RAPID7

KUNDENRATGEBER

Security Information and Event Management-Lösungen (SIEM)

Praktische Tipps für die Auswahl Ihrer ersten (bzw. nächsten) SIEM-Lösung

TABLE OF CONTENTS

Einführung: Willkommen zur neuen Herausforderung des Security Information and Event Management

Obwohl Lösungen für das Security Information and Event Management (SIEM) bereits seit beinahe zwei Jahrzehnten auf dem Markt sind, erinnern moderne SIEM-Lösungen nur noch wenig an die ursprünglich zu diesem Zweck verwendeten Log-Management-Systeme. Nicht nur die Sicherheitslandschaft hat sich weiterentwickelt, auch bei den SIEM-Lösungen hat sich etwas getan (zumindest bei einigen).

Heute beinhalten die effektivsten automatisierten Lösungen eine Benutzer- und Angreiferverhaltensanalyse, Täuschungstechnologie (Angreiferfallen), sowie weitere innovative Elemente zur Erkennung von bekannten und unbekannten Bedrohungen. Außerdem bieten sie eine umfassende Netzwerktransparenz und beschleunigen die Bedrohungsanalyse und -behebung.

Zwar senkt die erfolgreiche Bereitstellung einer SIEM-Lösung das Risiko deutlich, jedoch gibt es dabei einen großen Makel: Projekte zur Bereitstellung von SIEM-Lösungen scheitern häufig. Auch heute tun sich zu viele Unternehmen noch sehr schwer mit der Bereitstellung einer neuen SIEM-Lösung. Der Erfolg stellt sich nicht so rasch ein und die Lösung entfaltet nicht ihr volles Potenzial. Meistens liegt das daran, dass die gewählte SIEM-Lösung nicht optimal auf die speziellen Anforderungen, die Reife und die Ressourcen des Unternehmens abgestimmt ist.

Ganz gleich, ob Ihr Unternehmen derzeit über keine SIEM-Lösung verfügt oder die aktuelle SIEM-Lösung Ihre Nerven überstrapaziert hat, kann sich die Suche nach der richtigen SIEM-Lösung für Ihr Unternehmen auf dem Markt für Sicherheitsprodukte zu einem richtigen Vollzeitjob entwickeln. (Was natürlich nicht in Frage kommt, weil Ihr Job eigentlich darin besteht, Risiken in Bezug auf die Mitarbeiter und IT-Assets zu identifizieren und zu mindern.)

Dieser Ratgeber gibt Ihnen das Rüstzeug für die Evaluierung der SIEM-Lösungen an die Hand, indem Sie zunächst eine kurze Einführung in den heutigen Markt für SIEM-Produkte, sowie in die angebotenen Funktionen erhalten. Darüber hinaus erfahren Sie, wie sich die Funktionen dieser Lösungen individuell an Ihre speziellen Anforderungen anpassen lassen. Sie erfahren ferner, welche drei Funktionalitäten jede SIEM-Lösung unbedingt bereitstellen sollte und welche Fragen Sie den Anbietern stellen sollten, um einschätzen zu können, wie gut die jeweilige Funktionalität umgesetzt wird.

SIEM-Lösungen fördern Wachstum der Sicherheitsausgaben weltweit

Laut dem Forschungs- und Beratungsunternehmen Gartner werden Lösungen für die Sicherheitsprüfung, das IT-Outsourcing und das Security Information and Event Management (SIEM) die am schnellsten wachsenden Teilsegmente des Sicherheitsmarktes sein und das Wachstum in den Segmenten für Infrastrukturschutz und Sicherheitsservices antreiben. Weltweit werden laut Gartner im Jahr 2018 voraussichtlich 96 Milliarden US-Dollar für Unternehmenssicherheit ausgegeben.[1]

1 Gartner, „Gartner Forecasts Worldwide Security Spending Will Reach $96 Billion in 2018, Up 8 Percent from 2017", 7. Dezember 2017.

01 Schutz vor heutigen Bedrohungen

Während die Guten sich mit Sicherheitslösungen und Best Practices wappnen, um die Oberhand über Cyberkriminelle zu gewinnen, kann es in Bezug auf neue Technologien weiterhin zu einem Wettrüsten kommen. Als Beispiel hierfür wären Big Data und künstliche Intelligenz (KI) zu nennen. Ebenso wie ihre White-Hat-Pendants nutzen Cyberkriminelle zunehmend maschinelles Lernen und KI, um durch intelligente Auswertung von Big Data Erkenntnisse zu gewinnen. Cyberkriminelle setzen diese Technologien ein, um ihre Angriffe zu perfektionieren und erfolgreicher zu gestalten.

