Bericht über den Stand von SOAR 2020

Die vierte jährliche Umfrage zur Behebung von Sicherheitsverstößen

Inhalt

Kurzfassung

Dies ist der vierte Jahresbericht zum aktuellen Stand von SOAR. Wie in den vergangenen Jahren haben wir wieder Hunderte Sicherheitsfachleute befragt, die verschiedene Positionen in großen Unternehmen unterschiedlicher Branchen innehaben. Dieses Jahr standen das Incident-Response-Management (IR) und die aktuelle oder geplante Nutzung von SOAR (Security Orchestration, Automation, and Response) im Rahmen ihrer Sicherheitsstrategie im Mittelpunkt.

Einige Highlights aus dem Bericht:

- **Die Cyberbedrohungen werden immer gravierender**. Die Angreifer verfolgen unterschiedliche Taktiken und ihre Kampagnen nehmen immer größere Ausmaße an. 63 Prozent der Befragten mussten unter anderem Angriffe seitens mutmaßlich staatlicher Akteure abwehren.
- **Die IR-Prozesse sind äußerst aufwendig**. Analysten müssen im Durchschnitt 6,8 Bedrohungsdatenfeeds verfolgen und zahllose Warnmeldungen manuell bearbeiten. Für die IR-Prozesse wird eine Vielzahl von Systemen genutzt, was zu einem abteilungsübergreifenden Workflow führt.
- **Die COVID-19-Pandemie hat die Lage zusätzlich verschärft**. Sie bringt neue Herausforderungen und Bedrohungen mit sich und erschwert die Zusammenarbeit der SOC-Teammitglieder. 40 Prozent der Umfrageteilnehmer sind der Ansicht, dass die Pandemie zu Ressourcenknappheit geführt oder diese verschärft hat.
- **Die Analysten wissen, was sie zur Verbesserung des Incident-Response-Managements benötigen**. Sie wünschen sich Folgendes:
  - » Ausweitung der Automatisierung zur Beschleunigung der IR-Prozesse und Reduzierung der manuellen Aufgaben. 65 Prozent der Befragten werden die IR-Automatisierung innerhalb der nächsten 12 Monate priorisieren.
  - » Integration der SOC-Tools in Drittanbietersysteme, damit problemlos Verbindungen zu anderen Abteilungen und IR-Prozessen hergestellt werden können. 30 Prozent der Umfrageteilnehmer wünschen sich eine einheitliche Plattform für abteilungsübergreifende Prozesse.
  - » Mehr Playbooks, einschließlich Playbooks von Drittanbietern und eine Community für den Informationsaustausch, um aus den Erfahrungen anderer Teams zu lernen. 78 Prozent der Befragten wünschen sich ein einheitliches Framework und eine Community zum Austausch von Informationen, Integrationen und Playbooks.
  - » Integration von Bedrohungsdaten in SecOps-Tools, um die Überwachung zahlreicher Feeds zu vereinfachen und sicherzustellen, dass keine gravierenden Bedrohungen übersehen werden. 52 Prozent der Umfrageteilnehmer glauben, dass ihre Sicherheits-Workflows durch die Integration von Bedrohungsdaten verbessert werden könnten.
- **SOC-Teams müssen die Warnungsmüdigkeit bekämpfen**. Sie benötigen ein Tool, das entweder die Zahl der Warnmeldungen reduziert oder deren Bearbeitung beschleunigt.
- **SOAR-Lösungen können bei vielen dieser Herausforderungen helfen**. Damit können SOC-Teams Zeit sparen, die Ersteinschätzung beschleunigen und die Zahl der Schritte in IR-Prozessen reduzieren.
  - » 45 Prozent der SOC-Teams nutzen SOAR für die Bedrohungserkennung und -abwehr. Zu den weiteren Anwendungsbereichen gehören die Priorisierung von Sicherheitslücken (37 %), Complianceprüfungen (30 %) und Sicherheitsaudits (30 %).
  - » In Zukunft möchten SOC-Teams SOAR-Lösungen auch für das IoT-Management (23 %), Red-Team-Workflows (17 %) und die Cloud-Sicherheit (38 %) einsetzen.
  - » 43 Prozent der Umfrageteilnehmer wollten 2020 mehr in SOAR-Tools investieren. Weitere 24 Prozent haben die Implementierung von SOAR-Lösungen innerhalb der nächsten 12 Monate geplant.
  - » Aufgrund der COVID-19-Pandemie haben 47 Prozent der Befragten ihre SOAR-Nutzung ausgeweitet.

Einführung

In diesem Bericht werden die Ergebnisse einer jährlichen Umfrage unter Sicherheitsfachleuten zusammengefasst und damit auch die Trends im Incident-Response-Management und potenzielle Anwendungsbereiche für SOAR-Technologie (Security Orchestration, Automation, and Response) bei den IR-Prozessen aufgezeigt. Die Umfrageteilnehmer sind bei großen Unternehmen verschiedener Branchen beschäftigt und bekleiden diverse Positionen mit Verantwortung für die Sicherheit.

Die Security Operations Center (SOC) und die Sicherheitsanalysten benötigen Unterstützung. Die SOC-Teams stehen ständig unter Druck und müssen eine Vielzahl an verschiedenen Angriffen abwehren (siehe Abbildung 1). 86 Prozent der Befragten gaben an, dass sie innerhalb der letzten 12 Monate Phishing-Angriffe abwehren mussten. Weitere 63 Prozent mussten Malware-Angriffe identifizieren und möglichst schnell neutralisieren. Passwortangriffe, DoS-Angriffe (Denial of Service) und Ransomware traten bei jeweils 51, 39 und 37 Prozent der Befragten auf.

Gartner stellte im Bericht „Top Security and Risk Management Trends“ 2020 fest: „Die Frequenz und die Kreativität der Angriffe nehmen zu. Die Hacker werden weiterhin ein breites Spektrum an Tools, Taktiken und Techniken für sich nutzen, um auf immer breiterer Front zum Erfolg zu kommen. All dies erschwert die Voraussage und die Vermeidung von Sicherheitsvorfällen.“[1]

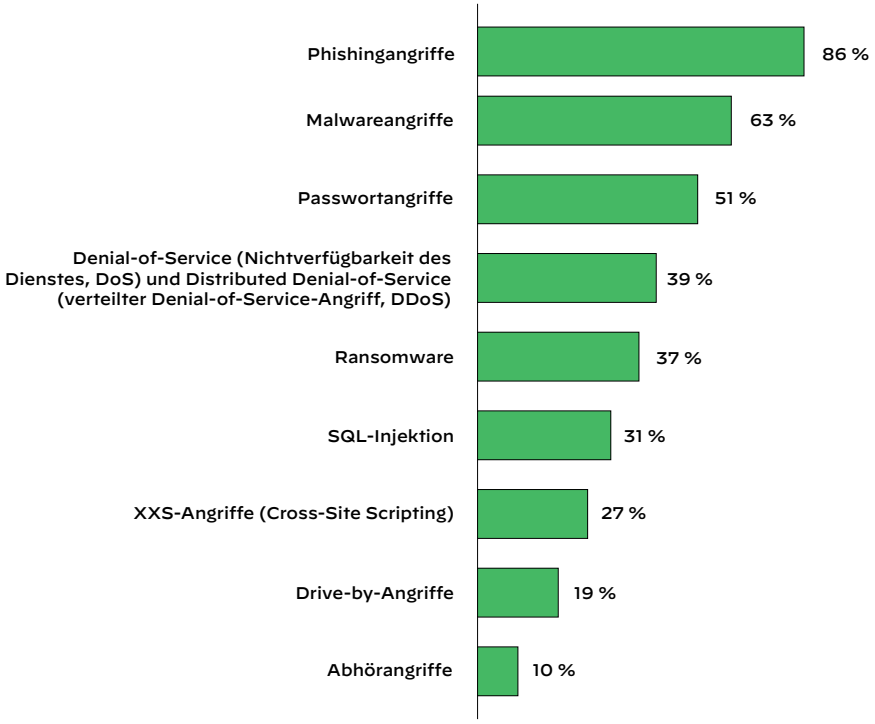

Abbildung 1: Angriffe auf die Unternehmen der Umfrageteilnehmer innerhalb der letzten 12 Monate

Bemerkenswert ist, dass 63 Prozent der Umfrageteilnehmer eigenen Angaben zufolge innerhalb der letzten 12 Monate mindestens einen Cyberangriff erlebt hatten, der vermutlich von einer staatlich gesponserten Hackergruppe durchgeführt wurde. Zu den Taktiken dieser Angreifer gehören unter anderem Phishing, DDoS, Ransomware und SQL-Injektion. Die Coronakrise verschärft die Situation zusätzlich (mehr dazu im Abschnitt „Die Auswirkungen der COVID-19-Pandemie auf das IR-Management“).

Überblick über SOAR

SOAR ist eine Kategorie von Sicherheitstechnologie, mit der SOC-Teams die IR-Prozesse effizienter und effektiver verwalten können. SOAR-Lösungen wurden bei dem Versuch entwickelt, IR-Workflows zu automatisieren, denn diese werden immer noch überwiegend manuell ausgeführt. Zudem soll die Technologie SOC-Analysten bei der Orchestrierung der IR-Prozesse zwischen mehreren Systemen helfen, beispielsweise SIEM-Lösungen (Security Incident and Event Management) und Plattformen für das Fallmanagement.

SOAR-Lösungen ermöglichen ein schnelleres und effektiveres IR-Management, stellen detaillierte, praxistaugliche forensische Daten zu Vorfällen bereit und bieten SOC-Teams einige grundlegende Funktionen:

- **Die Orchestrierung** ermöglicht die Verknüpfung von Funktionen in verschiedenen Systemen, um die Ziele des IR-Workflows zu erreichen. Dazu werden in der Regel Standard-APIs (Application Programming Interfaces) verwendet, sodass SOAR-Lösungen beispielsweise Funktionen auf anderen Systemen nutzen können, um Benachrichtigungs-E-Mails zu versenden, Bedrohungen zu suchen und Tickets zu erstellen.
- **Automatisierung** bedeutet unter anderem, Geräte so zu konfigurieren, dass sie Aufgaben ausführen, die bisher manuell erledigt werden mussten. Bei SOAR wird die Automatisierung weitgehend zur Unterstützung der Mitarbeiter eingesetzt, nicht um diese zu ersetzen. Sie entlastet SOC-Analysten von vielen repetitiven und langweiligen Aufgaben und beschleunigt das IR-Management und die Vorfallsuntersuchungen.
- **Playbooks** sind vorab festgelegte Ablaufskripte, die das SOC-Team in die SOAR-Lösung integrieren kann, um bestimmte Bedrohungen abzuwehren. Wenn das Team beispielsweise eine bekannte CVE-Bedrohung (Common Vulnerabilities and Exposures) identifiziert und über ein Playbook für diesen Fall verfügt, kann es die darin beschriebenen Abwehrmaßnahmen umgehend einleiten und muss nicht erst selbst eine geeignete Reaktion erfinden. Dadurch wird der IR-Prozess wesentlich schneller und effizienter.
- **Die Berichterstellung und Datenvisualisierung** helfen dem SOC-Team, Vorfälle intuitiv und effizient zu identifizieren, zu korrelieren und zu priorisieren. Außerdem können der Verlauf, die einzelnen Schritte des IR-Prozesses und die Ergebnisse dokumentiert werden.

