SIEM versus SOAR

Cybersicherheitsbedrohungen zuverlässig erkennen

Kai-Oliver Detken

Anomalie-Erkennung wird in Unternehmensnetzen immer notwendiger, um sich gegen Cyberattacken wirksam schützen zu können. Dafür werden immer mehr sogenannte SIEM-Systeme eingesetzt. Diese analysieren den Netzwerkverkehr und sammeln Loginformationen von diversen Netzkomponenten. Allerdings sind sie auf die Mithilfe von Security Operation Centern (SOC) angewiesen, in denen Sicherheitsspezialisten die Vorfälle analysieren und Handlungsempfehlungen aussprechen. Eine Gegenmaßnahme zu einem Angriff hängt daher von der menschlichen Bearbeitungszeit und Level-Agreements ab. Größere Wartezeiten können daher die Sicherheit eines Unternehmens beeinflussen.

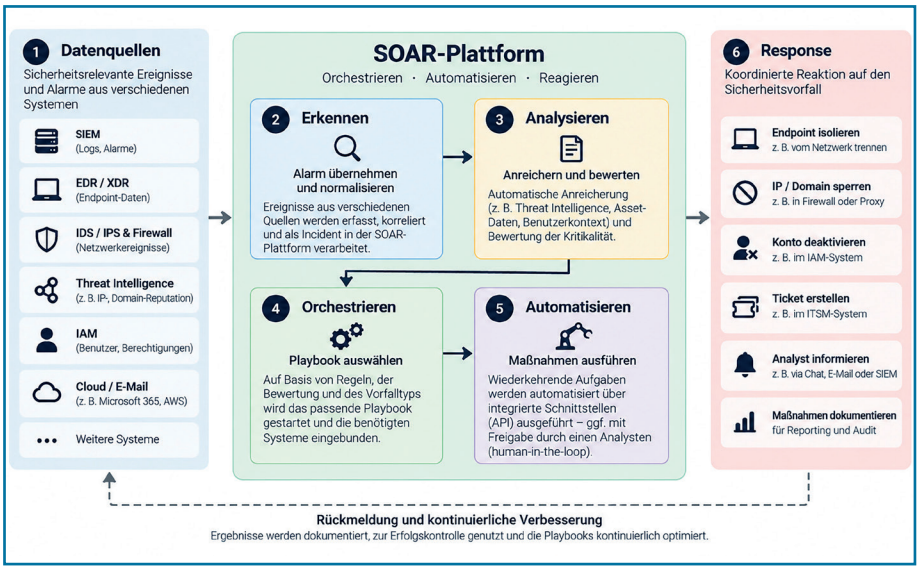


Bild 1: Das Ablaufdiagramm zeigt den Weg von einem Sicherheitsereignis von den Datenquellen über die SOAR-Plattform bis zur automatisierten oder manuellen Reaktion (Abbildung: Detken)

Die Weiterentwicklung von SIEM sind daher sogenannte SOAR-Systeme, die Daten über Cybersicherheitsbedrohungen sammeln, und auf Sicherheitsereignisse mit wenig oder gar keinen menschlichen Eingriffen zu reagieren. Doch wie funktionieren diese und welche Vor- und Nachteile lassen sich gegenüber SIEM ausmachen?

Security Orchestration, Automation and Response (SOAR) ist als reine Softwarelösung in der Cybersicherheit zu verstehen, die verschiedene Sicherheitstools verbindet, wiederkehrende Aufgaben automatisiert und die Reaktion auf Vorfälle beschleunigt. Sie besteht aus drei Kernsäulen:

- Orchestrierung (Orchestration): Integriert disparate Sicherheitstools, wie Firewalls, Endpunkt-Agenten und SIEM-Systeme, auf einer zentralen Plattform.
- Automatisierung (Automation): Erledigt Routineaufgaben wie Ticket-Erstellung, Datenanreicherung oder das Sperren kompromittierter Benutzerkonten ohne menschliches Eingreifen.
- Reaktion (Response): Nutzt standardisierte Arbeitsabläufe (Playbooks), um Bedrohungen koordiniert und in Sekundenschnelle abzuwehren.

Im Gegensatz dazu sammelt und korreliert ein Security Information and Event Management (SIEM) Sicherheitsereignisse und erzeugt daraus Alarme. SOAR setzt stärker bei der anschließenden Bearbeitung und Reaktion an und koordiniert dafür verschiedene Systeme. In modernen Plattformen verschwimmen diese Grenzen allerdings zunehmend.