Unternehmen, die nicht mit den aktuellen Neuerungen in puncto Sicherheit Schritt halten, leiden immer noch stark unter Datensicherheitsverletzungen. Alljährlich gelangen so personenbezogene sowie Finanz- und Patientendatensätze im zweistelligen Millionenbereich in die falschen Hände. Laut Angaben der US-amerikanischen Organisation Identity Theft Resource Center wurde im Jahr 2017 mit 1.579 entdeckten Datensicherheitsverletzungen ein Negativrekord verzeichnet. Dies entspricht einer Steigerung um 45 % gegenüber dem Vorjahr.[2]

2 Identity Theft Resource Center, 2017 „Annual Data Breach Year-End Review", 2018

Spear-Phishing- und Social-Engineering-Angriffe entwickeln sich ebenfalls weiter. In seinem Data Breach Investigations Report von 2018 berichtet Verizon, dass Phishing und Pretexting zu den beiden wichtigsten Taktiken für Social-Engineering-Angriffe gehören.

Cyberkriminellen einen Schritt voraus bleiben

Die heutige Bedrohungslandschaft ist zweifelsohne beunruhigend, aber es stehen Lösungen zur Verfügung, mit denen Sicherheitsteams den Cyberkriminellen einen Schritt voraus bleiben können. Eine SIEM-Lösung, die Log- und Eventdaten in einem modernen Netzwerk zentralisieren kann, ist beispielsweise zur Erkennung von verdächtigen Aktivitäten in der Lage, die zu Datensicherheitsverletzungen führen können. Hierzu zählen u. a. Identitätsbetrug mithilfe gestohlener Zugangsdaten und Seitwärtsbewegungen im Netzwerk (das sogenannte Lateral Movement). Durch Analyse der Angriffe bei unseren Managed Detection and Response-Kunden, die Forschungsarbeit bei Rapid7, sowie unsere Incident-Response- und Penetrationstest-Teams konnten wir feststellen, dass sich Angreifer immer wieder auf drei Aspekte konzentrieren, um unerlaubten Zugang zu Netzwerken zu erlangen: (1) Schwachstellen, (2) Fehlkonfigurationen und (3) Zugangsdaten.

ANGRIFFSVEKTOR	WARUM TRANSPARENZ NOTWENDIG IST	WELCHE UNTERSTÜTZUNG SIEM BIETET
Schwachstellen	In mehr als 250 Szenarien haben Penetrationstester in 84 % der Fälle mindestens eine Schwachstelle in Produktionssystemen ausgenutzt.	Erkennt Aktivitäten (z. B. Rechteausweitungen und Lateral Movement), die im Zusammenhang mit der Ausnutzung von Schwachstellen auftreten.
Fehlkonfigurationen	In 80 % der Fälle wurde bei Penetrationstests mindestens eine Netzwerk-Fehlkonfiguration erfolgreich ausgenutzt. Bei Betrachtung aus der Innenperspektive steigt dieser Wert sogar auf 96 %.	Zeigt Fehlkonfigurationen von Benutzerkonten und Komponenten auf (z. B. unbekannte Administratoren, gemeinsam genutzte Konten und Überwachung der Dateiintegrität).
Zugangsdaten	Bei 53 % der Penetrationstests konnten mindestens einmal erfolgreich Zugangsdaten abgefangen werden.	Identifiziert verdächtige Authentifizierungen und löst ggf. Untersuchungs-Workflows aus.

Quelle: Rapid7, „Under the Hoodie: 2018"

FRAGEN SIE SICH: **Warum eine SIEM-Lösung einsetzen?**

Stellen Sie sich die folgenden Fragen, um besser zu verstehen, weshalb die Implementierung einer SIEM-Lösung in Ihrem Unternehmen notwendig ist:

Welche Ergebnisse haben Ihre letzten Penetrationstests erbracht?

Welche Ergebnisse hat der letzte Test Ihres Incident-Response-Plans erbracht?

Wie würden Sie die Qualität und Wirksamkeit Ihrer Bedrohungsanalyse bewerten? Dies schließt Informationen ein, die Ihr Team möglicherweise aus der Analyse von Angriffen auf Ihr Netzwerk bereitstellt.

Wie sieht der erfolgreiche Einsatz einer SIEM-Lösung aus?

Sehen Sie sich unseren Webcast „Smashing the Mold: What to Expect from Modern SIEM“ an, in dem näher erläutert wird, was Sie von einer modernen SIEM-Lösung erwarten können.

02 Einsatz von SIEM-Lösungen für die Bedrohungserkennung und -Überwachung sowie das Incident Management

Wahrscheinlich durchforsten Sie den Markt nach einer SIEM-Lösung, weil Sie die Fähigkeit Ihres Unternehmens zur Erkennung gängiger und neuen Bedrohungen verbessern möchten. Eventuell suchen Sie auch nach einer SIEM-Lösung, die verbesserte Funktionen für die Sicherheitsüberwachung bereitstellt und eine stärkere Transparenz ermöglicht (insbesondere in den heute gängigen Hybrid- und Multi-Cloud-Umgebungen). Falls die Compliance-Berichterstattung ein ausschlagender Faktor ist, sollte die jeweilige SIEM-Lösung in der Lage sein, Unterstützung mit Dashboards zu bieten und die Durchsetzung der Sicherheitsrichtlinien zu gewährleisten.