1. Peter Firstbrook, Neil MacDonald, Lawrence Orans, Mario de Boer, Katell Thielemann, Bart Willemsen, Akif Khan und Michael Kranawetter, „Top Security and Risk Management Trends“ (ID G00466211), Gartner, 27. Februar 2020, https://www.gartner.com/en/documents/3981492/top-security-and-risk-management-trends.

IR: ein Zusammenspiel von Personen, Prozessen, Tools und Daten

Jedes der befragten Unternehmen hat seinen eigenen IR-Workflow. Die meisten dieser Prozess bestehen jedoch aus den folgenden vier Phasen:

- **Import und Anreicherung von Vorfallsdaten**: Bei diesem Prozess sammelt das SOC detaillierte Informationen zu dem Sicherheitsvorfall und reichert sie mit weiteren Daten an, um die Abläufe besser nachvollziehen zu können. Wenn sich ein Angriff beispielsweise auf eine bestimmte CVE zurückführen lässt, können bei der Anreicherung unter anderem Details zu der CVE, den betroffenen Systemen und möglichen Abwehrmaßnahmen hinzugefügt werden.
- **Fallmanagement**: Jeder Sicherheitsvorfall wird vom SOC als Fall behandelt (oder sollte zumindest als solcher betrachtet werden). Zur Bearbeitung muss das SOC mitunter andere Mitarbeiter im Unternehmen hinzuziehen, zum Beispiel das IT- und Netzwerkteam, die Rechtsabteilung oder die Personalabteilung.
- **Vorfallsuntersuchung**: Sicherheitsanalysten müssen Vorfälle genau untersuchen, um die beste Abwehrmaßnahme zu finden und ähnliche Ereignisse in Zukunft zu vermeiden. Für diese Untersuchungen sind einerseits Fachkenntnisse und Erfahrung gefragt, andererseits sind die Experten aber auch auf Systeme angewiesen, die die erforderlichen Details zur Ursache liefern.
- **Abwehrmaßnahmen und Richtliniendurchsetzung**: In dieser Phase werden die bei der Untersuchung ausgewählten Abwehrmaßnahmen umgesetzt.

Die verschiedenen Phasen ergänzen und überlappen einander. Die Datenanreicherung hilft bei der Untersuchung und diese wiederum erleichtert die Wahl der geeigneten Abwehrmaßnahmen. Mit Tools und Richtlinien für das Fallmanagement werden die Workflows strukturiert und stets alle relevanten Stakeholder informiert – so lautet zumindest die Theorie.

Die Auswirkungen der COVID-19-Pandemie auf das IR-Management

60 Prozent der Umfrageteilnehmer gaben an, dass sie aufgrund der Pandemie neue Arbeitsmodelle einführen mussten, zum Beispiel auch das Homeoffice für Mitarbeiter und Mitglieder des SOC-Teams. 42 Prozent haben das Gefühl, dass die virtuelle Zusammenarbeit durch die Pandemie an Bedeutung gewonnen hat, aber 40 Prozent sind der Ansicht, dass dies zu Ressourcenknappheit geführt oder diese verschärft hat. Das ist vielleicht auch der Grund, warum 24 Prozent angeben, dass der Bedarf an Automatisierung in der Coronakrise zugenommen hat, und 23 Prozent aufgrund der Pandemie neue Cloud-Services eingeführt haben.

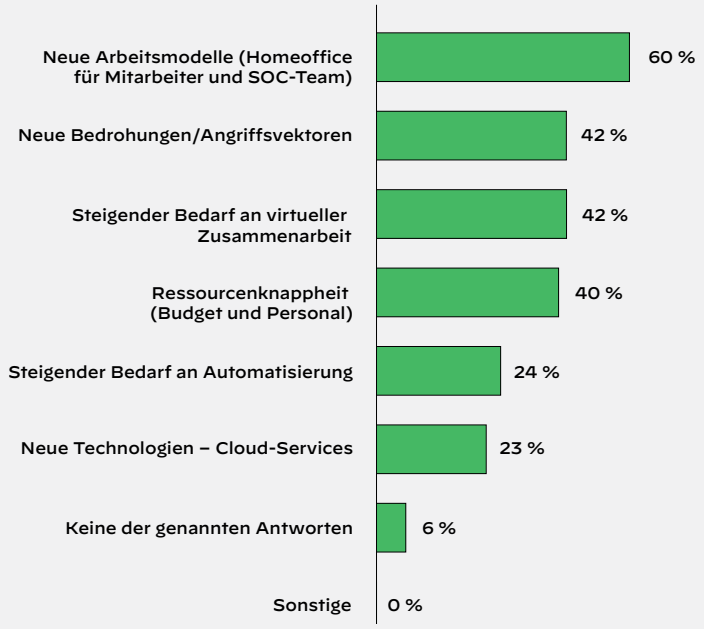

Abbildung 2: Umfrageergebnisse zu den Auswirkungen der COVID-19-Pandemie auf die SOC-Teams und Sicherheitsanalysten

Auch der Sicherheitsstatus und die Sicherheitsmaßnahmen sind davon betroffen. 42 Prozent der Befragten gaben an, dass während der Pandemie neue Bedrohungen und Angriffsvektoren aufgetreten sind. Bei der SOAR-Einführung sind die Meinungen geteilt: 47 Prozent der Befragten, in deren Unternehmen SOAR bereits teilweise genutzt wurde, gaben an, dass sie die Nutzung aufgrund der Pandemie ausweiten und die Einführung beschleunigen werden. Ebenso viele haben allerdings das Gegenteil beschlossen: 47 Prozent haben wegen der Pandemie die SOAR-Nutzung reduziert und die Implementierung verzögert.

Wichtigste Ergebnisse aus der SOAR-Umfrage 2020

In der SOAR-Umfrage 2020 haben sich einige Ergebnisse aus den Vorjahren bestätigt. SOC-Teams erhalten nach wie vor mehr Warnmeldungen, als sie bearbeiten können. Die Lage wird zusätzlich durch den Fachkräftemangel verschärft, der auch im Gartner-Bericht „Top Security and Risk Management Trends“ für 2020 thematisiert wird: „Der Fachkräftemangel wird sich weiter zuspitzen, da die IT-Systeme immer komplexer und die Sicherheitstools immer schneller weiterentwickelt werden, um die äußerst dynamischen Infrastrukturen zu schützen.“[2]

Die SOC-Teams wünschen sich eine Ausweitung der Automatisierung, um die Belastung etwas zu verringern. In den Umfrageergebnissen wird auch das Interesse an der Anbindung von Drittanbietersystemen deutlich. Ein weiterer Wunsch der SOC-Teams sind mehr Playbooks und manche würden in diesem Zusammenhang Marktplattformen von Drittanbietern und einen Informationsaustausch in Communitys begrüßen. Die Leute wollen wissen, wie andere Teams die Probleme gelöst haben, vor denen sie jetzt stehen.

Aktuelle IR-Prozesse: immer komplexere und anspruchsvollere Workflows

Jedes Unternehmen entwickelt eigene Verfahren und Tools für das IR-Management. Die Umfrage zeigt, dass die IR-Prozesse in den Unternehmen auf unterschiedlichen Lösungen starten. Wie in Abbildung 3 zu sehen, beginnen mehr als die Hälfte der IR-Workflows in SIEM-Lösungen und 33 Prozent auf Ticketplattformen wie ServiceNow® und Zendesk®. Nur 6 Prozent starten in Tools für das Fallmanagement und lediglich 2 Prozent in SOAR-Lösungen.

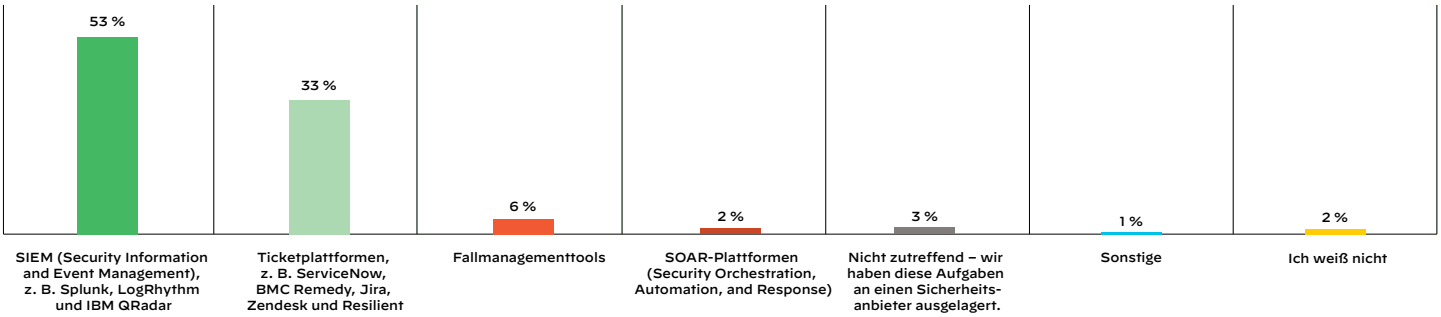

Abbildung 3: „Über welche Lösung starten Sie in der Regel die Incident-Response-Workflows?“

Ein Teil der Aufgaben entfällt auf externe Anbieter und manuelle Prozesse (siehe Abbildung 4). Bei 22 Prozent der IR-Workflows sind Anbieter von Managed Security Services (MSSP) und MDR-Services (Managed Detection and Response) eingebunden. Wenn Arbeit an externe Anbieter ausgelagert wird, lassen sich manuelle Prozesse im IR-Workflow kaum vermeiden. Sofern der MSSP oder MDR-Service nicht mit automatisierten IR-Tools verknüpft ist, muss ein Teil des IR-Managements manuell durchgeführt werden.

Bei der Vorfallsuntersuchung werden 38 Prozent der Prozesse manuell gehandhabt, bei den Abwehr-maßnahmen und der Richt-liniendurchsetzung sind es 35 Prozent. Angesichts der in Abbildung 3 dargestellten Umfrageergebnisse ist der nach wie vor große Anteil manueller Prozesse durchaus verständlich: Wenn 53 Prozent der IR-Workflows in SIEM-Lösungen beginnen, die in der Regel nicht über automatisierte IR-Funktionen verfügen, muss ein SOC-Teammitglied die Fälle in die anderen Tools einpflegen.

