAC-Strategien (Network Access Control) ergänzen. Ein Beispiel wäre die Integration eines Erkennungssystems, das bei der ursprünglichen NAC-Entscheidung noch nicht zur Diskussion stand.
Benutzerverwaltung	Die Benutzerverwaltung stellt sicher, dass einzelne Konten schnell und systematisch aktiviert und deaktiviert werden können; so unterbindet man Insider-Bedrohungen, Kontenübernahmen und den Missbrauch von Zugangsdaten.
Penetrationstests	Die Produktivität des Pentest-Teams steigt, wenn Asset-Erkennung und -Klassifikation, Zielpriorisierung etc. automatisiert sind.
Informationsaustausch	Unternehmen, die Sicherheitsinformationen austauschen, können von automatisierten Playbooks profitieren. Durch Automatisierung steigt auch die Produktivität der Fachleute, und zeitkritische Informationen stehen viel schneller zur Verfügung als bei manuellen Prozessen.

Weitere SOAR-Use-Cases ergeben sich aus der Vielzahl weiterer Herausforderungen, bei denen die Sicherheitsteams Kriterien zur Erkennung und Automatisierung festlegen. Am besten werfen Sie dazu einen Blick in unser E-Book „Fünf Use Cases für die Automatisierung mit Splunk SOAR“.

SOAR-Grundlagen

Bewertungskriterien

Die Kriterien einer SOAR-Lösung lassen sich in drei Kategorien unterteilen: **Kernfunktionen, Plattformeigenschaften** und **geschäftliche Erwägungen.**

Kernfunktionen

Die Kernfunktionen bilden die Grundlage (bzw. Grundbausteine) einer SOAR-Lösung. Wir gehen im Folgenden auf jede Funktion und jede Komponente ein und erläutern die wichtigsten Überlegungen bei der Abwägung Ihrer Optionen.

Orchestrator

- **Datenaufnahme**
  Security-Daten müssen zunächst eingelesen werden. Ein Orchestrator kann Daten aus jeder Quelle und in jedem Format aufnehmen und kompilieren, wobei die Daten logisch getrennt bleiben. Im Fall von unstrukturierten Daten sollte ein Data Handler die Daten interpretieren und zugänglich machen.
- **Entscheidungsfindung**
  Sie sollten die Möglichkeit haben, automatisierte Playbooks auf ihre jeweiligen Datenquellen anzuwenden. So passt ein E-Mail-Phishing-Playbook für eine E-Mail-Datenquelle, während ein Playbook, das auf Malware abklopft, für eine SIEM-Quelle (Security Information and Event Management) richtig ist.
- **Aufgabenausführung**
  Automatisierte Aufgaben werden zum geeigneten bzw. optimalen Zeitpunkt an die Automatisierungs-Engine zur Ausführung übergeben.
- **Menschliche Aufsicht**
  Maschinelle Automation und die notwendige menschliche Überwachung müssen einander ergänzen. In der Regel gibt es drei Szenarien, in denen Fachleute gefordert sind: 1) wenn zur Ausführung einer Sicherheitsmaßnahme die Genehmigung der Asset-Eigentümer nötig ist, 2) wenn kontrolliert werden soll, ob Sicherheitsmaßnahmen und Geschäftsfortführung im Einklang miteinander stehen, 3) wenn die kodifizierte Entscheidungslogik erweitert werden muss (z. B. bei einem Fehler).
- **Datenmanagement**
  Es muss sichergestellt sein, dass der Daten-Output einer Aktion ordnungsgemäß geparst, normalisiert und strukturiert wird, sodass künftige Aktionen darauf zugreifen können. Der Orchestrator sollte relevante Daten auch zwischenspeichern können, damit er nicht andere Ressourcen belastet.
- **Fehlertoleranz**
  SOAR interagiert andauernd mit vielen anderen Produkten und Services. Deren Verfügbarkeit ist jedoch nicht immer gewährleistet; der Zugriff auf externe Dienste kann unterbrochen oder gestört sein. In diesem Fall sollte der Orchestrator vorhersagbar reagieren und den Betrieb wie konfiguriert bruchlos wieder aufnehmen und fortsetzen.

Automatisierungs-Engine

Die Automatisierungs-Engine ist bei den meisten SOAR-Lösungen im wahrsten Sinne des Wortes der Motor des Ganzen. Die Engine empfängt Aktionen (bzw. Aufgaben) vom Orchestrator und reagiert dann entsprechend. Da die Automatisierung abseits aller menschlichen Interaktion abläuft, sind Skalierbarkeit und Erweiterbarkeit ganz entscheidende Kriterien.

- **Skalierbarkeit**
  Im Laufe der Zeit kommen immer neue (automatisierte) Use Cases hinzu. Mit Blick auf die damit steigende Rechenlast muss die Automatisierungs-Engine vertikal und horizontal skalierbar sein.
- **Erweiterbarkeit**
  Security entwickelt sich schnell weiter. Neue Funktionen sollten daher unterstützt werden, ohne dass größere Umstrukturierungen nötig sind. Die Automatisierungs-Engine sollte am besten so flexibel sein, dass sie den besonderen Fähigkeiten ihrer jeweiligen Umgebung gerecht wird.