Um diesen zentralen Anwendungsfällen sowie weiteren Szenarios gerecht zu werden, müssen SIEM-Lösungen drei wichtige Fähigkeiten bereitstellen (auf die in Kapitel 3 näher eingegangen wird):

- **Datensammlung:**
  Daten in Ihrer Umgebung erheben und zentralisieren und das einfache Durchsuchen dieser Daten ermöglichen
- **Analyse:**
  Identifizieren von Risiken und Bedrohungen durch Auswertung der Daten mithilfe verschiedener Techniken
- **Gegenmaßnahmen:**
  Unterstützung bei der Ergreifung von Maßnahmen in Bezug auf die Ergebnisse mittels Orchestrierung und Berichterstattung

Der eigentliche Unterschied zwischen den heute auf dem Markt verfügbaren SIEM-Lösungen besteht in der Art und Weise, wie diese die einzelnen Fähigkeiten implementieren. Einige Lösungen legen das Hauptaugenmerk stärker auf die Datensammlung und das Datenmanagement, während andere Lösungen die Analyse über die Gegenmaßnahmen stellen. Wieder andere Lösungen stellen umfassende Funktionalitäten in allen drei Bereichen bereit.

IN BEZUG AUF SIEM-LÖSUNGEN ZU VERMEIDENDE FALLSTRICKE

Zu viele Alerts: Durch aussagekräftigen Kontext und Priorisierung wird eine Flut an Alerts vermieden

Vertrauen auf Regeln: In Log-Dateien sind nicht alle Anzeichen von Eindringungsversuchen zu finden. Stellen Sie sicher, dass Ihre SIEM-Lösung zusätzliche Erkennungstechnologien (z. B. Honeypots und Honey Credentials) verwendet, um loggestützte Erkennungsregeln zu ergänzen.

Langwierige, komplexe Bereitstellungen: Suchen Sie nach einer intuitiven Lösung mit unmittelbar einsatzbereiten Analysefunktionen und vorgefertigten Erkennungsverfahren. Oder wählen Sie besser eine Cloud-Lösung, um die Hardware- und Softwareinstallation sowie den zugehörigen Verwaltungsaufwand zu vermeiden.

Keine Analyse der Benutzeraktivitäten: Bestehen Sie auf Funktionen für die Analyse von Benutzeraktivitäten, um den Missbrauch von gestohlenen Zugangsdaten bzw. unsichere Zugangsdaten zu erkennen.

Zu hoher Zeit- und Kostenaufwand für die Datenverwaltung: Wählen Sie eine Lösung, die ein Preismodell auf Asset-Basis anbietet, um Kosten für Überschreitungen des Datenkontingents zu vermeiden.

Beschränkte Transparenz von Cloud-Diensten: Da immer mehr Unternehmen zu Cloud-Lösungen wie Microsoft Office 365 oder Salesforce übergehen, muss Ihre SIEM-Lösung sich in Ihre Cloud-Dienste und IaaS integrieren lassen und deren Überwachung ermöglichen.

SIEM-Bereitschaft des Unternehmens beurteilen

Um für Ihr Unternehmen ungeeignete SIEM-Lösungen und enttäuschende Ergebnisse zu vermeiden, müssen Sie die einzelnen Aspekte dieser drei Funktionalitäten sorgfältig abwägen und auf der Grundlage einer ehrlichen Einschätzung der Fähigkeiten und Ressourcen Ihres Teams feststellen, ob die Lösung den Anforderungen Ihres Unternehmens gerecht wird.

Folgende Fragen sollten Sie sich diesbezüglich stellen:

- **Welchen Kompetenzstand besitzt Ihr Team gegenwärtig in puncto Sicherheit?**

  SIEM-Rundumlösungen können Ihre Mitarbeiter leicht mit Funktionen überfordern, die Ihr Unternehmen eigentlich nicht für die erfolgreiche Arbeit benötigt.

- **Verfügt Ihr Team über die internen Qualifikationen rund um das Schreiben von Log-Abfragen, die Prüfung von Warnmeldungen und die Incident Response, sowie zur Umsetzung der Prüfungsergebnisse in präventive Schutzmaßnahmen?**

  Mangelnde Qualifikationen sind ein gängiges Problem für Unternehmen und stellen häufig auch den Grund für das Scheitern von SIEM-Projekten dar. Dies bedeutet jedoch nicht, dass Sie auf die Bereitstellung einer SIEM-Lösung verzichten müssen: Ein MDR-Service (Managed Detection and Response) ist möglicherweise für Ihre aktuellen Anforderungen die bessere Wahl.

- **Verfügen Sie über erprobte, skalierbare Prozesse rund um die Bedrohungserkennung und -untersuchung?**

  Viele Teams haben Mühe, alle eingehenden Alerts zu prüfen, da die Überprüfung und Vorabsichtung das Umschalten zwischen mehreren Tools und die Suche in nicht aufbereiteten Logs erfordert. Ziehen Sie den Einsatz einer SIEM-Lösung mit Orchestrierungs- und Automatisierungsfunktionen oder unterstützte Integrationen in Anwendungen von SOAR/SAO-Anbietern in Betracht. So können Sie wiederkehrende Prozesse – u. a. auch die Bedrohungseindämmung – automatisieren und gängige Tools (Active Directory, EDR, Firewall und NAC) direkt in der SIEM-Lösung verwalten.