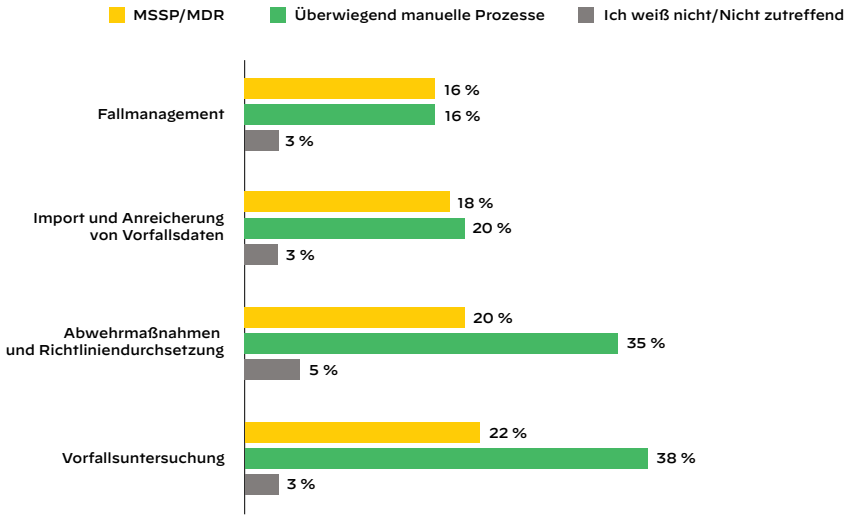

Abbildung 4: „Welche Lösungen verwenden Sie für die folgenden Schritte des Incident-Reponse-Prozesses?“

2. „Top Security and Risk Management Trends“, Gartner, 27. Februar 2020

Zu langsame und nicht skalierbare IR-Prozesse

Laut den Antworten der Umfrageteilnehmer sind die IR-Prozesse zu langsam und nicht skalierbar. Weniger als die Hälfte der Befragten können ihre Dashboards anpassen. Nur 40 Prozent haben Zugriff auf Echtzeit- und geplante Berichte und nur 15 Prozent erhalten Empfehlungen zur Verbesserung der Sicherheitsmaßnahmen von ML-basierten Algorithmen. Aufgrund dieser ineffizienten SecOps-Umgebungen sind alle Abläufe sehr zeitaufwendig. Wenn den SOC-Teams nur Standard-Dashboards zur Verfügung stehen, die eventuell nicht einmal an die spezifische Rolle jedes Analysten angepasst sind und keine Berichte enthalten, kommen sie natürlich langsamer voran. Außerdem sind die Ergebnisse weniger aussagekräftig. Maschinelles Lernen ist eine mögliche Lösung, aber leider (wie in der Abbildung zu sehen) nur in jedem sechsten SOC verfügbar.

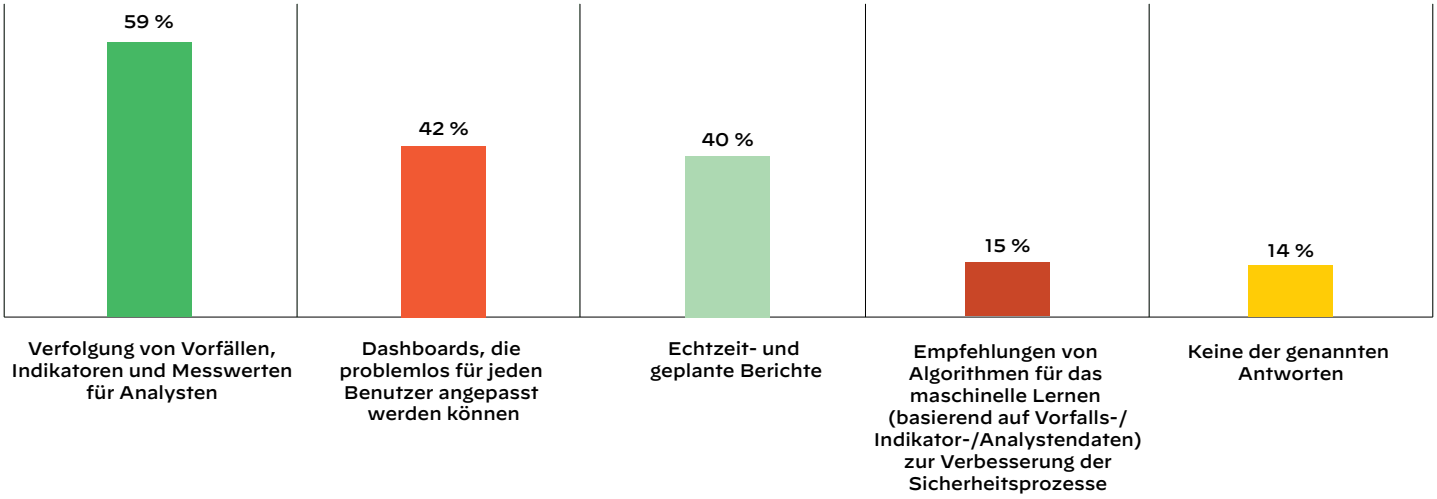

Abbildung 5: „Über welche Mittel für Incident-Response-Maßnahmen und die Verfolgung der Leistung Ihrer Analysten verfügen Sie derzeit? Bitte wählen Sie alle zutreffenden Antworten aus."

Mehr automatisierte Prozesse und Playbooks für das IR-Management

Die Umfrageergebnisse machen deutlich, dass eine stärkere Automatisierung der IR-Prozesse erforderlich ist. Laut den Angaben der Umfrageteilnehmer sind 44,7 Prozent der IR-Prozesse automatisiert. Der Prozentsatz mag hoch erscheinen, aber er reicht nicht aus. Wenn 4 von 10 Prozessen automatisiert sind, ist das zwar besser als nichts, aber die zahlreichen manuellen Abläufe verhindern ein effektives und effizientes IR-Management. Die Zahlen sprechen für sich: 93 Prozent der Sicherheitsteams sagen, dass die Ausweitung der Automatisierung im kommenden Jahr höchste Priorität hat.

Bisher nur teilweise Automatisierung des Imports und der Anreicherung von Vorfallsdaten

Der Import und die Anreicherung von Vorfallsdaten für IR-Prozesse sind nur teilweise automatisiert. Wie in Abbildung 6 zu sehen, ist die Hälfte des Datenimports für mehrere Quellen automatisiert. Bei der Priorisierung von Warnmeldungen und der produktübergreifenden Korrelation von Warnmeldungen und Indikatoren ist der Prozentsatz fast genauso hoch (je 46 Prozent) Doch da die SOC-Teams immer noch stark überlastet sind, reicht es offensichtlich nicht, nur die Hälfte des Workflows zu automatisieren. Bei der Datenanreicherung ist die Zahl deutlich geringer. Nur 28 Prozent der Befragten gaben an, dass sie für diesen Zweck automatisierte Prozesse nutzen. Weitere 30 Prozent reichern die Daten manuell an.

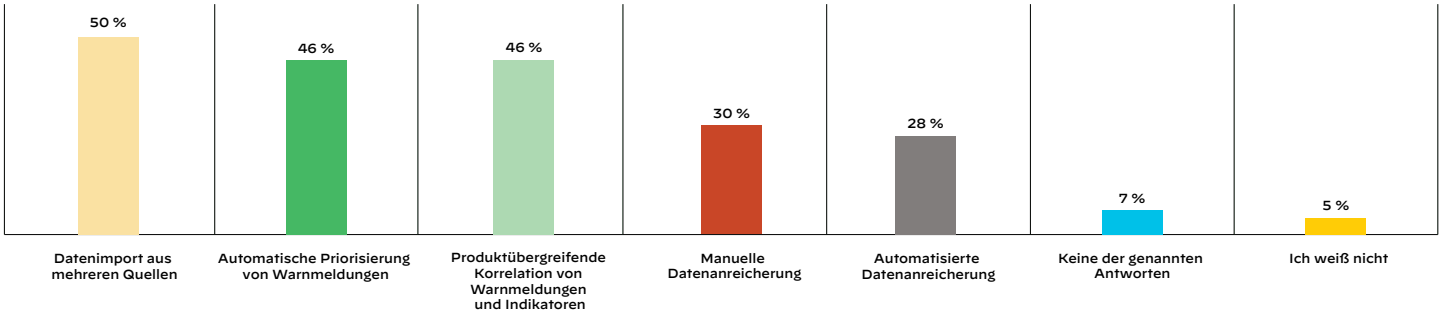

Abbildung 6: „Welche Möglichkeiten stehen Ihnen für den Import und die Anreicherung von Vorfallsdaten derzeit zur Verfügung? Bitte wählen Sie alle zutreffenden Antworten aus."

Implementierung von IR-Prozessen: eine Kombination aus automatisierten und manuellen Workflows

Auch bei der Implementierung von IR-Prozessen werden verschiedene Maßnahmen kombiniert. Bei 53 Prozent der Unternehmen kommt eine Kombination aus manuellen und automatisierten Playbooks, Runbooks und Prozessen zum Einsatz (siehe Abbildung 7). Nur 18 Prozent verwenden automatisierte Playbooks und Runbooks. Auffällig ist, dass lediglich 6 Prozent ganz ohne Playbooks auskommen. Die meisten SOC-Teams nutzen Playbooks für die Implementierung von IR-Prozessen – und der Automatisierungsgrad ist nicht sehr hoch.

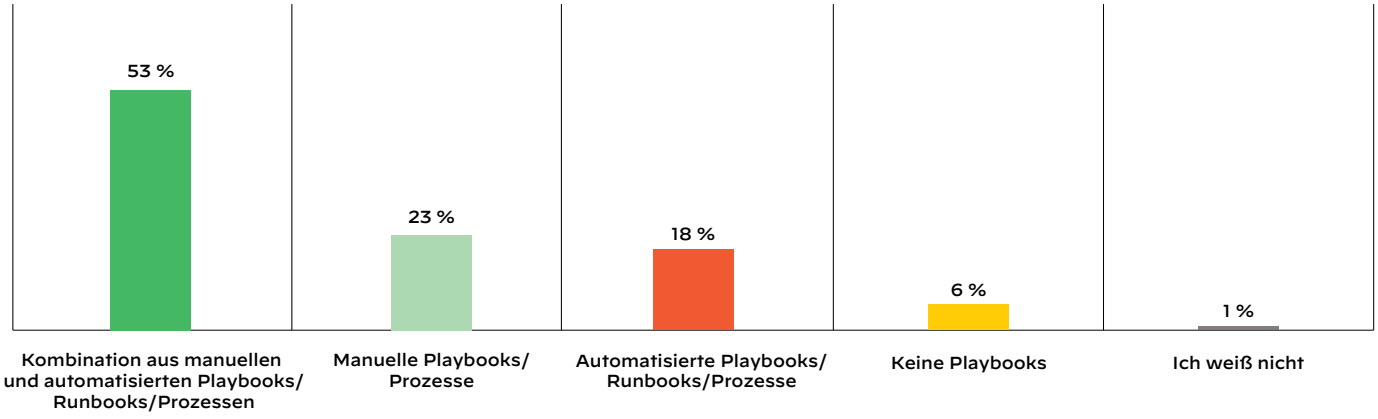

Abbildung 7: „Welche der folgenden Aussagen beschreibt Ihre Incident-Response-Prozesse am besten?“

Begrenzte Automatisierung der Workflows für die Untersuchung und die Aufarbeitung eines Sicherheitsvorfalls

Die Untersuchungsphase des IR-Prozesses ist teilweise automatisiert. Bei den per Fernzugriff genutzten Sicherheitstools werden 37 Prozent der Einsätze automatisch gesteuert, 49 Prozent hingegen manuell. Bemerkenswert ist, dass nur bei 18 Prozent der IR-Workflows die Untersuchungsschritte automatisch dokumentiert werden. Das würde bedeuten, dass mehr als 80 Prozent der Aktivitäten bei der Vorfallsuntersuchung manuell – oder gar nicht – dokumentiert werden.