Alert-Management

Nach der Datenaufnahme werden eintreffende Warnmeldungen aufgereiht und nach Priorität sortiert. Die Untersuchungen werden dann manuell oder automatisiert durchgeführt, je nach dem, was das Höchstmaß an Produktivität und Präzision verspricht.

Damit die richtigen Informationen zur richtigen Zeit verfügbar sind, sollte die Oberfläche die Benachrichtigungen in einem Format anordnen und priorisieren, das problemlos zu verarbeiten ist. Auf diese Weise bleiben den Fachleuten umständliche Suchläufe und Kontextwechsel erspart, und sie können relevante Events rasch überschauen.

- **Alarmdetails**
  Die Einzelheiten einer Sicherheitsmeldung sollten so organisiert sein, dass das Fachpersonal das Event rasch erfassen und verarbeiten kann. Dazu gehört eine übersichtliche Darstellung der wesentlichen technischen Daten, einschließlich IP-Adressen, Domain-Namen, Datei-Hashes, Benutzernamen, E-Mail-Adressen und anderer Datenfelder. Ein Standardformat wie CEF (Common Event Format) ist beim Datenaustausch von großem Vorteil.
- **Aktionsausführung**
  Sicherheitsfachleute sollten direkt aus Untersuchung, Eindämmung und Behebung heraus manuelle Aktionen durchführen können, und zwar im besten Fall so, dass sie im Interface dazu einfach die betreffenden Daten auswählen. Außerdem sollte es möglich sein, auf Warnmeldungen mit einem automatisierten Bündel von Aktionen zu reagieren (sogenannten Playbooks).
- **Aktionsergebnisse**
  Die Ergebnisse von Aktionen sollten sowohl zusammenfassend (z. B. in einer Tabellenansicht) als auch in einem ausführlichen Format verfügbar sein (z. B. in der gängigen JavaScript Object Notation/JSON), damit sie leicht zugänglich und einfach einzusehen sind.
- **Aktivitätsprotokoll**
  Das Activity Log zeichnet akribisch sämtliche Aktionen auf, die in Bezug auf eine Warnmeldung getätigt wurden, ob manuell oder durch ein automatisiertes Playbook. Zu jeder Aktion sollte das Ergebnis angezeigt werden und dazu ein Indikator, der über Erfolg bzw. Misserfolg Auskunft gibt, sodass klar wird, ob die Aktion vollständig ausgeführt wurde.
- **Warnstatus, Schweregrad und Schutzwürdigkeit**
  Warnmeldungen sollten Indikatoren mitbringen, die den Status anzeigen (z. B. „neu“, „offen“ oder „abgeschlossen“), den Schweregrad und wie sensibel die jeweiligen Daten sind, z. B. per TLP-Einstufung (Traffic Light Protocol). Diese Indikatoren sollte man sowohl auf der Alert-Management-Oberfläche als auch in den Playbooks ändern können.
- **Zusammenarbeit bei Warnmeldungen**
  Die Oberfläche sollte einen eigenen Bereich zur Zusammenarbeit haben, in dem die Security-Fachleute Alerts kommentieren und Informationen über eine Meldung und die darauf bezogenen Daten austauschen können.

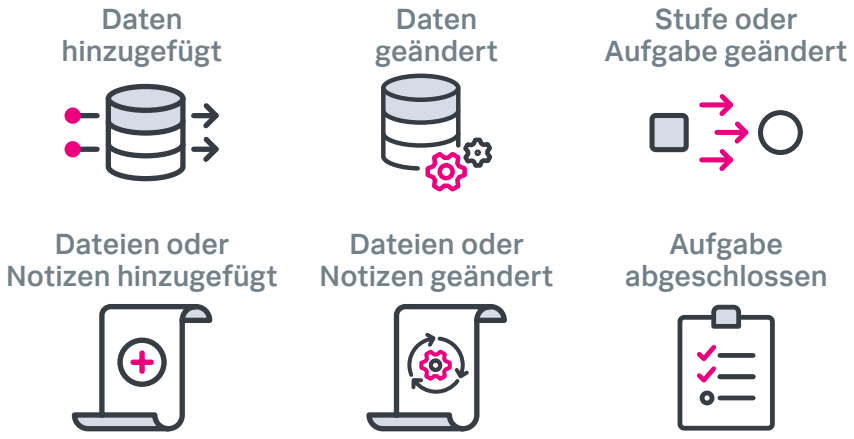
Ticket-/Fallmanagement

Das Fallmanagement bietet eine weiter gefasste, funktionsübergreifende Sicht auf den Verlauf eines Vorfalls: von der Erstellung bis zur Lösung. Dabei können mehrere Warnmeldungen und/oder Ereignisse als ein einziges Ticket bestätigt, zusammengefasst und eskaliert werden. Während das Alert-Management in der Regel technisch und auf den Einzelfall ausgerichtet ist, kann das Ticket-Management auch nichttechnische Schritte einbeziehen.

Außerdem ist die Menge der Fälle insgesamt in der Regel viel geringer als die der Warnmeldungen, die Zahlen liegen in der Regel im einstelligen Bereich.