FRAGEN SIE SICH:

Welche Ziele verfolgen Sie mit der Implementierung der SIEM-Lösung?

Wichtige Anwendungsfälle für SIEM-Lösungen sind u. a. Bedrohungserkennung, Überwachung und Transparenz, Compliance-Berichterstattung und Incident-Response-Management. Darüber hinaus gibt es jedoch zahlreiche weitere Anwendungsfälle. Bevor Sie mit der Suche nach einer SIEM-Lösung beginnen, sollten Sie Ihre wichtigsten Anwendungsfälle ermitteln und sich darüber klar werden, wie Sie diese mithilfe einer SIEM-Lösung abdecken möchten. Auf diese Weise können Sie Ihre Anstrengungen auf die Lösungen konzentrieren, die Ihren Anforderungen präzise gerecht werden, und lassen somit das undurchschaubare Dickicht der zahlreich angebotenen Lösungen auf einem stark umkämpften Markt hinter sich.

03 Evaluieren von SIEM-Lösungen

Betrachten wir nun die drei wichtigsten Funktionalitäten einer SIEM-Lösung im Detail. In jedem Abschnitt finden Sie eine Liste von Fragen, die Sie dem SIEM-Lösungsanbieter stellen können, um mehr darüber zu erfahren, wie der Anbieter die jeweilige Funktionalität implementiert und warum das wichtig ist.

Datensammlung

Die Datensammlung bildet die Grundlage jeder SIEM-Lösung. Dieser Aspekt hat sich seit der erstmaligen Einführung von SIEM-Lösungen nicht verändert. Verändert hat sich allerdings die Art und Weise, in der SIEM-Lösungen damit umgehen.

Die von Ihnen gewählte SIEM-Lösung sollte Sie beim Management der von Sicherheitsanwendungen generierten Rich Data unterstützen. Sie sollte es Ihnen ermöglichen, sämtliche Event- und Log-Daten zu zentralisieren, zu durchsuchen und zu visualisieren und die Authentifizierung für alle Nutzer und alle Komponenten und Dienste, darunter auch Cloud-Dienste, nachzuverfolgen.

Um „blinde Flecken" für das Sicherheitsteam zu vermeiden, sollte die SIEM-Lösung das gesamte Netzwerk überwachen können, einschließlich der Endpunkte, die sich außerhalb des Unternehmens befinden. Seien Sie vorsichtig bei Preismodellen auf der Basis der Menge der verarbeiteten oder indexierten Daten. Diese könnten Unternehmen eventuell davon abhalten, wichtige Datenquellen einzubeziehen. Damit Angriffe zuverlässig erkannt werden können, muss die SIEM-Lösung alle Aktivitäten im Netzwerk erfassen. Wird die Anzahl der Datenquellen aus Kostengründen beschränkt, kann dies die Fähigkeit der SIEM-Lösung zur Erkennung von Bedrohungen ernsthaft behindern.

FRAGEN SIE DEN LÖSUNGSANBIETER:

Wie gründlich erfolgt die Datensammlung bei dem Anbieter? SIEM-Lösungen, deren Fokus auf der Erkennung von Bedrohungen liegt, wissen um die Bedeutung der Sammlung von Daten in der gesamten Umgebung, u. a. Daten von integrierten oder modularen EDR-Agenten (Endpoint Detection and Response). Die Integration in Cloud-Dienste ist bei vielen SIEM-Lösungen heute Standard. Stellen Sie jedoch sicher, dass der Anbieter die von Ihrem Unternehmen genutzten Dienste unterstützt.

Erfasst der Lösungsanbieter Daten zur Unterstützung der Benutzerverhaltensanalyse? Eine SIEM-Lösung ist das einzige Sicherheitstool mit der realen Möglichkeit, gefährliches Lateral Movement und die Verwendung gestohlener Zugangsdaten aufzudecken. Zu diesem Zweck sammelt die Lösung Daten in der IT-Umgebung (z. B. Active Directory). Sie benötigen keine SIEM-Lösung, wenn Sie lediglich Firewall-Logs leichter für die Suche zugänglich machen wollen. Sie brauchen eine solche Lösung dagegen zwingend, um Bedrohungen zu erkennen, die Sie sonst übersehen würden. Darum ist es von entscheidender Bedeutung, dass Ihre SIEM-Lösung die richtigen Daten sammelt, um Risikobenutzer und externe Angreifer automatisch zu erkennen.

Wo werden die Daten gespeichert? Je weniger Vollzeitkräfte Sie für sicherheitsbezogene Aufgaben abstellen können, desto eher sollten Sie eine Cloud-SIEM-Lösung (Software as a Service, SaaS) in Betracht ziehen. On-Premise-Bereitstellungen erfordern eine Hardware- und Softwareverwaltung sowie Upgrades, um mit dem Datenzuwachs Schritt zu halten. Dagegen übernehmen Cloud-SIEM-Lösungen die gesamte Datenspeicherung, -verwaltung und -sicherheit für Sie, wobei Sie die Gewissheit haben können, dass Ihre Event- und Logdaten nicht in die Hände von Hackern fallen.