SOC-Teams haben in der Regel keine Zeit, jeden einzelnen Schritt festzuhalten. Doch diese Informationen sind äußerst hilfreich, wenn später Analysen durchgeführt und Verbesserungen zur Vorbereitung auf den nächsten Vorfall vorgenommen werden sollen. Durch ihre minimale Automatisierung vergeben viele Unternehmen die Chance, aus Vorfällen zu lernen und die Prozesse zu verbessern. Auch bei den Workflows für die Aufarbeitung eines Sicherheitsvorfalls gaben nur 23 Prozent der Befragten an, dass die einzelnen Schritte automatisch erfasst werden.

Automatisierung hat im IR-Management zukünftig höchste Priorität

Die Prioritäten und Zukunftspläne sind sehr aufschlussreich. Bei 65 Prozent der Befragten hat die IR-Automatisierung im kommenden Jahr hohe Priorität (siehe Abbildung 8). Für 58 Prozent hat die automatisierte Priorisierung von Warnmeldungen eine hohe Priorität. Für 46 Prozent trifft dies auf die Automatisierung der Berichterstellung und eine größere Transparenz in den Teams zu. Nur wenige gaben an, dass die Automatisierung nicht zu ihren Prioritäten gehört. Bei dem IR-Management waren es lediglich 2 Prozent.

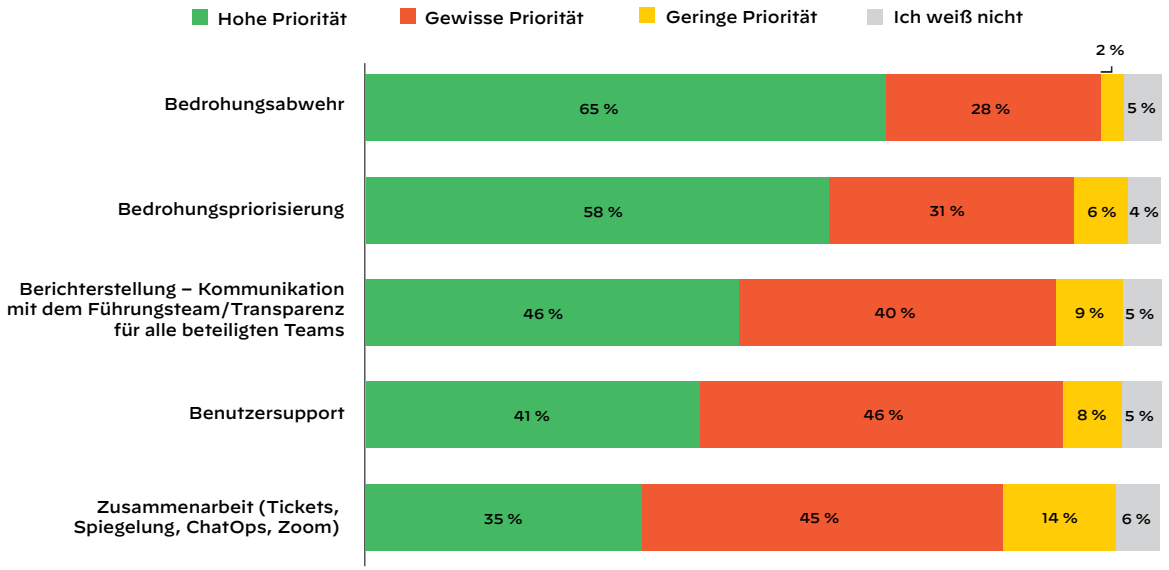

Abbildung 8: „Welche Priorität hat die Ausweitung der Automatisierung für die folgenden Sicherheitsprozesse innerhalb der nächsten 12 Monate?“

Einfachere Verwaltung von Bedrohungsdaten und bessere Integration in IR-Workflows

Da die globale Bedrohungslage immer komplexer und vielfältiger wird, müssen SOC-Teams stets über die neuesten Entwicklungen informiert sein. 81 Prozent der Umfrageteilnehmer gaben an, dass Bedrohungsdaten für ihre IR-Prozesse entscheidend sind. Um auf dem Laufenden zu bleiben, abonnieren Unternehmen im Durchschnitt 6,8 Bedrohungsdatenfeeds. Werden diese Datenströme nicht umfassend verwaltet und integriert, werden allerdings potenziell gefährliche Bedrohungen leicht übersehen. 62 Prozent der Umfrageteilnehmer beschreiben die Nutzung von Bedrohungsdaten als zeitaufwendig.

Bei der Wahl eines neuen Sicherheitstools hat die Integration der Bedrohungsdaten daher höchste Priorität. 50 Prozent der Umfrageteilnehmer gaben an, dass sich die Sicherheits-Workflows durch die Integration von Bedrohungsdaten stark verbessern ließen (siehe Abbildung 9). Rechnet man die 46 Prozent hinzu, die in ihrer Antwort angaben, dass ihre IR-Workflows „ein wenig“ davon profitieren würden, sind sogar beachtliche 96 Prozent der Befragten für die Integration von Bedrohungsdaten.

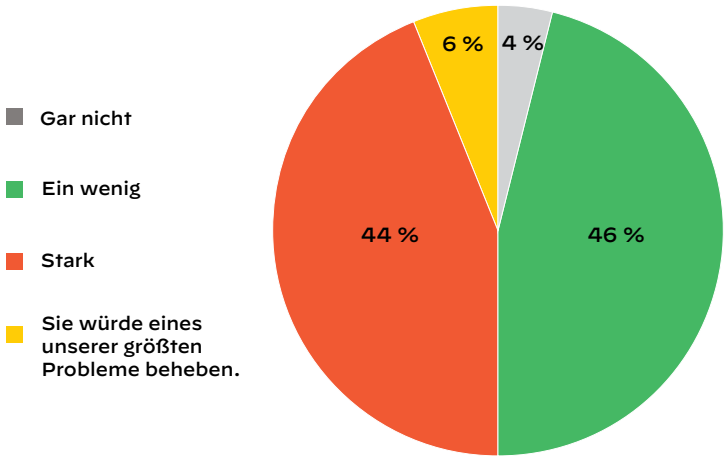

Abbildung 9: „Wie stark würde Ihr Sicherheits-Workflow von einer besseren Integration der Bedrohungsdaten profitieren?“

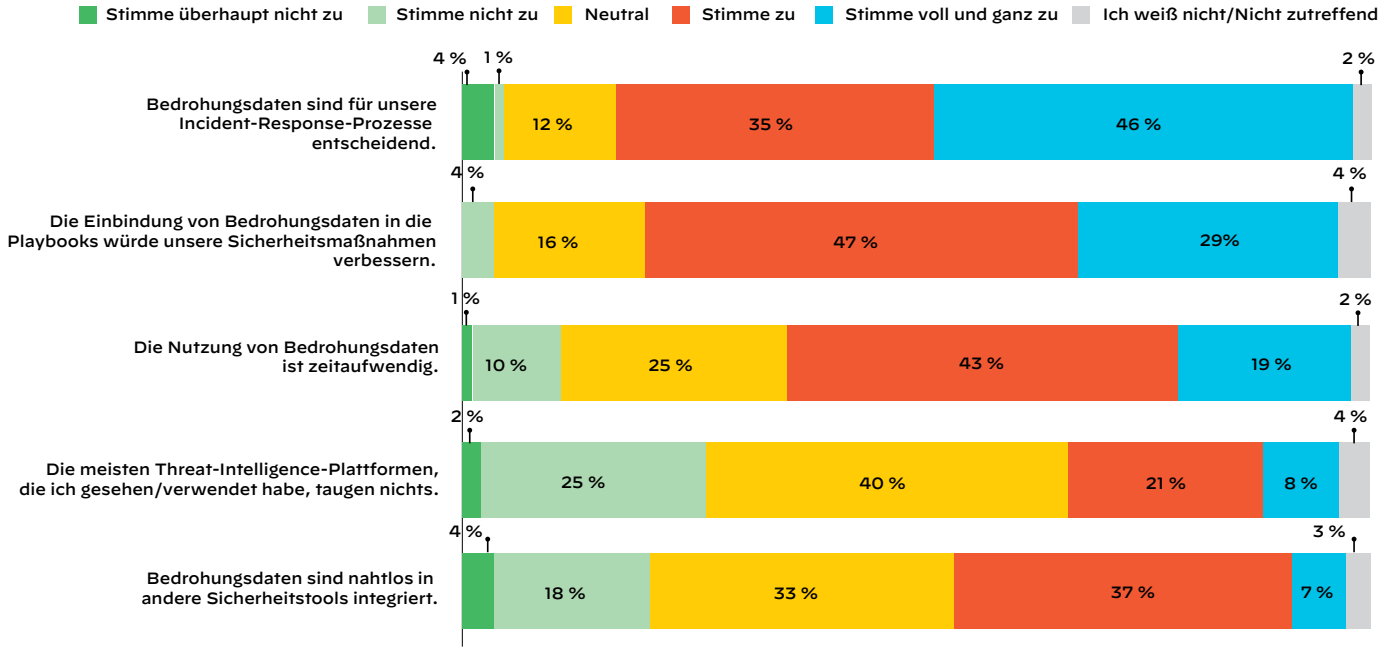

Abbildung 10: „Bitte geben Sie an, inwieweit Sie den folgenden Aussagen zu Bedrohungsdaten zustimmen.“

Der aktuelle Stand der Integration lässt allerdings zu wünschen übrig. Nur 43 Prozent der Befragten stimmten der Aussage „Bedrohungsdaten sind nahtlos in andere Sicherheitstools integriert“ zu. Zudem sind lediglich 28 Prozent der Untersuchungsprozesse mit Bedrohungsdatenquellen verknüpft.

Bestimmte Umfrageergebnisse geben Aufschluss darüber, weshalb sich viele zwar die Integration von Bedrohungsdaten wünschen, diese bisher aber kaum erfolgt ist. Eines der Probleme ist, dass zahlreiche unterschiedliche Mitarbeiter in das Bedrohungsdatenmanagement involviert sind. Wie in Abbildung 11 zu sehen, gehören dazu SecOps-Teams, Mitglieder des unternehmensinternen Sicherheitsteams, IT-Teams, separate Threat-Intelligence-Teams und andere Abteilungen. Auch die Einschätzung der Qualität der Threat-Intelligence-Plattformen spielt eine Rolle, denn 29 Prozent der Befragten stimmten der Aussage „Die meisten Threat-Intelligence-Plattformen, die ich gesehen/verwendet habe, taugen nichts“ zu.