SOAR-Arbeitsweise

Die Abbildung 1 zeigt ein Ablaufdiagramm, das den Weg von einem Sicherheitsereignis von den Datenquellen über die SOAR-Plattform bis zur automatisierten oder manuellen Reaktion zeigt, um die Arbeitsweise von

Prof. Dr.-Ing. Kai-Oliver Detken studierte Informationstechnik an der Universität Bremen und promovierte im Fachbereich Informatik. Heute ist er Geschäftsführer der DECOIT GmbH & Co. KG, doziert an der Hochschule Bremen und arbeitet als freier Autor im IT-Umfeld

solchen Systemen zu verdeutlichen. Die SOAR-Plattform bildet dabei die zentrale Koordinationsinstanz. Sicherheitsrelevante Ereignisse und Alarme werden zunächst aus unterschiedlichen Quellen übernommen, beispielsweise aus einem SIEM, Endpoint Detection and Response (EDR) und Extended Detection and Response (XDR), Firewalls, Intrusion Detection System (IDS) und Intrusion Prevention System (IPS), Identity and Access Management (IAM) oder Threat-Intelligence-Diensten.

Anschließend erfolgen eine automatisierte Anreicherung und Bewertung des Ereignisses. Beispielsweise kann eine verdächtige IP-Adresse mit Threat-Intelligence-Quellen abgeglichen, ein betroffener Benutzer im IAM identifiziert und gleichzeitig geprüft werden, welche weiteren Aktivitäten von dem betreffenden Endgerät ausgegangen sind. Auf Basis dieser Informationen entscheidet die SOAR-Plattform anhand eines hinterlegten Playbooks, welche weiteren Schritte erforderlich sind. Ein Playbook beschreibt dabei einen standardisierten Incident-Response-Prozess. Je nach Art und Kritikalität des Ereignisses können einzelne Maßnahmen automatisch ausgeführt oder einem Sicherheitsanalysten zur Entscheidung vorgelegt werden. Die eigentliche Reaktion (Response) kann beispielsweise darin bestehen, einen kompromittierten Endpunkt zu isolieren, eine IP-Adresse oder Domain auf der Firewall zu sperren, ein Benutzerkonto vorübergehend zu deaktivieren oder automatisch ein Ticket für das SOC zu erzeugen. Sämtliche Maßnahmen und Ergebnisse werden dokumentiert und können wiederum zur Optimierung der Playbooks verwendet werden.

Playbook-Praxisbeispiel

Ein Playbook ist eines der zentralen Elemente einer SOAR-Plattform. Es beschreibt einen standardisierten, möglichst automatisierbaren Ablauf zur Behandlung eines bestimmten Sicherheitsereignisses. Man kann es sich als digitalen Incident-Response-Prozess vorstellen, der festlegt, welche Prüfungen durchgeführt, welche Entscheidungen getroffen und welche Gegenmaßnahmen ausgelöst werden. Ein Playbook besteht typischerweise aus einzelnen Aktionen,

Ein Playbook beschreibt einen standardisierten Ablauf zur Behandlung eines Sicherheitsereignisses

Bedingungen und Entscheidungspunkten. Dabei können vollständig automatisierte Schritte mit manuellen Freigaben durch einen SOC-Analysten kombiniert werden. Gerade bei Maßnahmen mit größeren Auswirkungen – etwa der Sperrung eines Benutzerkontos oder der Isolation eines produktionskritischen Servers – ist ein solcher Human-in-the-Loop sinnvoll (Bild 1).

Als Praxisbeispiel wird hier einmal eine Phishing-Mail-Attacke durchgespielt, wie sie durch ein SOAR-System bekämpft werden würde. Ein Mitarbeiter meldet dabei eine verdächtige E-Mail. Dadurch wird im SOAR-System ein Playbook erstellt, das in Tabelle 1 wiedergegeben wird. Dabei wird das Ereignis erfasst, die E-Mail analysiert, Indikatoren extrahiert, Threat-Intelligence-Quellen abgefragt, das Risiko bewertet, Maßnahmen eingeleitet und abschließend der Vorfall dokumentiert. Entscheidend ist hierbei die Entscheidungslogik, denn ein Playbook ist keine lineare Folge von Befehlen. Das SOAR orchestriert die verschiedenen Systeme und führt einen erheblichen Teil dieser Schritte automatisch durch, wie die Tabelle 1 zeigt.