Analysefunktionen

Während klassische SIEM-Lösungen allgemeine, regelbasierte Analysen für die Korrelation von Informationen auf Netzwerkebene bereitstellen, müssen SIEM-Lösungen heute erweiterte Analysefähigkeiten bieten, um Bedrohungen, u. a. auch mehrstufige Angriffe und ungewöhnliches Nutzerverhalten, besser erkennen zu können. Erweiterte Analysefunktionen minimieren die Anzahl der Fehlalarme, priorisieren Alerts auf der Grundlage des Risikos und verringern die Gesamtzahl der zu prüfenden Alerts.

FRAGEN SIE DEN LÖSUNGSANBIETER:

Wie unterstützt Sie die SIEM-Lösung bei der Erkennung der im MITRE ATT&CK Framework dokumentierten Schwachstellen?[3] Bei monolithischen Legacy-SIEM-Lösungen müssen neue Erkennungsverfahren vom Anbieter erstellt, in der On-Premise-SIEM-Lösung bereitgestellt, vom Analystenteam möglicherweise aktiviert, mit relevanten Daten abgeglichen und bei Auslösung anschließend auch konzeptionell vom SOC-Analysten verstanden werden. Hierdurch entstehen Zeitverzögerungen und mehrere Problemstellen, welche die Nichterkennung von Bedrohungen zur Folge haben können. Der Vorteil einer Cloud-SIEM-Lösung besteht darin, dass der Anbieter die Erkennungsverfahren kontinuierlich aktualisiert und die Lösung so mit der Weiterentwicklung des Angreiferverhaltens Schritt halten kann. Es entstehen keine Zeitverzögerungen und es müssen auf Ihrer Seite keine zusätzlichen Maßnahmen für die Aktualisierung der Software ergriffen werden.

Wie entwickeln sich die Erkennungsfunktionen von SIEM-Lösungen in Reaktion auf neue Bedrohungen weiter? Bei monolithischen Legacy-SIEM-Lösungen müssen neue Erkennungsverfahren vom Anbieter erstellt, in der On-Premise-SIEM-Lösung bereitgestellt, vom Analystenteam möglicherweise aktiviert, mit relevanten Daten abgeglichen und bei Auslösung anschließend auch konzeptionell vom SOC-Analysten verstanden werden. Hierdurch entstehen Zeitverzögerungen und mehrere Problemstellen, welche die Nichterkennung von Bedrohungen zur Folge haben können. Der Vorteil einer Cloud-SIEM-Lösung besteht darin, dass der Anbieter die Erkennungsverfahren kontinuierlich aktualisiert und die Lösung so mit der Weiterentwicklung des Angreiferverhaltens Schritt halten kann. Es entstehen keine Zeitverzögerungen und es müssen auf Ihrer Seite keine zusätzlichen Maßnahmen für die Aktualisierung der Software ergriffen werden.

Liefert die Lösung zuverlässige Alerts und erleichtert sie deren Prüfung? Anstatt einer Unmenge von Fehlalarmen liefern SIEM-Lösungen, die zuverlässige Alerts generieren, eine geringe Anzahl echter Positivmeldungen, auf die Sie unmittelbar mit Maßnahmen reagieren können. Um festzustellen, ob die Lösung dies leistet, fragen Sie den Anbieter, wie die Erkennungsverfahren abgestimmt sind und wie Fehlalarme unterdrückt werden. Stellen Sie gleichzeitig sicher, dass es möglich ist, vordefinierte SIEM-Analysen für Ihre Umgebung anzupassen. Sie können den SIEM-Anbieter dazu beispielsweise um einen Proof of Concept bitten und eine Angriffssimulation durchführen, um die Erkennungsverfahren der Lösung zu testen.

Wie können die Untersuchungsfunktionen der SIEM-Lösung die Effizienz meiner Analysten steigern? Halten Sie Ausschau nach einfachen Pivot-Tabellen für Log- und Endpunktdaten, unkomplizierten Integrationen in Ihre bestehenden Workflows (z. B. Ticketing- oder Chat-Systeme), sowie nach Eindämmungs- und Orchestrierungsfunktionen, damit Sie direkte Maßnahmen zur Eindämmung von Bedrohungen ergreifen oder forensische Daten zu einer Bedrohung erhalten können.

Spielen Sie mit dem Gedanken, eine eigene SIEM-Lösung zu entwickeln?

Einige Unternehmen entscheiden sich dazu, eine eigene SIEM-Lösung für die Analyse von Log-Daten auf der Basis von Open-Source-Tools zu entwickeln. Obwohl Open-Source-Software im Grunde genommen kostenlos ist, können die anfänglichen und laufenden Investitionskosten in die Entwicklung und Wartung einer unternehmensinternen SIEM-Lösung auf Open-Source-Basis erheblich sein und beträchtliche technische Belastungen und Risiken nach sich ziehen.

Bevor Sie sich jedoch zu einer Do-it-yourself-Lösung entschließen, sollten Sie sich fragen, ob es sich lohnt, die Ressourcen Ihres Teams für die Entwicklung einer Lösung einzusetzen, die wahrscheinlich nicht über alle Funktionen verfügt, die Sie eigentlich benötigen.