In den Bedrohungsdatenprozess sind 12 unterschiedliche Systeme eingebunden (siehe Abbildung 12). Die in Abbildung 11 aufgeführten Mitarbeiter nutzen für die Bedrohungsdaten SIEM-Lösungen, Tools für die Analyse des Netzwerkverkehrs, Intrusion-Detection-Systeme (IDS) und weitere Produkte. Es versuchen also zu viele Personen mit zu vielen, nicht richtig integrierten Plattformen, die Bedrohungsdaten zu verwalten. Da wundert es kaum, dass sie frustriert sind.

Weniger Warnmeldungen für SecOps-Teams

SOC-Analysten müssen viel zu viele Warnmeldungen bearbeiten und sind überfordert. Warnungsmüdigkeit ist tatsächlich ein Problem und kann zu einem Burn-out oder zur Abwanderung der Mitarbeiter führen. Außerdem besteht das Risiko, dass wichtige Bedrohungen in der Masse der Benachrichtigungen übersehen werden. Die COVID-19-Pandemie verschärft die Lage zusätzlich. 47 Prozent der Unternehmen erhalten seit dem Beginn der Pandemie mehr Warnmeldungen. In diesen Unternehmen stieg die Zahl der Warnmeldungen im Durchschnitt um 34,2 Prozent.

Einfache Integration der SecOps-Technologien in Lösungen von Drittanbietern

Die IR-Workflows beginnen an verschiedenen Stellen (siehe Abbildung 13) und im weiteren Verlauf werden zahlreiche Lösungen und Abteilungen eingebunden. Die Integration der IR-Tools in Drittanbieterlösungen kann dabei helfen, Vorfälle effektiv abzuwehren, und dadurch auch die Produktivität der SOC-Teams steigern. Laut der Umfrage wird dies generell unterstützt. 30 Prozent der Befragten gaben an, dass sie sich eine Plattform für abteilungsübergreifende Prozesse wünschen. Allerdings steht bisher nur 32 Prozent der Umfrageteilnehmer eine solche Plattform zur Verfügung.

Um die Ausmaße dieses Problems zu verstehen, muss man wissen, dass SOC-Teams in jeder der vier großen IR-Phasen diverse Tools verwenden. Wie in Abbildung 13 zu sehen, werden überwiegend SIEM-Lösungen eingesetzt: Hier finden 69 Prozent der Prozesse für den Datenimport und die Datenanreicherung sowie knapp die Hälfte des Fallmanagements und der Vorfallsuntersuchung statt. SOAR-Plattformen werden bei 20 Prozent der Prozesse für die Abwehrmaßnahmen und Richtliniendurchsetzung sowie bei 22 Prozent der Vorfallsuntersuchungen genutzt. Threat-Intelligence-Plattformen sind weniger weit verbreitet und werden nur für knapp 20 Prozent der Prozesse in allen vier Bereichen eingesetzt.

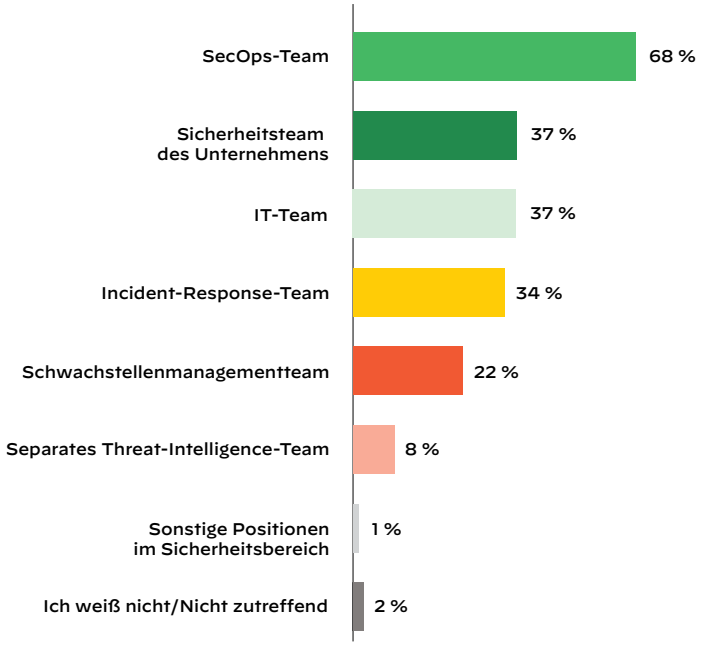

Abbildung 11: „Wer ist in Ihrem Unternehmen in das Bedrohungsdatenmanagement involviert?“

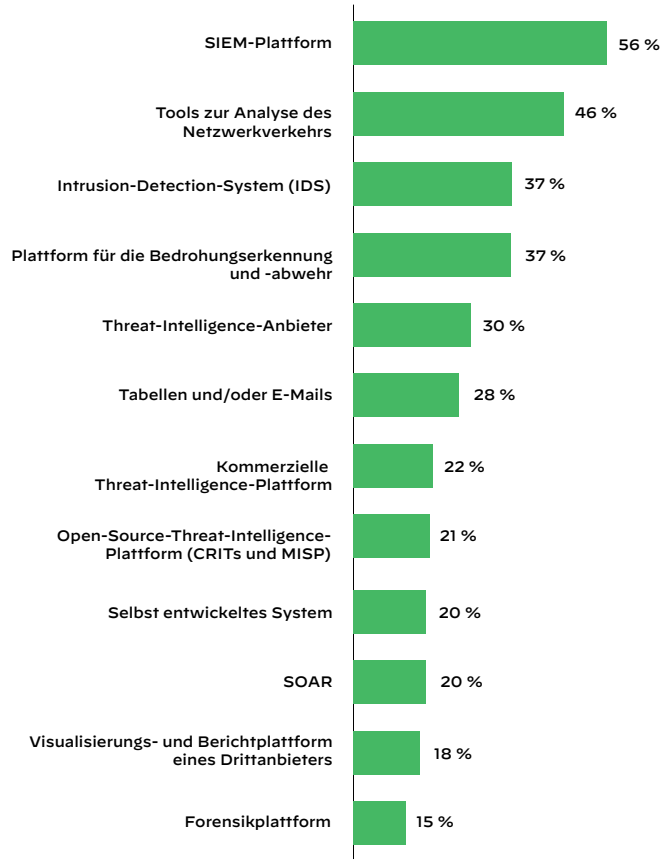

Abbildung 12: „Welche Managementtools und/oder -Funktionen verwenden Sie, um Bedrohungsdaten zu aggregieren, zu analysieren und/oder zu präsentieren? Bitte wählen Sie alle zutreffenden Antworten aus.“

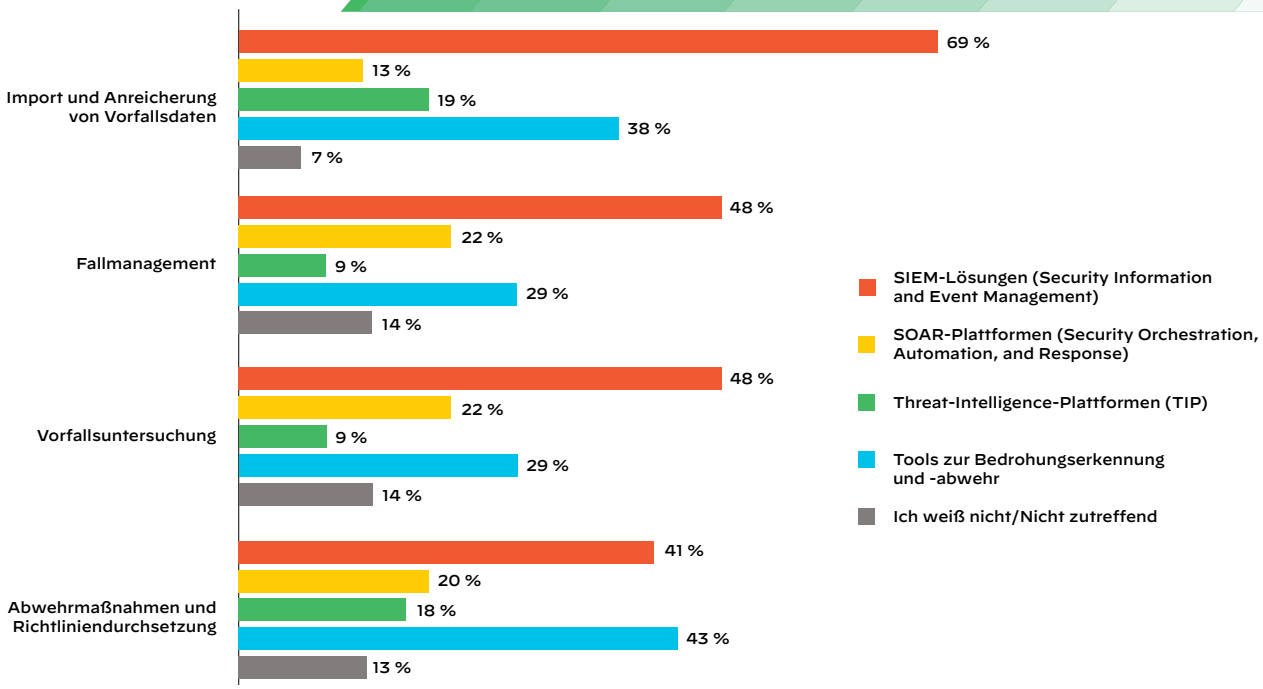

Abbildung 13: „Welche Lösungen verwenden Sie für die folgenden Schritte des Incident-Reponse-Prozesses? Bitte wählen Sie alle zutreffenden Antworten aus."

Obwohl viele verschiedene Abteilungen eines Unternehmens am IR-Workflow beteiligt sind, gibt es kaum Verknüpfungen zwischen den einzelnen Systemen. Am besten sind die IR-Lösungen und die Tools der IT-Teams integriert: 23 Prozent der Systeme und Prozesse wurden als „eng verzahnt" beschrieben (siehe Abbildung 14). Mit den NOC-Teams (Network Operations Center) gibt es nur in 16 Prozent der Fälle eine enge Verzahnung. Bei den Personalabteilungen waren sogar die Hälfte der Systeme und Prozesse vollständig separat. Bei den Rechtsabteilungen und den Complianceteams laufen 48 Prozent bzw. 30 Prozent der Verfahren vollständig getrennt ab.