Playbooks bilden in einer SOAR-Plattform standardisierte Incident-Response-Prozesse in Form ausführbarer Workflows ab. Sie definieren auf Basis eines bestimmten Sicherheitsereignisses die erforderlichen Analyse-, Entscheidungs- und Reaktionsschritte und koordinieren hierfür die angebundenen Sicherheitssysteme. Einzelne Aktionen können vollständig automatisiert oder nach Freigabe durch einen Sicherheitsanalysten ausgeführt werden. Abbildung 2 zeigt zusätzlich zur Tabelle 1 übersichtlich als Grafik, wie ein Playbook bei einer Phishing-Mail ablaufen könnte.

Schritte	Aktion des Playbooks	Automatisierung
1	Verdächtige E-Mail aus E-Mail-System übernehmen	Automatisch
2	Absender, Header, URLs und Anhänge extrahieren	Automatisch
3	IPs, Domains und Datei-Hashes gegen Threat-Intelligence-Quellen prüfen	Automatisch
4	Reputation und weitere vorhandene Alarme zum Absender ermitteln	Automatisch
5	Risiko anhand der Ergebnisse klassifizieren	Automatisch
6	Bei hohem Risiko wird die E-Mail aus weiteren Postfächern entfernt	Automatisch / Freigabe
7	Schädliche Domain bzw. URL auf Proxy/Firewall sperren	Automatisch / Freigabe
8	Prüfen, ob Benutzer den Link bereits aufgerufen haben	Automatisch
9	Bei kompromittiertem Konto das Benutzerkonto sperren und vorhandene Sessions beenden	ggf. Analysten-freigabe
10	Incident-Ticket erzeugen und alle Aktionen dokumentieren	Automatisch

Tabelle 1: Anhand dieses Playbooks ist zu sehen, wie das SOAR die verschiedenen Systeme orchestriert und einen erheblichen Teil dieser Schritte automatisch selbst durchführt

Vergleich mit SIEM-System

Wenn man SOAR-Systeme mit SIEM-Systemen direkt vergleicht, kann man allgemein feststellen, dass SIEM-Systeme hauptsächlich erkennen und bewerten und SOAR-Systeme organisieren und reagieren. Bei SIEM-Systemen muss daher der IT-Administrator oder das Security Operation Center (SOC) mehr manuell agieren und kann sich weniger auf Automatismen verlassen.

Der Unterschied zwischen beiden Systemen wird an einem anderen konkreten Vorfall besonders deutlich. Ein SIEM-System erhält beispielsweise Login-Ereignisse aus dem Active Directory (AD) und stellt fest, dass es 20 fehlgeschlagene Anmeldungen gab, bevor eine Anmeldung erfolgreich war, sowie dass der Standort der Anmeldung ungewöhnlich ist und auf sensible Systeme zugegriffen wird. Durch die Korrelation dieser Ereignisse erzeugt das SIEM dann folgenden Alarm: „Verdacht auf kompromittiertes Benutzerkonto“ mit einer hohen Kritikalität (roter Alarm). Ein IT-Administrator muss nun entscheiden, ob er diesem Alarm nachgehen möchte. Das kann am Wochenende zu einem großen Zeitfenster für den Angreifer führen und kann nur durch den kostspieligen 24/7-Betrieb eines SOC kompensiert werden.

Im Zusammenspiel mit einem SOAR-System kann dieser Alarm hingegen vom SIEM an das SOAR übergeben werden. Dort startet dann beispielsweise das Playbook „Compromised Account“. Dieses fragt automatisch weitere Informationen ab, überprüft die IP-Adresse über Threat Intelligence, fragt EDR/XDR nach Aktivitäten des betreffenden Rechners und kontrolliert weitere Anmeldungen des Benutzers. Erhärtet sich der Verdacht, kann das SOAR anschließend beispielsweise aktive Sessions beenden, das Benutzerkonto sperren, den Endpunkt isolieren, ein Incident-Ticket anlegen und den SOC-Analysten informieren. Kritische Aktionen können zusätzlich von einer manuellen Freigabe abhängig gemacht werden. So könnte auch am Wochenende schnell und adäquat reagiert werden.