[3] Das MITRE ATT&CK Framework (Adversarial Tactics, Techniques and Common Knowledge, ATT&CK™) ist eine kuratierte Wissensdatenbank sowie ein Modell für das Verhalten von Cyberangreifern, das die verschiedenen Lifecycle-Phasen von Cyberangreifern sowie die Plattformen wiedergibt, die diese üblicherweise angreifen. Weitere Informationen zu diesem Thema finden Sie auf der folgenden Website: https://attack.mitre.org/wiki/Main_Page.

Abwehrmaßnahmen über den gesamten Incident Lifecycle

Damit Sie Ihre gewählte SIEM-Lösung maximal ausschöpfen können, sollte sich die Lösung an Ihre bestehenden Prozesse anpassen lassen und die Ergreifung von Gegenmaßnahmen mittels einer Sicherheitsorchestrierung und -automatisierung (SOAR oder SAO) beschleunigen. Ihre Prozesse sind von Ihren jeweiligen Anwendungsfällen abhängig, wobei für die Bedrohungserkennung andere Prozesse als für die Compliance-Berichterstattung erforderlich sind.

Sehen wir uns hierzu beispielsweise die einzelnen Phasen des Incident-Response-Prozesses laut Definition des SANS Institute an:

Vorbereitung

In dieser Phase bereiten Sie Ihr Team darauf vor, unmittelbar Incidents zu bearbeiten. Sie umfasst alles vom Festlegen der Richtlinien und Verfahren bis zur Ausstattung Ihres Teams mit den Tools, die es für die Ergreifung von Gegenmaßnahmen für Bedrohungen benötigt, u. a. mit einer SIEM-Lösung.

FRAGEN SIE SICH:: Bietet die SIEM-Lösung vollständige Transparenz der IT-Umgebung (mit Kontext zu Schwachstellen und den Endpunkten)?

Identifikation

Handelt es sich tatsächlich um einen Incident? In dieser Phase geht es um die Identifizierung und Beurteilung potentieller Bedrohungen. Eine zuverlässige Warnmeldung durch die SIEM-Lösung könnte das erste Anzeichen eines gerade auftretenden Incident sein.

FRAGEN SIE SICH: Kann Sie die SIEM-Lösung bei der Erkennung der wahrscheinlichsten Bedrohungen unterstützen, mit denen Ihr Unternehmen konfrontiert sein wird? Und verwendet die Lösung dazu eine Kombination aus vordefinierten Erkennungsverfahren und einer Funktion für die Anpassung und Erstellung von benutzerdefinierten Regeln?

Eindämmung

In dieser Phase setzen Sie alles daran, den durch eine Bedrohung verursachten Schaden zu begrenzen und weiteren Schaden abzuwenden. Eine SIEM-Lösung kann Ihnen dabei helfen, schnell das Ausmaß des Incidents zu erfassen und zu bestätigen, dass die Gegenmaßnahmen zur Eindämmung erfolgreich waren.

FRAGEN SIE SICH: Können Sie Bedrohungen nach deren Identifizierung direkt in der SIEM-Lösung eindämmen?

Eliminierung

Hier liegt das Hauptaugenmerk auf der Entfernung der Bedrohung. Eine SIEM-Lösung kann Ihnen dabei helfen, die ordnungsgemäße Eliminierung einer Bedrohung von den betroffenen Systemen zu bestätigen.

FRAGEN SIE SICH: Stellt die SIEM-Lösung Untersuchungs-Workflows, ein Fallmanagement, sowie Integrationen in IT-Service-Tools bereit, damit Ihr Team auf der Grundlage derselben Informationen zusammenarbeiten kann und Einsicht darin erhält wer welche Aufgabe hat?

Wiederherstellung

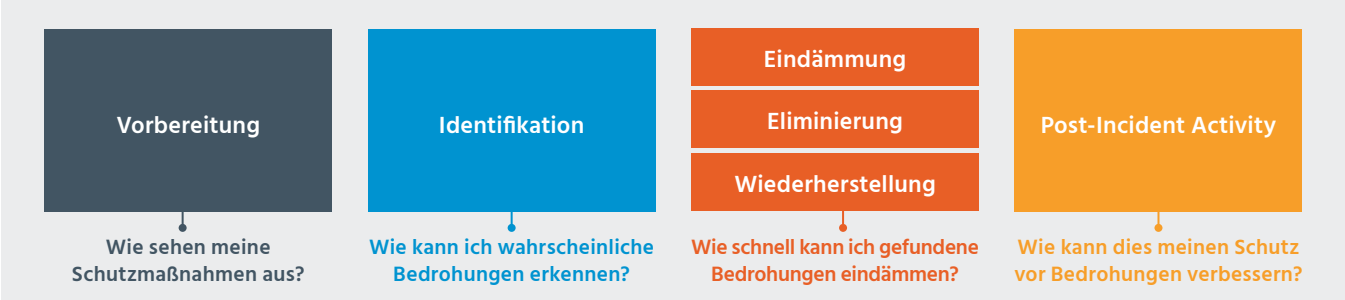
Sobald die Systeme wieder im Einsatz sind, können Sie diese mit einer SIEM-Lösung überwachen und sicherstellen, dass diese nicht erneut infiziert oder gefährdet werden.