- **Ticket-Datenorganisation**
  Sämtliche Daten, die sich auf einen bestimmten Fall beziehen, sollte man in der Ticket-Management-Komponente versammelt finden. Die gebündelte Anzeige dieser Informationen macht es den Fachleuten einfacher, alles ohne Kontextwechsel zu erfassen.
- **Erweiterte Falldaten**
  Die relevanten technischen Daten sollten dem betreffenden Ticket beigefügt sein (z. B. Quelldaten, Ergebnisse von Aktionen etc.). Aber auch relevante nichttechnische Informationen (z. B. Notizen, Memos, E-Mails, Screenshots, Aufzeichnungen und letztlich beliebige Dateien, sofern sie relevant sind) sollte man ergänzen können.
- **Ticket-Alert-Verknüpfung**
  Idealerweise sollte die Ticket-Management-Oberfläche von jedem Fall aus mit dem Alert-Management verknüpft sein. Dies ist besonders dann praktisch, wenn die Fachleute feststellen, dass ein Teil der Daten genauer untersucht oder dass eine Maßnahme zur Eindämmung ergriffen werden muss.
- **Zuordnung zu bestehenden Prozessen**
  Die meisten Unternehmen haben Standardvorgehensweisen (Standard Operating Procedures/SOPs) für Vorfallreaktion, Notfälle, Katastrophenfälle und andere Krisensituationen. Passend dazu sollte es mit dem Ticket-Management auch möglich sein, Prozesse und Workflows zu definieren und als Vorlage abzuspeichern. Jeder Ablauf wird dabei in Stufen unterteilt, wobei jede Stufe eine oder mehrere Aufgaben umfasst, für die jeweils Verantwortliche benannt werden.
- **Protokollierung**
  Neue oder aktualisierte Informationen, inklusive Statusaktualisierungen, sollten per Prüfpfad protokolliert werden und leicht exportierbar sein.

  Hier einige Beispiele möglicher Änderungen an einem Fall:

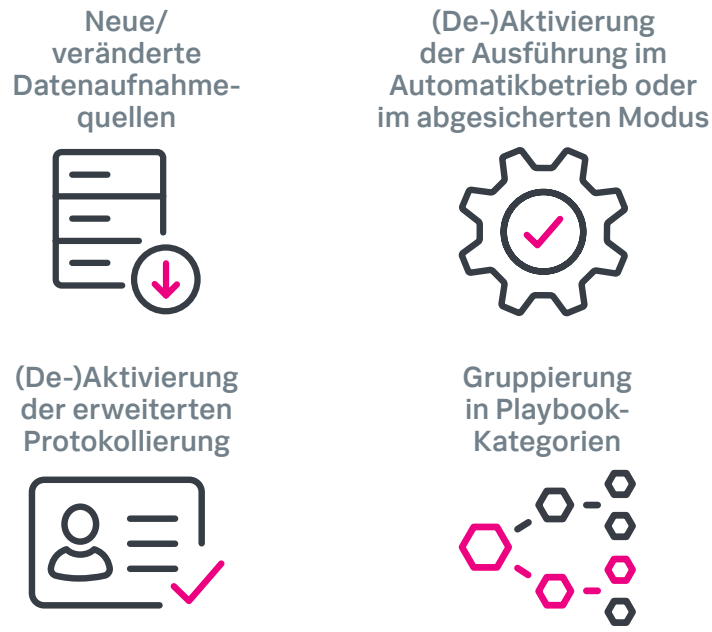


Playbook-Management

Das Playbook-Management erleichtert die Implementierung und Pflege von Standardvorgehensweisen (SOPs) im Unternehmen (und manchmal auch über dessen Grenzen hinaus). Im besten Fall verfügt diese Komponente außerdem über eine Revisions-/Versionskontrolle und eine Möglichkeit der geregelten Weiterverwendung.

- **Playbook-Organisation**
  Die SOAR-Lösung sollte es den Security-Fachleuten erlauben, ihre Playbooks nach eigenen Kategorien zu gruppieren. Die Einteilung (z. B. nach Schutzwürdigkeit, betrieblichen Einheiten, Assets oder Themen) orientiert sich in der Regel daran, was am besten funktioniert oder am besten für das Unternehmen passt.
- **Benutzerdefinierte Funktionen**
  Den Fachleuten sollte es auch möglich sein, eigenen Code zu schreiben und eigene Funktionen zu entwickeln, sodass sie sich nicht auf das beschränken müssen, was einsatzfertig out of the box (OOTB) verfügbar ist. Diese Funktionen sollten sich dann einerseits in beliebigen Playbooks verwenden lassen, andererseits der zentralen Codeverwaltung und Versionskontrolle unterstehen.
- **Versionskontrolle und Ausgabe**
  Die Anbindung des Playbook-Managements an eine Versionsverwaltung (Version Control System/VCS) ist in hohem Maße anzuraten. In puncto Bereitstellung erleichtert ein VCS die geordnete Ausgabe der Playbooks; in puncto Entwicklung wiederum kann man mit einem VCS Änderungen nachverfolgen und Updates bei Bedarf wieder zurückziehen.
- **Stapelverarbeitung**
  Jedes Playbook dürfte in seiner Funktionsweise einzigartig sein. Doch auf Verwaltungsebene gibt es durchaus Gemeinsamkeiten. Das Playbook-Management sollte daher eine Option zur Stapelverarbeitung enthalten.