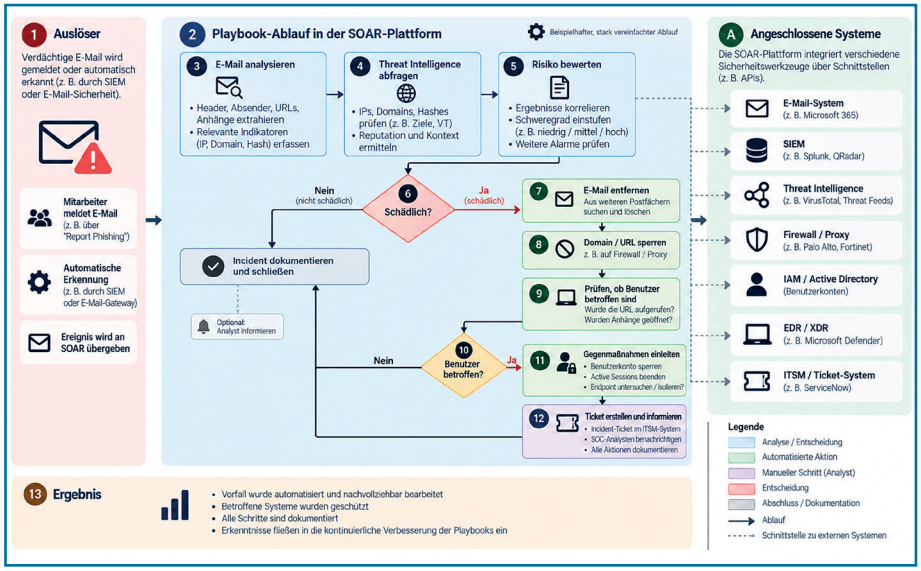


Bild 2: Playbooks bilden in einer SOAR-Plattform standardisierte Incident-Response-Prozesse in Form ausführbarer Workflows ab. Hier ist zu sehen, wie ein Playbook bei einer Phishing-Mail ablaufen könnte (Abbildung: Detken)

Fazit

Insgesamt kann man festhalten, dass der Automatisierungsgrad bei einem SOAR-System höher ist, als bei vergleichbaren SIEM-Lösungen. Dadurch werden automatische Reaktionen ermöglicht, die den IT-Administrator entlasten, ohne gleich ein SOC mit 24/7-Betrieb hinzuziehen zu müssen. Allerdings kann dies auch dazu führen, dass sensible und wichtige Systeme vorschnell ausgeschaltet werden, ohne die Folgen ausreichend abzuwägen.

Der Automatisierungsgrad bei einem SOAR-System ist höher, als bei vergleichbaren SIEM-Lösungen

Auf der anderen Seite verschmelzen die Grenzen zwischen SIEM und SOAR auch immer mehr, weil auch SIEM-Produkte inzwischen Automatisierungs- und Response-Funktionen anbieten. Vergleicht man die Produkte von Herstellern, die beide Funktionalitäten integriert haben oder SOAR als gekoppeltes Produkt zur Verfügung stellen, wird deutlich: Während SIEM und SOAR ursprünglich als getrennte Lösungsbereiche betrachtet wurden, führen moderne Hersteller beide Funktionen zunehmend in integrierten Security-Operations-Plattformen zusammen. Beispiele hierfür sind Microsoft Sentinel, Splunk Enterprise Security, Google Security Operations und Elastic Security. Andere Anbieter wie Fortinet bieten weiterhin dedizierte SIEM- und SOAR-Produkte an, integrieren deren Funktionen jedoch ebenfalls zunehmend in übergreifende SOC-Plattformen.

Elastic Security bietet beispielsweise eigene Workflows an, die der Hersteller selbst als native SOAR-Funktionalität bezeichnet. Diese Workflows haben direkten Zugriff auf Alerts, Cases und Untersuchungsdaten und können den Ablauf von der Auswahl über Anreicherung und Eskalation bis zur Reaktion automatisieren. Dadurch soll kein separates SOAR-Produkt erforderlich sein. Damit steht Elastic beispielhaft für die zunehmende Verschmelzung von SIEM, SOAR und XDR zu integrierten Security-Operations-Plattformen. Dieser Weg wird auch zunehmend von anderen Herstellern angestrebt.