Die Aussage „Wir nutzen einige Systeme/Prozesse gemeinsam" traf für 51 Prozent der Complianceteams, 56 Prozent der IT-Teams und 52 Prozent der NOC-Teams zu. Bei den anderen Gruppen und Abteilungen überschneiden sich weniger als die Hälfte der Systeme und Prozesse. Die geringste Verzahnung gab es zwischen den IR-Workflows und den Rechtsabteilungen mit nur 7 Prozent. Das ist unter Umständen darauf zurückzuführen, dass die Rechtsabteilungen spezielle Systeme für das Fallmanagement verwenden. Es sind auch nicht alle Sicherheitsvorfälle für die Rechtsabteilungen relevant, doch die unzureichende Verzahnung kostet unnötig Zeit und Geld, da die Teams die Workflows manuell abgleichen müssen.

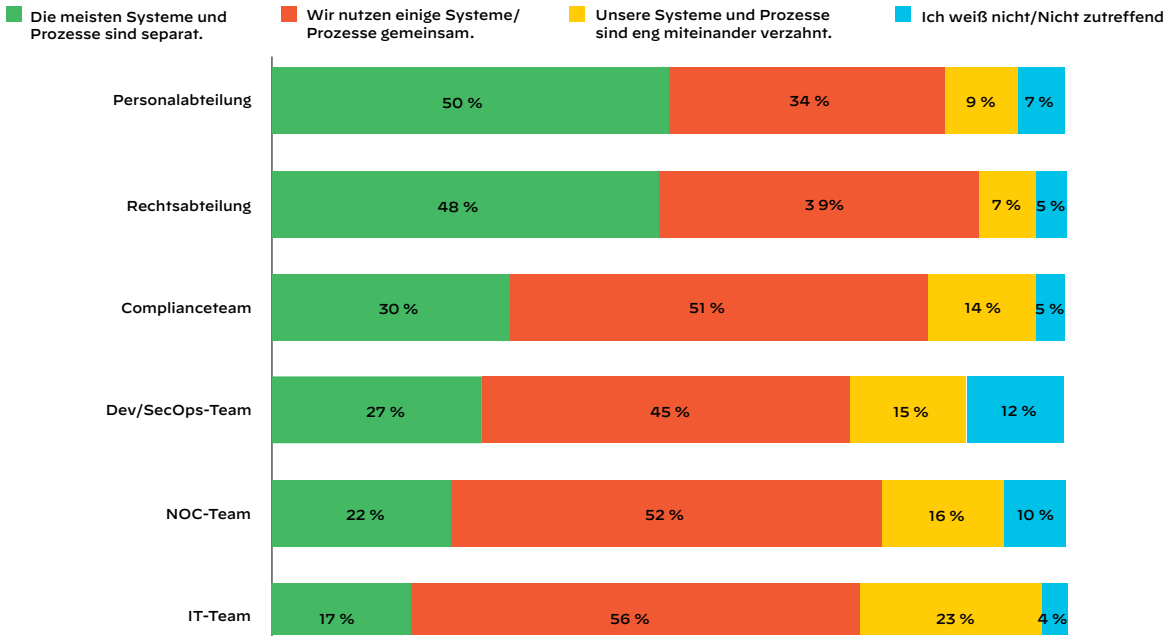

Abbildung 14: „In welchem Maße nutzen Sie Tools, Prozesse, Systeme und Datenströme gemeinsam mit den folgenden Teams?"

Großes Interesse an Marktplattformen von Drittanbietern und Communitys für den Informationsaustausch

In der Cybersicherheitsbranche ist es üblich, dass sich Entwickler und Unternehmen in Communitys austauschen, um die Sicherheitsmaßnahmen zu optimieren. Das ist eventuell darauf zurückzuführen, dass es ursprünglich überwiegend Open-Source-Versionen der Sicherheits- und Computertechnologien gab und dass viele Experten ihre Karriere in der Strafverfolgung oder beim Militär begonnen haben, wo der Informationsaustausch aktiv gefördert wird. In der Realität ist das nicht immer umsetzbar, der Wunsch nach einem solchen Informations- und Erfahrungsaustausch ist dennoch deutlich zu spüren.

Die Umfrageergebnisse zeigen dies ebenfalls, denn 78 Prozent der Befragten gaben an, dass sie sich ein einheitliches Framework und eine Community für den Austausch von Informationen, Integrationen und Playbooks wünschen. Nur 42 Prozent sind der Ansicht, dass sie die besten Playbooks selbst entwickeln. Neben den Communitys zeigten die Befragten auch großes Interesse an Marktplattformen von Drittanbietern. 52 Prozent gaben an, dass sie eine nützliche Integration in Drittanbieter-Tools kaufen würden. In Abbildung 15 sind die Prozentzahlen für das Interesse an einheitlichen Frameworks, Communitys für den Informationsaustausch und Marktplattformen von Drittanbietern angegeben.

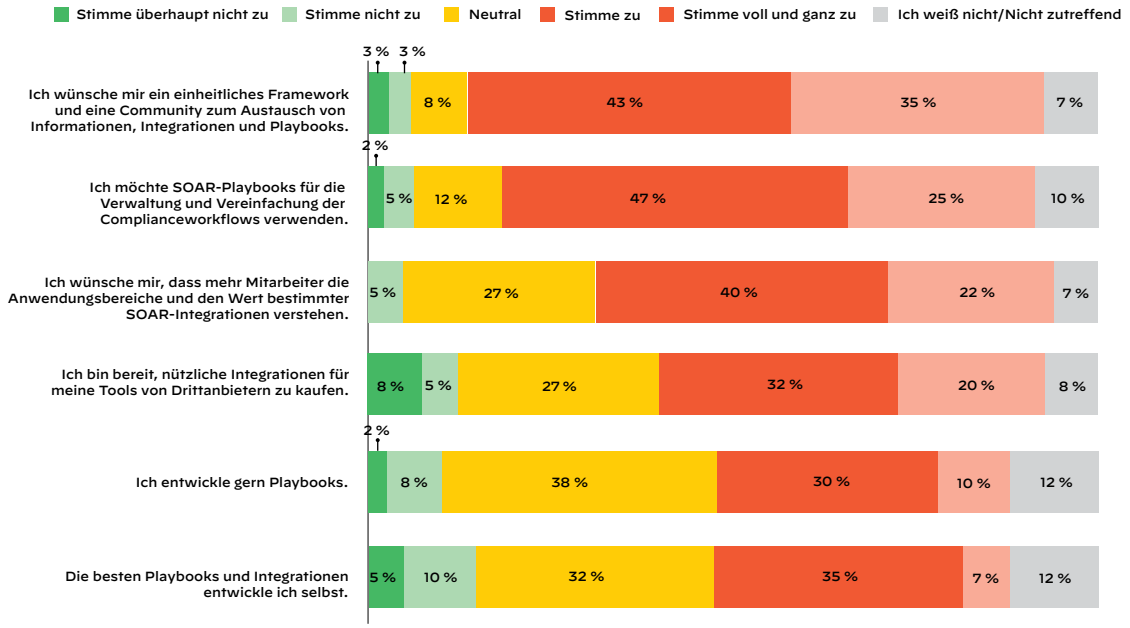

Abbildung 15: „In welchem Maße nutzen Sie Tools, Prozesse, Systeme und Datenströme gemeinsam mit den folgenden Teams?“*

Welchen Playbooks würden Sicherheitsexperten vertrauen? Das größte Vertrauen genießen SOAR-Anbieter. 53 Prozent der Umfrageteilnehmer gaben an, dass sie am ehesten von Anbietern zertifizierten Playbooks vertrauen würden (siehe Abbildung 16). Darauf folgen selbst entwickelte Playbooks (47 %), von SOAR-Anbietern erstellte Playbooks (44 %) und von MSSP oder anderen Sicherheitspartnern erstellte Playbooks (35 %).

Interessant ist, dass sich zwar fast 8 von 10 Umfrageteilnehmern eine Community wünschen, aber nur 20 Prozent den Playbooks von Community-Mitgliedern vertrauen würden. Diese Diskrepanz ist vermutlich darauf zurückzuführen, dass 53 Prozent der Befragten von Anbietern zertifizierte Playbooks bevorzugen. Diese Ergebnisse unterstreichen also, wie wichtig eine Zertifizierung ist.

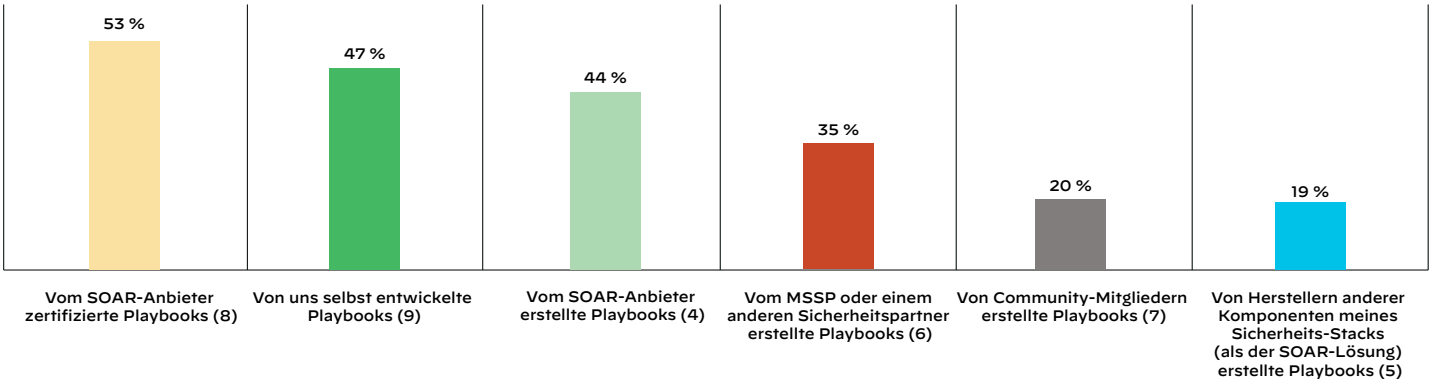

Abbildung 16: „Welchen dieser Quellen für SOAR-Playbooks würden Sie am ehesten vertrauen? Bitte wählen Sie alle zutreffenden Antworten aus.“

* Durch die Rundung überschreiten die Prozentwerte 100 %.

Der Stand von SOAR

Mit SOAR lassen sich viele der in der Umfrage genannten Herausforderungen bewältigen, darunter die Ausweitung der Automatisierung und die Reduzierung der Warnungsmüdigkeit. Das ist möglicherweise eine Ursache für das große Interesse an SOAR, das es unseren Umfrageergebnissen zufolge gibt. Der Anteil der Umfrageteilnehmer, die bereits SOAR-Lösungen verwenden oder die Implementierung innerhalb der nächsten 12 Monate geplant haben, ist erstaunlich hoch. SOAR spielt in dem IR-Workflow und der SecOps-Umgebung insgesamt eine immer größere Rolle und wird im kommenden Jahr wahrscheinlich noch wichtiger werden.