FRAGEN SIE SICH: Kann die SIEM-Lösung „normales" Benutzerverhalten erkennen, wenn Bezugswerte für typische Komponenten- und Benutzeraktivitäten in Ihrer Umgebung festgelegt werden?

Post-Incident Activity/Lessons Learned

Ist der Incident vorüber, ist es an der Zeit, Lehren für die Optimierung des Incident Response-Verhaltens Ihres Teams zu ziehen und den Incident zu Referenzzwecken zu dokumentieren. Ihre SIEM-Lösung sollte die Feinabstimmung unterstützen, damit Sie die im Zusammenhang mit dem Incident gewonnenen Erkenntnisse zur Verbesserung Ihrer Sicherheitslage nutzen können.

FRAGEN SIE SICH: Steht in der SIEM-Lösung die Möglichkeit zur Verfügung, bei den Untersuchungen gesammelte Bedrohungsinformationen hinzuzufügen, um künftige Erkennungsbemühungen zu unterstützen?



Incident-Response-Prozess

Quelle: SANS Institute, the Incident Handler's Handbook

04 Managed Detection and Response

Ein Unternehmen mit unbegrenzten Sicherheitsressourcen und ohne zeitliche Zwänge oder Budgetvorgaben ist selten (und in der Regel sehr groß). Für beinahe alle anderen sind diesbezügliche Beschränkungen eine beständige Realität. Falls Ihr Unternehmen zu großen Ressourcenzwängen unterliegt, sei es in puncto Mitarbeiter, Budget und/oder Qualifikationen, um eine SIEM-Lösung einzusetzen, stellt ein Managed Service eventuell die beste Alternative dar.

Anders als ein Managed Security Service Provider (MSSP), der die Netzwerksicherheitsmaßnahmen überwacht und Sie benachrichtigt, sobald Unregelmäßigkeiten festgestellt werden, aber keine Untersuchung von Bedrohungen durchführt und auch keine Gegenmaßnahmen ergreift, fungiert ein MDR-Service (Managed Detection and Response) als Erweiterung Ihres Sicherheitsteams und führt rund um die Uhr Erkennungs- sowie Gegenmaßnahmen durch. Der MDR-Service basiert auf einem schlüsselfertigen Ansatz und unterstützt Ihr Team bei der Erkennung und Behebung von Bedrohungen, insbesondere von gezielten, hochentwickelten Bedrohungen und internen Bedrohungen.

Falls es Ihrem Unternehmen an den Ressourcen oder den Kompetenzen für die Unterstützung aller gewünschten SIEM-Anwendungsfälle mangelt, sollten Sie einen MDR-Service in Betracht ziehen. Dieser bietet Ihnen eine Kombination aus zentralisiertem Log-Management und durchgängiger Überwachung durch einen erfahrenen Sicherheitspartner.

FRAGEN SIE DEN LÖSUNGSANBIETER:

Verwendet der MDR-Service Benutzerverhaltensanalysen? Die Benutzerverhaltensanalyse stellt die einzige verlässliche Methode dar, um die Verwendung von gestohlenen Zugangsdaten sowie Bedrohungen von innen zu erkennen.

Verfügt der MDR-Service über eine Threat-Hunting-Methode? Durch die Kombination von mehrstufigen Analysen und Threat Hunting können die in Ihrem Auftrag tätigen Sicherheitsexperten unbekannte Bedrohungen und Incidents schneller identifizieren.

Stellt der MDR-Service rund um die Uhr an allen Wochentagen im gesamten Jahr Unterstützung bereit? Bei einem Sicherheits-Incident müssen Sie sich darauf verlassen können, dass der Anbieter die entsprechende technische Sicherheitskompetenz bereitstellt und geeignete Gegenmaßnahmen veranlasst. Während Sie mit der Incident Response und Behebung beschäftigt sind, ist kontinuierlicher Kontakt mit Ihrem Team besonders wichtig.

05 Bereitstellen einer SIEM-Lösung mit schneller Time-to-Value

Herkömmliche SIEM-Lösungen haben aufgrund der ihnen innewohnenden Komplexität in der Vergangenheit sehr häufig zum Scheitern von SIEM-Projekten geführt. Eine neue Generation von SIEM-Lösungen schickt sich an, dies zu ändern. Rapid7 InsightIDR ist intuitiv, benutzerfreundlich, schnell zu implementieren, immer auf dem aktuellen Stand und anpassbar.

Es handelt sich dabei um eine Cloud-Lösung, die Sie dabei unterstützen soll, Bedrohungen schnellstmöglich zu erkennen und zu beheben. Die Kunden können die Lösung nicht nur innerhalb weniger Stunden bereitstellen, sondern erhalten durch die Implementierung unmittelbaren Mehrwert, da gefährliche Fehlkonfigurationen und Benutzeraktivitäten aufgedeckt werden.