  Hilfreich ist dies z. B. in den folgenden Fällen:



Automatisierungseditor

Mithilfe des Automatisierungseditors können IT-Fachleute Abläufe als Playbooks codieren. Mit einem visuellen Editor geht diese Aufgabe sehr viel leichter als mit einem schlichten Quellcode-Editor. Dann können alle Beteiligten unabhängig von ihrer Programmiererfahrung Abläufe auf Quellcode-Ebene schreiben und umfassende, anspruchsvolle Playbooks erstellen.

Der visuelle Editor sollte dem BPMN-Standard (Business Process Model and Notation) genügen. Für geschäftliche User hat BPMN intuitive Symbole, während technische User weitergehende Möglichkeiten zur Darstellung hochkomplexer Prozesse bekommen.

- **Elemente der Benutzeroberfläche**
  Die Benutzeroberfläche ist zunächst eine Leinwand, auf der visuelle Playbooks erstellt werden. Gebraucht wird dazu ein Bereich, in dem die gewünschten Aktionen angegeben werden (z. B. `block_ip` oder `file_reputation`) und dazu die Parameter (per Eingabe oder Listenauswahl). Benötigt wird ferner ein Ort zum Testen und Debuggen, mit einfachem Wechsel zwischen Bearbeitungs- und Testmodus sowie einer Quellcodeansicht.

- **Code als Blöcke**
  Mithilfe von Blöcken zur Darstellung wichtiger Schritte lassen sich umfassende und komplexe Playbooks schreiben, ohne dass man in den Quellcode einsteigen müsste. Blöcke sollten 1:1, 1:n oder n:1 aufeinander bezogen sein, sodass eine geordnete Ausführung möglich wird.

- **Menschen im Entscheidungsprozess**
  Überwachte Automatisierung wird oft benötigt. Dann ist an einer Stelle in der Automatisierungssequenz ein Mensch gefragt, etwa um die weitere Ausführung freizugeben, zu überprüfen oder zu ergänzen. In den Playbooks sollte man daher festlegen können, wer auf diese Weise einbezogen werden soll, am besten zusammen mit der Art der Benachrichtigung oder der gewünschten Genehmigungsstufe sowie der Art des Fehlers, der gemeldet werden soll, falls ein oder mehrere Dienste nicht verfügbar sind.

- **Verfügbarkeit der Aktionsergebnisse**
  Neue Informationen sollten auf der Oberfläche des Automatisierungseditors als Eingaben, Parameter, nachgelagerte Aktionen, Entscheidungsblöcke usw. verfügbar sein. Die Ergebnisse vorangegangener Aktionen sollten visuell zugänglich und per Dropdown-Menü wählbar sein, wenn sie als Parameter einer nachgelagerten Aktion übergeben werden.

- **Zugriff auf den Playbook-Quellcode**
  Die Playbooks werden zwar im visuellen Editor erstellt, doch sollte deren Quellcode in Echtzeit generiert werden und der Autorin bzw. dem Autor zugänglich sein. Manche wollen ihre Playbooks (oder einen Teil davon) vielleicht lieber direkt als Quellcode erstellen. Der Wechsel zwischen dem visuellen und dem Quellcode-Modus sollte fließend möglich sein.

- **Kombinierte Arbeit an Playbooks**
  Im Automatisierungseditor sollte man das Playbook sowohl im Quellcode als auch auf der Ebene der visuellen Blöcke bearbeiten können. Mitunter kommt es vor, dass bei einzelnen Blöcken (z. B. Aktionen oder Entscheidungen) Modifizierungen auf Quellcode-Ebene nötig sind, die über die Möglichkeiten des visuellen Editors hinausgehen. Auch danach sollte es immer noch möglich sein, das Playbook weiter visuell zu bearbeiten.

- **Integriertes Testen, Debuggen und Laufzeitprotokollierung**
  Zu integrierten Entwicklungsumgebungen (Integrated Development Environments/IDEs) gehören standardmäßig auch Test- und Debugging-Funktionen. Im Automatisierungseditor sollte man also Playbooks gegen Warnmeldungen ausführen und dann die Ausführung verfolgen und die Ergebnisse festhalten können. Letztlich geht es darum, dass man die Playbooks auf einer einzigen Oberfläche umstandslos bearbeiten, testen und debuggen kann.

- **Abgesicherter Modus**
  Der Automatisierungseditor sollte auch einen abgesicherten Modus für Probeläufe neuer Playbooks bieten. Dieser Modus simuliert die Ausführung, ohne die Gegenstände der Automatisierung zu verändern.

App-Framework

Das App-Framework ist die Erweiterungsschnittstelle für neue Integrationen. Es verbindet die Plattform mit den Tausenden von Drittanbieter-Einzelprodukten, die es heutzutage gibt.

- **Offenes Ökosystem**
  Jede SOAR-Lösung verliert mit der Zeit an Schlagkraft, wenn sie nicht in der Lage ist, neue bzw. gefragte Marktangebote zu integrieren. Aus diesem Grund sollte eine SOAR-Lösung als offenes Ökosystem konzipiert sein, das die App-Entwicklung fördert. Neue Technologien müssen sich außerdem schnell integrieren lassen, ohne dass Änderungen an der Kernlösung erforderlich sind.
- **App-Entwicklung**
  Die App-Entwicklung ist eine Schlüsselkomponente offener Ökosysteme, denn damit lassen sich ganz unterschiedliche Technologien in die Playbooks integrieren. Eine SOAR-Lösung sollte daher direkt im Produkt die Möglichkeit einer optimierten App-Entwicklung bieten, sodass man vorhandene Apps einsehen, testen, erweitern und bearbeiten sowie eigene Apps neu erstellen kann – alles aus derselben Oberfläche heraus.