Wachsende Zahl an SOAR-Anwendungsbereichen

SOC-Teams nutzen SOAR-Lösungen in verschiedenen Bereichen. Wie in Abbildung 17 zu sehen, werden SOAR-Lösungen bisher am häufigsten in der Bedrohungserkennung und -abwehr (45 %), der Priorisierung von Sicherheitslücken (37 %), bei Compliancepr üfungen (30 %) und Sicherheitsaudits (30 %) eingesetzt.

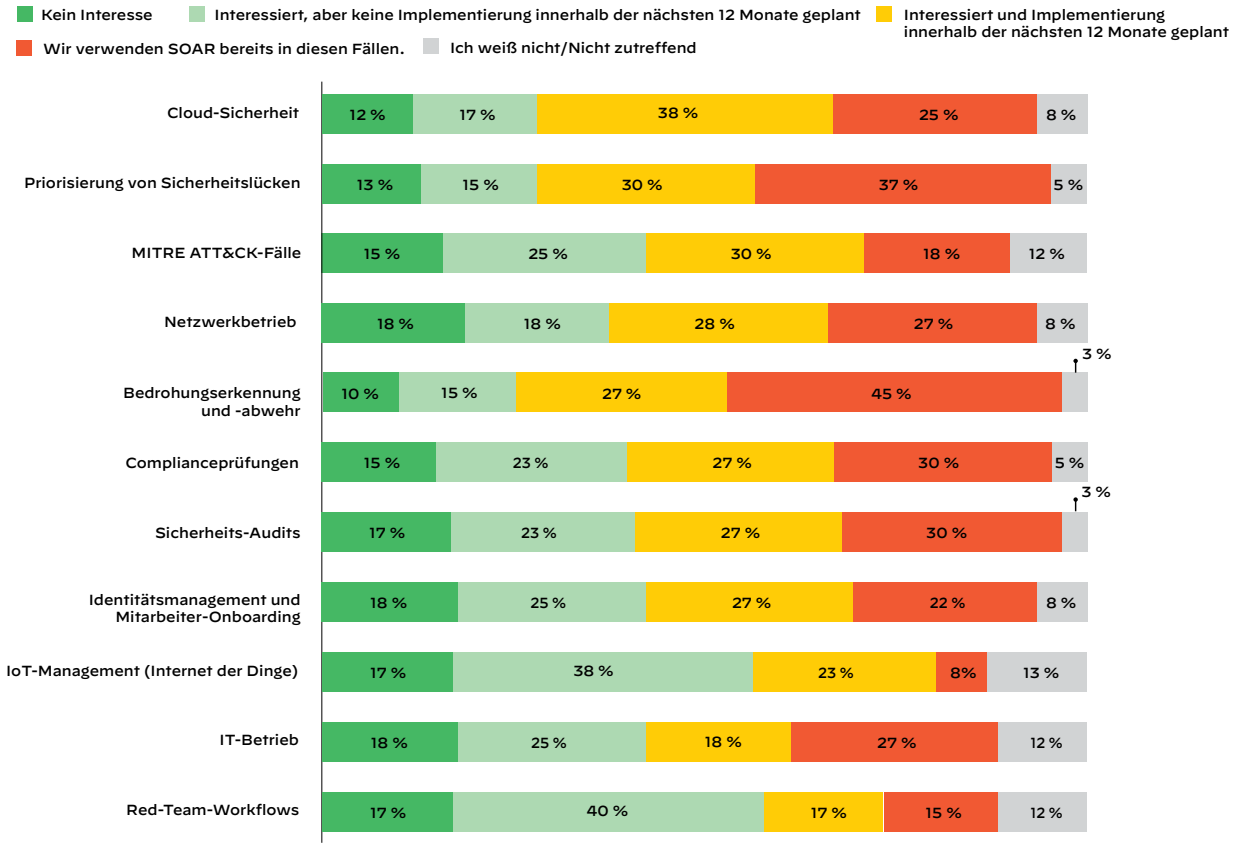

Abbildung 17: „In welchem Maße planen Sie, SOAR-Lösungen in den folgenden Anwendungsbereichen einzusetzen?“

In den anderen in der Umfrage genannten Bereichen werden SOAR-Lösungen bisher nicht so häufig genutzt, aber die Technologie wird grundsätzlich eingesetzt. Sicherheitsteams nutzen SOAR-Lösungen für Red-Team-Workflows (15 %), IT-Abläufe (27 %), den Netzwerkbetrieb (27 %) und MITRE ATT&CK®-Fälle (18 %). Diese Ergebnisse deuten darauf hin, dass die Sicherheitsteams durchaus an SOAR-Lösungen interessiert sind, die Implementierung allerdings bisher nur langsam voranschreitet.

Zunehmende SOAR-Nutzung

Laut den Umfrageergebnissen nimmt die SOAR-Nutzung in den SOC zu. Knapp die Hälfte der Befragten (46 Prozent) gaben an, dass sie bereits SOAR-Lösungen verwenden oder diese innerhalb der nächsten 12 Monate einsetzen möchten. Es gibt allerdings bisher kaum Langzeitnutzer. Nur 7 Prozent der Umfrageteilnehmer verwenden die Technologie seit mehr als zwei Jahren. In Abbildung 18 ist die SOAR-Nutzung aufgeschlüsselt. Erwähnenswert ist, dass 41 Prozent der Befragten SOAR zwar kennen, aber nicht planen, es innerhalb der nächsten 12 Monate einzusetzen, und 12 Prozent noch nie davon gehört haben. Für den letzten Punkt ist allerdings eventuell auch die Änderung der Kategoriebezeichnung von SAO zu SOAR vor noch nicht allzu langer Zeit verantwortlich.

SOAR-Vorteile für IR und SecOps

SOAR bringt Vorteile für verschiedene IR- und SecOps-Bereiche mit sich, unter anderem auch, weil sich damit bestimmte SecOps-Prozesse automatisieren lassen. Gartner hat es so zusammengefasst: „Die neue SOAR-Technologie verspricht ein Maß an Automatisierung, Konsistenz und Effizienz in SOC, das mit SIEM bisher nicht erreicht werden kann.“[3]

54 Prozent der Umfrageteilnehmer, die SOAR seit mindestens zwei Jahren nutzen, gaben an, dass sie mit der Technologie nun schneller auf Vorfälle reagieren können. Zu den Verbesserungen zählten außerdem die schnellere Abwehr von Bedrohungen (51 %), die bessere Reaktionszeit insgesamt (47 %) und die schnellere Ersteinschätzung (44 %). Weitere 37 Prozent gaben an, dass sie mithilfe von SOAR die Zahl der IR-Schritte reduzieren konnten.

In Abbildung 19 ist erkennbar, wie stark SOAR-Lösungen die SOC-Leistung dieser Unternehmen verbessert haben, insbesondere durch:

- Besser definierte Prozesse (79 %)
- Bessere Kommunikation mit anderen Teams (53 %)
- Reduzierung oder sogar Vermeidung unnötiger Workflow-Schritte (47 %)
- Flachere Hierarchie im Team durch die Verbesserung der Fertigkeiten der Analysten (42 %)
- Die Möglichkeit, auch komplexere Sicherheitsfälle anzugehen (42 %)
- Flachere Hierarchie im Team durch die Automatisierung der Prozesse (37 %)

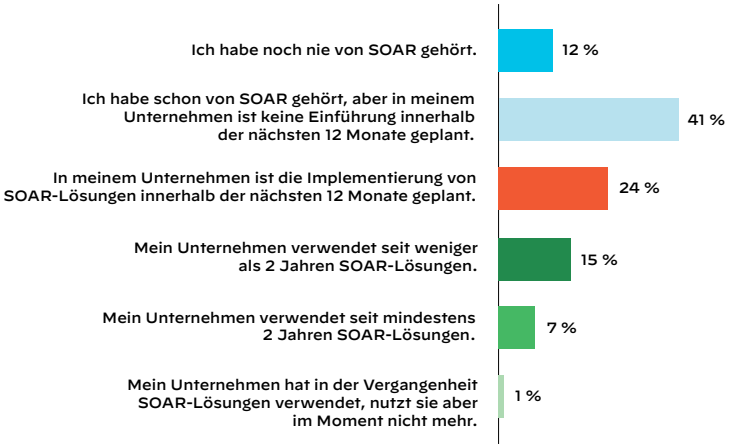

Abbildung 18: „Welche der folgenden Aussagen beschreibt Ihre Nutzung, Ihr Interesse an und Ihre Kenntnisse der SOAR-Tools am besten?“

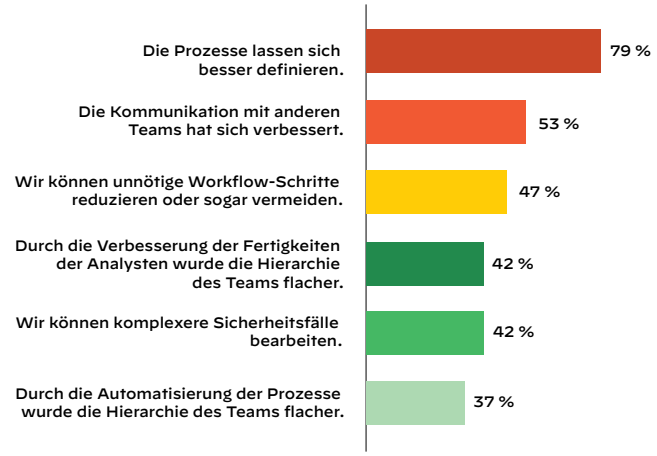

Abbildung 19: „Inwiefern haben sich die Workflows nach der Implementierung von SOAR-Lösungen geändert? Bitte wählen Sie alle zutreffenden Antworten aus.“ Hinweis: N = 19

Diese Ergebnisse deuten darauf hin, dass SOAR eine zuverlässige Lösung für einige der aktuellen Herausforderungen der SOC-Teams bietet. Die bessere Kommunikation mit externen Teams trägt zur Lösung des in Abbildung 14 genannten Problems (wenig effektive Zusammenarbeit zwischen SOC-Teams und Rechts-, Personal- und IT-Abteilung sowie anderen Mitarbeitern) bei. Da die Verwaltung und die Behebung von Vorfällen weniger Zeit in Anspruch nehmen, helfen SOAR-Lösungen auch dabei, den potenziellen Druck durch die zahlreichen Warnmeldungen und die Kontrolle der vielen Bedrohungsdatenfeeds zu reduzieren. Dank der schnelleren Ersteinschätzung und größeren Produktivität können sich die SOC-Teams auf schwerwiegende Vorfälle konzentrieren und verschwenden keine Zeit mit unwichtigen Warnmeldungen.

3. „Top Security and Risk Management Trends“, Gartner, 27. Februar 2020

Steigendes Interesse und mehr Kaufabsichten

Welche Rolle spielt SOAR in den Zukunftsplänen der Sicherheitsmanager? 43 Prozent aller Umfrageteilnehmer planen, im kommenden Jahr mehr in SOAR-Tools zu investieren.