So unterstützt Sie die Insight-Plattform von Rapid7 im Verlauf des Incident Response-Lifecycles:

- **Angreiferverhaltensanalyse:** InsightIDR verfügt über eine integrierte Bedrohungsanalyse (für die Erkennung von Verhaltensweisen, nicht von statischen Indikatoren). Die Analysefunktion wird von unseren weltweiten Security Operations Centern (SOC), sowie vom Team für die Bedrohungsanalyse gepflegt, sodass Sie neu auftretenden Bedrohungen jederzeit einen Schritt voraus bleiben – ohne dass Sie hierzu selbst Maßnahmen ergreifen müssen.
- **Eindämmung:** Sie können Bedrohungen nicht nur erkennen, sondern auch direkte Maßnahmen ergreifen, um die Ausbreitung einer Bedrohung zu verhindern. Dies umfasst das Management vorhandener EDR-Tools zum Beenden von Prozessen oder Isolieren von Komponenten (Quarantäne). In InsightIDR haben Sie zudem die Möglichkeit, Maßnahmen für Verzeichnisdienste, für Firewalls, sowie für Tools zur Netzwerkzugriffssteuerung zu ergreifen.
- **Fachkompetenz:** Rapid7-Analysten stehen rund um die Uhr an sieben Tagen in der Woche mit dem Service für Managed Detection and Response zur Überwachung Ihres Netzwerks zur Verfügung. Außerdem bieten sie die Entwicklung von Incident-Response-Plänen, die Angriffssimulation, sowie Incident Response Retainer an, damit Sie Bedrohungen entschieden begegnen können. Managed Detection and Response von Rapid7 stellt eine Erweiterung Ihres Sicherheitsteams dar und kombiniert die InsightIDR-Technologie, sowie proprietäre Tools mit einer Echtzeit-Bedrohungsanalyse und Analysten der Spitzenklasse, sodass eine Überwachung Ihres Netzwerks rund um die Uhr gewährleistet ist. Das Beste daran: Das Fachwissen und die Erkenntnisse der Analysten fließen direkt in InsightIDR ein. Auf diese Weise profitieren alle Rapid7-Kunden davon.

Kundenstimmen

„Splunk und ähnliche Lösungen erfassen lediglich die Logs. Aber ich möchte wissen, ob etwas Seltsames oder Ungewöhnliches vor sich geht. Und genau darüber werde ich von InsightIDR informiert. Das war die beste Lösung mit genau den Analysefunktionen, die ich benötige. Das alles zu einem angemessenen Preis."

– Benjamin Nawrath, Energie Südbayern Fallstudie lesen >

„[InsightIDR] hat sich leicht implementieren lassen und war von Anfang an ein echter Gewinn für das Unternehmen. Mit nur einer Lösung haben wir nun volle Transparenz und können beinahe alle Komponenten unseres Netzwerks überwachen."

– IT-System-und Sicherheitsadministrator, über Gartner Peer Insights Bewertung lesen >

„Was ich an InsightIDR besonders schätze, ist die Tatsache, dass die Funktionen zur Kombination eines rein reaktiven Incident-Management-Ansatzes mit einem proaktiven Threat-Hunting-Ansatz bereits in das Tool integriert sind."

– Christopher Calvert, Visier Kundenstatement ansehen >

Nächste Schritte

Die Wahl der richtigen SIEM-Lösung ist für die Sicherheit Ihres Unternehmens bzw. Ihrer Organisation wichtiger denn je. Lassen Sie sich bei der Wahl der Lösung von Ihren Anwendungsfällen, den Qualifikationen Ihrer Teams, Ressourcenbeschränkungen und Ihrer Risikoexposition leiten, um nachhaltig und skalierbar für Erfolg zu sorgen.

Um mehr darüber zu erfahren, ob InsightIDR von Rapid7 die SIEM-Lösung sein kann, nach der Sie gesucht haben, oder um eine **kostenlose 30-Tage-Testversionl**,

Website: **rapid7.com/insightidr**

Sie suchen Unterstützung bei der Überwachung und beim Threat Hunting **rund um die Uhr an allen Wochentagen im gesamten Jahr?** Dann beauftragen Sie doch unser Managed Detection and Response-Team als Ihren persönlichen Cybersecurity-Partner. Weitere Informationen finden Sie auf der folgenden

Website: **rapid7.com/MDR**

Über RAPID7

Rapid7 unterstützt Ihre SecOps durch allgemeine Transparenz, Analyse und Automatisierung für alle Sicherheits-, IT- und Entwicklungsteams. Die Plattform Rapid7 Insight ermöglicht es diesen Teams, gemeinsam Risiken zu beheben und zu verringern, Angreifer zu erkennen und unschädlich zu machen, sowie die Abläufe zu analysieren und zu optimieren. Mit seinen Technologien und Services, sowie seiner Forschungstätigkeit treibt Rapid7 die Entwicklung in puncto Schwachstellen-Management, Anwendungssicherheit, Incident Detection and Response (SIEM), Orchestrierung und Automatisierung, sowie Log Management für mehr als 7.100 Unternehmen in mehr als 120 Ländern voran, von denen 55 % zu den Fortune 100 zählen.

Weitere Informationen zu Rapid7 finden Sie auf der Website von Rapid7 unter

unter www.rapid7.com.