Metriken und Berichte

Metriken und Berichte sind überall dort unverzichtbar, wo es darum geht, die Dinge zu verstehen und zu quantifizieren. Eine SOAR-Lösung ist da keine Ausnahme. Während die Automatisierung mehr Leistung und Produktivität verspricht, sind Metriken der Weg, um die jeweilige Effektivität zu messen und herauszufinden, wo Optimierungen möglich oder gar nötig sind.

- **Flexible Dashboards**
  Die relevanten Erfolgskennzahlen unterscheiden sich von Unternehmen zu Unternehmen und hängen von vielen Faktoren ab. Man muss also in der Lage sein, die wichtigsten Leistungsindikatoren (Key Performance Indicators/KPIs) so zu organisieren, wie es für das Unternehmen sinnvoll ist. Mit einer ordentlichen SOAR-Lösung sollte man die Daten entsprechend anpassen und ordnen können.
- **Leistungsberichte**
  Effizienz ist in der Regel das Hauptmotiv der Automatisierung. Ob die Investition sich rechnet, zeigt sich erst dann, wenn Leistungszuwachs und Ressourceneinsparungen quantifizierbar sind.

  Das Reporting hierzu sollte u. a. diese Metriken umfassen:
  - Mean Time to Resolve (MTTR), die mittlere Zeit bis zur Behebung eines Fehlers.
  - Mean Dwell Time (MDT), die mittlere Verweildauer: die Zeitspanne von der Kompromittierung bis zu adäquaten Reaktionsmaßnahmen.
  - Durch automatisierte Ausführung eingesparte Fachkräftestunden.
  - Durch automatisierte Ausführung gewonnene Vollzeitäquivalente (VZÄ).
  - Durchschnittliche Zeitersparnis pro Playbook-Ausführung.
  - Finanzielle Ersparnis (VZÄ-Kosten × VZÄ-Gewinn).

- **Security-Effektivitätsberichte**
  Durch die Automatisierung sollten sich auch die Effektivität der Sicherheitsvorkehrungen und die Sicherheitslage des Unternehmens insgesamt verbessern. Außerdem sind die Anzahl der abgeschlossenen Sicherheitswarnungen und die Bearbeitungsgeschwindigkeit wichtige Argumente.

  Das Reporting hierzu sollte u. a. diese Metriken umfassen:
  - MTTR und MDT.
  - Gesamtzahl der neu ergangenen Warnmeldungen.
  - Täglich/stündlich/wöchentlich/monatlich neu ergangene Warnmeldungen.
  - Täglich/stündlich/wöchentlich/monatlich erledigte Warnmeldungen.
  - Leistung, gemessen an den Service Level Agreements (SLAs).

- **App-Integration und Playbook-Performance**
  Die Kenntnis der am häufigsten aufgerufenen Playbooks kann Aufschluss darüber geben, wo weiterer Investitionsbedarf besteht. Im Idealfall sollte das Playbook-Design darauf abzielen, dass falsch positive oder mit hoher Wahrscheinlichkeit richtig positive Alarme automatisch abgeschlossen werden.

  Damit Automatisierungslücken offenbar werden und die Effektivität der Tool-Integration messbar wird, sollte das Reporting hierzu u. a. die folgenden Metriken umfassen:
  - Automatisch abgeschlossene Alarme (z. B. pro Stunde, Tag, Woche, Monat).
  - App-Integrationen mit der größten Aktivität.
  - Am meisten eingesetzte Aktionen (manuell und automatisiert).
  - Automatik-Playbooks mit der größten Aktivität.
  - Ausführungszeiten der Playbooks.
  - Ausführungszeiten der Aktionen.

- **Anteil menschlicher Arbeit**
  Gleichwohl bleiben noch immer etliche Situationen, in denen IT-Fachleute im operativen Betrieb einer SOAR-Lösung selbst Hand anlegen müssen. Hierzu gehören Notfallpriorisierungen und Fälle, in denen bei einer Warnmeldung andere Maßnahmen zu ergreifen sind, sowie Playbooks, bei denen eine menschliche Genehmigung im Sinne einer überwachten Automatisierung vorgesehen ist.

  Damit der Anteil menschlicher Arbeit in den Abläufen der Automatisierung transparent wird, sollten beispielhaft die folgenden Metriken erfasst werden:
  - Warnmeldungen nach Person.
  - Abgeschlossene Warnmeldungen nach Person.
  - Durchschnittliche Genehmigungsdauer.
  - Anzahl der ausstehenden Genehmigungen.
  - Erforderliche Genehmigungen (z. B. pro Stunde, Tag, Woche, Monat).

Plattform-Merkmale

Einige wichtige Merkmale einer SOAR-Plattform sind eher qualitativer Natur. Zu prüfen sind die folgenden Kriterien daher in der Regel durch Beobachtung und durch den praktischen Umgang mit der Plattform.

Bereitstellungsoptionen

Eine SOAR-Lösung sollte sowohl On-premises- und Cloud- als auch Hybrid-Implementierungen unterstützen. Für welche Art der Bereitstellung Sie sich entscheiden, hängt in erster Linie von den Anforderungen Ihres Unternehmens ab (Budget, Speicher, Sicherheit etc.) sowie davon, wie Sie den Sicherheitsbetrieb am besten optimieren und den digitalen Wandel erleichtern.

Community-Modell

Im besten Fall unterstützt die SOAR-Lösung das Community-Modell durch ein offenes Ökosystem zur App-Entwicklung. Das sichert den langfristigen Erfolg, weil eine übermäßige Bindung an einen bestimmten Anbieter (Vendor Lock-in) vermieden wird und man leichter von einer Technologie zur anderen wechseln kann. Weil es in Sachen Sicherheit laufend Neues gibt, ist es außerdem unabdingbar, dass die Fachleute untereinander Playbooks, Best Practices und Konterstrategien gegen die aktuellen Bedrohungen austauschen.

Eine große, aktive Community

User profitieren am ehesten von den Erfahrungen Gleichgesinnter. Eine Community, die aktiv und groß genug ist, bietet die Möglichkeit, Playbooks und Apps auszutauschen oder Ideen für neue Use Cases der Automatisierung zu ventilieren. Für diesen Austausch von Ideen ist die möglichst einfache Community-Vernetzung eine entscheidende Voraussetzung. Speziell Messaging- und Kommunikationstools sind effektive Mittel zur technischen und gestalterischen Hilfestellung, zur Beantwortung von Fragen und für das Ideenspiel mit neuen Use Cases.

Zusammenarbeit

Zusammenarbeit ist ein wichtiges SOAR-Merkmal, das neben Funktionsumfang, App-Integration und Automatik-Playbooks bei der Vielzahl immer neuer Szenarien von entscheidender Bedeutung ist.

- **Zusammenarbeit in der Community**
  Was die Inhalte betrifft, so sollten sie über ein zentrales Repository zugänglich sein, ob sie nun von Anbietern stammen oder von Usern selbst. Dazu zählen sowohl technische Beiträge wie Playbooks, App-Integrationen und technische Hinweise als auch nichttechnische Beiträge wie Präsentationen, Blogs und andere Formen der Dokumentation.
- **Plattformweite Zusammenarbeit**
  Eine SOAR-Lösung sollte auch die Zusammenarbeit mit anderen befugten Stellen (Circles of Trust) erleichtern. Vor allem sollte sie unter privilegierten Gruppen im Sicherheitsteam des Unternehmens den Austausch sensibler Informationen unterstützen.

Kognition

Eine kognitive SOAR-Lösung nutzt menschliches Wissen zusammen mit früheren Beobachtungen bei künftigen Entscheidungen. Dieses Wissen wird in Form von Playbooks kodifiziert. Diese Methodik basiert auf Ausführungsstatistiken, bestimmten Merkmalen der eingespeisten Daten und den Resultaten vergangener Aktionen.

Aus diesen Informationen lassen sich Empfehlungen ableiten, die einzelne Aktionen oder ganze Playbooks bzw. Aktionsfolgen betreffen, die zusammen ein Playbook ergeben. Die derzeitigen kognitiven Fähigkeiten einer SOAR-Lösung sind ein ebenso wichtiges Entscheidungskriterium wie die entsprechende Strategie und Roadmap für zukünftige Implementierungen.

Optionale Automation

Die Teams beginnen die Use Cases der Automatisierung normalerweise einen nach dem anderen und gewinnen mit ihrem System immer mehr an Selbstsicherheit. Dann ist es extrem hilfreich, wenn die SOAR-Lösung Funktionen mitbringt, die eine selektive menschliche Interaktion mit automatisierten Playbooks erlauben. Die Einbindung menschlicher Expertise in einen Workflow sollte sowohl in Bezug auf bestimmte Assets (Punktsicherheitstools, Technologien etc.) als auch in Bezug auf einzelne Aktionen möglich sein.

Im ersten Fall (per Asset) sollten die jeweiligen Admins jedes Mal benachrichtigt werden, wenn eine betreffende Aktion ausgeführt wird. Im zweiten Fall (per Aktion) muss an jedem beliebigen Punkt eines Automatik-Playbooks eine Eingabeaufforderung möglich sein, die den Fachleuten die Möglichkeit gibt, fortzusetzen, anzuhalten oder abzubrechen. Mit solchen Instrumenten der Supervision können sich die Teams einfacher vergewissern, dass ihre programmierten Schritte wirklich funktionieren.

Sicherheit

Einer der wichtigsten SOAR-Aspekte ist logischerweise die eigene Sicherheit. Eine SOAR-Lösung handhabt Authentifizierungsdaten und andere hochsensible Informationen, verschlüsselt schutzwürdige Daten und unterstützt eine robuste rollenbasierte Zugriffskontrolle.

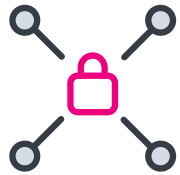
Zu den Security-Best-Practices einer SOAR-Lösung gehören u. a. diese:

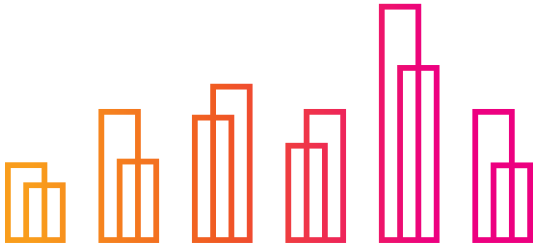
Verschlüsselte Security-Zugangsdaten

Keine Ablage von Zugangsdaten im Speicher

Unterstützung von IAM-Systemen (Identity and Access Management)

Unterstützung von Multi-Faktor-Authentifizierung





Skalierbarkeit

Eine taugliche SOAR-Lösung muss vertikal und horizontal skalierbar sein. Wenn im Laufe der Zeit immer weitere Use Cases hinzukommen, steigt damit auch der Bedarf an Rechenleistung. Eine SOAR-Lösung sollte daher so konzipiert sein, dass sie durch zusätzliche Hardware-Ressourcen (CPU, RAM etc.) vertikal skalierbar ist und durch eine größere Anzahl von Serverinstanzen für die Bereitstellung horizontal skalierbar.

Offen und erweiterbar

Security ist ständig in Bewegung, das zeigt allein die Unmenge der heutzutage erhältlichen Einzelprodukte. Eine SOAR-Lösung sollte daher auf Offenheit und Erweiterbarkeit ausgelegt sein. Sie sollte problemlos neue Sicherheitsszenarien, neue Produkte, neue Aktionen und neue Playbooks unterstützen.

Integrationsoffenes Framework

Unterm Strich besteht der Vorteil eines integrationsoffenen Frameworks darin, dass man Technologien integrieren und entfernen kann, ohne den automatisierten Betrieb zu beeinträchtigen. Außerdem sollte man die Möglichkeit haben, unabhängig vom SOAR-Anbieter eigene Integrationen zu entwickeln.

Gute Beispiele hierfür sind selbst entwickelte Anwendungen, benutzerdefinierte APIs, Anbieterschnittstellen in der Betaphase oder wenn die Funktionalität der gesamten Automatisierungsplattform erweitert wird. Das offene Framework sollte sich an anerkannte Standards und Programmiermodelle halten. Und es sollte an Dokumentation und Beispielen nicht sparen.

Schnittstellen ohne Einschränkungen

Einige Technologien bieten Schnittstellen als REST-APIs, mit SSH, für Syslog, benutzerdefinierte APIs oder mit bestimmten anderen Protokollen und Methoden. Ein erweiterbares Integrationsframework sollte aber keine Schnittstelleneinschränkungen erzwingen. Wenn die Automatisierungsplattform zu einem Produkt oder einer Anwendung Kontakt aufnehmen kann, dann sollte die Art der Schnittstelle bei der Integration keine Rolle spielen. Eine SOAR-Lösung muss einfach mit jeder Art von Schnittstelle umgehen können.

Mobil

Eine SOAR-Lösung ist dazu da, die Reaktionszeiten zu verkürzen, mit anderen Worten: die Verweildauer und die MTTR zu reduzieren. Rasche Reaktion bedeutet aber auch, dass die Sicherheitsfachleute erreichbar sein müssen. Nur sitzen die Profis nicht immer mit aufgeklapptem Laptop am Schreibtisch und warten darauf, dass sie gebraucht werden.

Deshalb ist es wichtig, dass eine SOAR-Lösung Plattformzugriff, -interaktivität und -kontrolle bequem von den Mobilgeräten der Fachkräfte aus ermöglicht. Dann können sie Playbooks unterwegs ausführen, sicherheitsrelevante Artefakte prüfen und Ereignisse nach Dringlichkeit sortieren, ohne dass sie ihren Laptop aufklappen müssten, sie können aus der Ferne Eingabeaufforderungen beantworten und sind immer erreichbar, ob am Schreibtisch oder unterwegs.

Einfache Handhabung

Professionelle Software ist selten wirklich einfach. Aber es ist doch möglich, die Reibungsverluste bei einer SOAR-Lösung zu reduzieren.

- **Installation und Einrichtung**
  Der Formfaktor einer virtuellen Appliance erleichtert die Bereitstellung, da viele Unternehmen ihre Infrastruktur schon (teilweise) virtualisiert haben.
- **Onboarding**
  Eine gute SOAR-Lösung kann die erste Lernkurve am Anfang erheblich leichter machen, und zwar durch einen Onboarding-Prozess, mit dem es leicht fällt, Systemeinstellungen zu konfigurieren, Verbindungen zu Datenquellen herzustellen und erste Playbooks zu aktivieren.
- **Rasche Automatisierung**
  Die Teams sollten möglichst schnell mit der Automatisierung beginnen können. Die SOAR-Lösung kann dazu beitragen, indem sie einen soliden Satz automatisierter Playbooks mitbringt. Wenn die User selbst schnell Automatik-Playbooks erstellen, testen und bereitstellen können, so ist das ein weiterer wichtiger Beschleuniger.

Geschäftliche Erwägungen

Die Technologie eines Unternehmens mag noch so großartig sein – dennoch gibt es jenseits des Produkts im klassischen Sinne Überlegungen, die wesentlichen Einfluss auf die Investitionsentscheidung haben. Ein wichtiger Gesichtspunkt ergibt sich aus den Qualitäten des Herstellerunternehmens. Wichtige Argumente sind aber auch die zusätzlichen Mehrwertdienste der Anbieter, die zusammen mit der Haupttechnologie letztlich erst das Gesamtprodukt bilden, das man als Käufer erwirbt und erlebt.

Anbietermerkmale

Bei einer Beschaffung spielen das Profil, die Qualität und das Zukunftspotenzial des Unternehmens eine Rolle. Tatsache ist, dass viele der neuen Anbieter früher oder später aufgeben müssen. Sicherer ist die Entscheidung für ein Unternehmen, das in der Lage ist, seine Versprechen zu halten.

Unternehmensgeschichte

Der Anbieter sollte über ausreichend Erfahrung in der Entwicklung von Sicherheitslösungen verfügen. Zwar ist SOAR ein relativ junges Marktsegment, doch seine Anfänge lassen sich viele Jahre zurückverfolgen. Es ist insofern durchaus von Bedeutung, wie es zur Gründung des Unternehmens kam und warum man sich auf das SOAR-Segment verlegt hat.

Ability to Execute

Am besten sehen Sie sich nach einem Unternehmen um, dessen Team aus erfahrenen Fachleuten besteht. Ob der Partner wirklich liefern kann – die „Ability to Execute“ –, lässt sich oft direkt an der Erfolgsbilanz der einzelnen Teammitglieder ablesen.

Kundenstamm

Die Art und die Qualität des Kundenkreises sind ein Abbild des Unternehmens selbst. Anspruchsvolle Unternehmenskunden haben einen potenziellen Anbieter vor dem Kauf gründlich überprüft.

Preise und Auszeichnungen

Werfen Sie auch einen Blick auf die Auszeichnungen und Preise, die das Unternehmen erringen konnte. Es sind Zeugnisse, die belegen, dass der Anbieter und seine Produkte den eigenen Ansprüchen auch gerecht werden. So unterschiedlich wie die Unternehmen ist auch die Qualität der Auszeichnungen.

Zusatzleistungen

Die Zusatzleistungen, die ein Unternehmen anbietet, können großen Einfluss darauf haben, wie die Umsetzung gelingt und ob das Projekt erfolgreich wird.

Professional Services

Der Security-Reifegrad in den Unternehmen ist sehr unterschiedlich. Im Zweifelsfall ist ein Anbieter ratsam, der professionelle Hilfestellung anbietet, was die Chancen einer erfolgreichen Einführung deutlich erhöht. Wichtig wäre auch, dass Fachleute zur Verfügung stehen, deren Dienste man in Anspruch nehmen kann, etwa bei der Einrichtung von Prozessen (falls nötig) oder bei der Umwandlung manueller Workflows in automatisierte Playbooks.

After-Sales Support

Viele Start-ups haben eine Spitzentechnologie und ausgezeichneten Support im Vorverkauf, doch bei der Unterstützung nach der Beschaffung ist Fehlanzeige. Es gilt also, zu prüfen, wie weit der Kundendienst reicht und ob das Unternehmen die Art von Service bietet, die Sie absehbar benötigen.

Und jetzt: Splunk

Unter Kontrolle statt unter Wasser – Dank Splunk.

Mit Splunk SOAR kann Ihr Team intelligenter arbeiten, schneller reagieren und die Sicherheit Ihres Unternehmens härten. Wiederkehrende Aufgaben können Sie damit einfach automatisieren. Dank automatischer Erkennung, Untersuchung und Reaktion bearbeiten Sie Sicherheitsvorfälle schneller, Sie steigern Produktivität, Effizienz und Präzision, und Sie stärken Ihre Verteidigung, indem Sie komplexe Workflows über Teams und Tools hinweg verbinden und koordinieren.

Splunk SOAR unterstützt auch eine breite Palette von Sicherheitsfunktionen: Event- und Ticket-Management, integrierte Bedrohungsinformationen, Reporting und Tools zur Zusammenarbeit sowie die Integration Ihrer bestehenden Sicherheitsinfrastruktur, sodass jeder Teil davon eine aktive Rolle in der Verteidigungsstrategie spielt und alles optimal zusammenarbeitet.

Noch mehr Möglichkeiten der Integration

Auf Splunkbase gibt es Tausende von Security-Apps von Drittanbietern zur Integration in Splunk SOAR. Mit solchen Integrationen kann Splunk SOAR Ihre Sicherheitstools eine Vielzahl an Aktionen ausführen lassen. Sie können z. B. VirusTotal anweisen, die File Reputation zu prüfen, oder die Cisco-Firewall, eine IP-Adresse zu blockieren. Das App-Modell von Splunk SOAR unterstützt die Integration von über 350 Tools und mehr als 2100 verschiedenen Aktionen, die alle auf Splunkbase verfügbar sind. Diese einsatzfertigen Apps, Dienstprogramme und Add-ons können Ihrem Team bei Themen wie Security Monitoring, Next-Generation Firewalls, fortgeschrittenem Bedrohungsmanagement und vielem mehr wertvolle Dienste leisten.

Erste Schritte.

Um mehr über Splunk SOAR zu erfahren, laden Sie die kostenlose Community Edition herunter oder fordern Sie hier weitere Informationen an.

22-23828-Splunk-SOAR Buyers Guide-EB-101_GER

splunk> turn data into doing