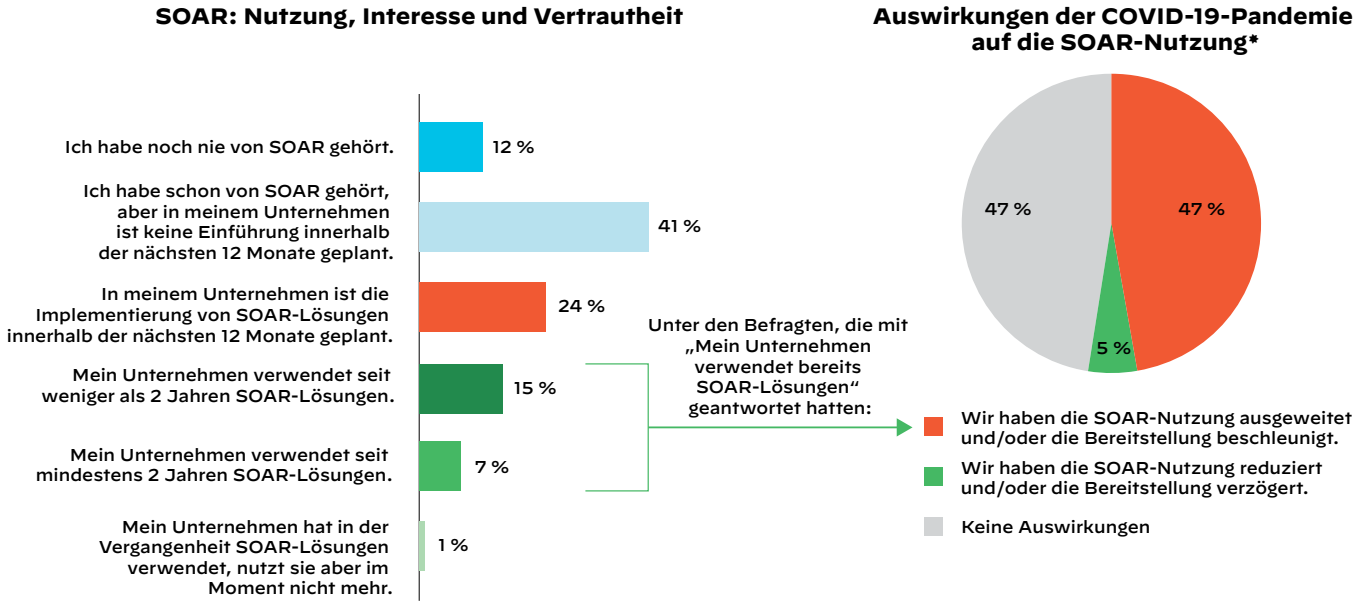

Abbildung 20: „Inwiefern hat die COVID-19-Pandemie die (geplante oder aktuelle) SOAR-Nutzung in Ihrem Unternehmen beeinflusst?“ Hinweis: N = 19

SOAR für IoT, MITRE und Red-Team-Einsätze

SOAR-Nutzer haben für die Zukunft schon die Ausweitung auf bestimmte Workloads geplant. In Tabelle 1 sind die Antworten auf die Frage „In welchem Maße planen Sie, SOAR-Lösungen in den folgenden Anwendungsbereichen einzusetzen?“ aufgeführt. 38 Prozent der Unternehmen, die bereits SOAR-Lösungen nutzen, planen, diese innerhalb der nächsten 12 Monate auch für das Internet der Dinge (IoT) zu verwenden. Weitere 23 Prozent sind prinzipiell an diesem Anwendungsbereich interessiert, planen aber nicht, dies schon im kommenden Jahr zu implementieren. Rechnet man die Unternehmen hinzu, die SOAR-Lösungen bereits für das IT-Management nutzen, kommt man auf beachtliche 69 Prozent, die die Technologie als Teil ihrer IoT-Managementstrategie betrachten.

Red-Team-Workflows, Cloud-Sicherheit und MITRE ATT&CK®-Fälle gehören ebenfalls zu den Bereichen, für die SOAR-Lösungen durchaus in Betracht gezogen werden. Je 57, 55 und 55 Prozent der Unternehmen nutzen SOAR-Tools bereits für diese Zwecke oder interessieren sich dafür. Selbst die Anwendungsbereiche, an denen die Unternehmen weniger interessiert sind (Priorisierung von Sicherheitslücken, IT-Abläufe sowie die Bedrohungserkennung und -abwehr), erzielen noch je 45, 43 und 42 Prozent.

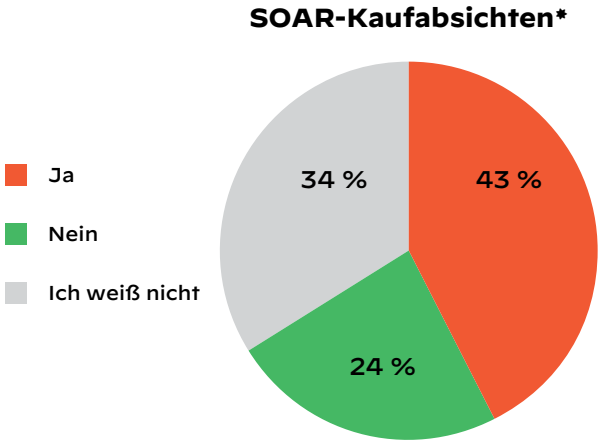

Abbildung 21: „Plant Ihr Unternehmen, 2020 die Ausgaben für SOAR-Tools zu erhöhen?“

* Durch die Rundung überschreiten die Prozentwerte 100 %.

Tabelle 1: Antworten auf die Frage „In welchem Maße planen Sie, SOAR-Lösungen in den folgenden Anwendungsbereichen einzusetzen?“		
	Interessiert und Implementierung innerhalb der nächsten 12 Monate geplant	Wir verwenden SOAR bereits in diesen Fällen.
IoT-Management	38 %	8 %
Red-Team-Workflows	40 %	15 %
Cloud-Sicherheit	17 %	25 %
MITRE ATT&CK-Fälle	25 %	18 %
Identitätsmanagement und Mitarbeiter-Onboarding	25 %	22 %
Complianceprüfungen	23 %	30 %
Sicherheitsaudits	23 %	30 %
Netzwerkbetrieb	18 %	27 %
Priorisierung von Sicherheitslücken	15 %	37 %
IT-Betrieb	25 %	27 %
Bedrohungserkennung und -abwehr	15 %	45 %
Mittelwerte	24 %	26 %

Wie Cortex XSOAR die Situation verbessert

Cortex™ XSOAR von Palo Alto Networks ist eine Plattform, die Aktionen über den gesamten Sicherheits-Stack hinweg orchestriert, um schnellere und besser skalierbare Incident-Response-Maßnahmen zu ermöglichen. Zudem verbindet sie isolierte Tools und automatisiert einfache, repetitive Aufgaben, bei denen ein Eingriff des Menschen nicht notwendig ist, und trägt somit zur Optimierung der IR-Prozesse bei. Cortex XSOAR ist die branchenweit erste Sicherheitslösung mit nativem Vorfallsmanagement und Funktionen für die Zusammenarbeit, Sicherheitsorchestrierung und -automatisierung sowie Bedrohungsdaten auf einer einzigen Plattform.

Mit Cortex XSOAR lassen sich viele der IR-Probleme der Umfrageteilnehmer beheben. Details dazu finden Sie in Tabelle 2.

Tabelle 2: Wie Cortex XSOAR IR-Herausforderungen angeht		
Herausforderung/Wunsch	Benötigte Lösung	Funktion von Cortex XSOAR
Zu viele manuelle IR-Prozesse	Ausweitung der Automatisierung zur Beschleunigung der IR-Prozesse und Reduzierung der manuellen Aufgaben	Automatisierung repetitiver Aufgaben, da Prozesse mithilfe von Playbooks für den gesamten Sicherheits-Stack koordiniert werden können
Keine Integration der Lösungen von Drittanbietern	Integration der SOC-Tools in Drittanbietersysteme, damit problemlos Verbindungen zu anderen Abteilungen und IR-Prozessen hergestellt werden können	Mehr als 450 Integrationen von Drittanbieterprodukten zur Koordination und Automatisierung von SecOps-Prozessen
Austausch von Playbooks, die von der Community/Kollegen erstellt wurden	Mehr Playbooks, einschließlich Playbooks von Drittanbietern sowie eine Community für den Informationsaustausch, um aus den Erfahrungen anderer Teams zu lernen	Mehr als 15.000 Experten tauschen sich in einer offenen DFIR-Community (Digital Forensics and Incident Response) über die Best Practices aus.
Überwachung von zu vielen Bedrohungsdatenfeeds	Integration von Bedrohungsdaten in SecOps-Tools, um die Überwachung zahlreicher Feeds zu vereinfachen und sicherzustellen, dass keine gravierenden Bedrohungen übersehen werden	Bedrohungsdatenmanagement, bei dem die SOC-Teams die Kontrolle über die Bedrohungsdatenquellen haben, um die Aggregation, Einstufung und Integration in bewährte Playbook-basierte Automatisierungsprozesse zu vereinheitlichen
Zu viele Warnmeldungen für eine effektive oder effiziente Bearbeitung	Reduzierung der Warnmeldungen	Bis zu 95 % weniger Warnmeldungen, die überprüft werden müssen

Fazit

In diesem vierten Jahresbericht zum Stand von SOAR wird einmal mehr deutlich, wie rasant sich die Cybersicherheit verändert. Die Bedrohungen werden immer gefährlicher und viele SOC-Teams müssen inzwischen sogar Angriffe staatlich gesponserter Hackergruppen abwehren, die äußerst versiert vorgehen. Es überrascht daher nicht, dass manche Analysten sich trotz der unleugbaren Verbesserungen im SecOps-Bereich nach wie vor von den IR-Prozessen überfordert fühlen. Sie erhalten schlicht zu viele Warnmeldungen und müssen zu viele Bedrohungsdatenfeeds überwachen. Außerdem gibt es immer noch zu viele manuelle Prozesse, die die Reaktion verzögern und Mitarbeiter von wirklich wichtigen Warnmeldungen ablenken.

Die Sicherheitsanalysten wissen, wie die Situation verbessert werden könnte. Sie wünschen sich eine stärkere Automatisierung von IR-Prozessen und weniger Warnmeldungen. Die SOC-Tools müssten mit Systemen von Drittanbietern kompatibel sein. Ein größeres Angebot an Playbooks (und insbesondere an von den Anbietern zertifizierten Playbooks) würde die Effizienz der SOC ebenfalls steigern. Und nicht zuletzt müssten die Bedrohungsdaten besser in die SecOps-Tools integriert werden.

SOAR-Lösungen können bei vielen dieser Herausforderungen helfen. Mit Plattformen wie Cortex XSOAR können SOC-Teams Zeit sparen, die Ersteinschätzung beschleunigen und die Zahl der Schritte in IR-Prozessen reduzieren. Wie die Umfrageergebnisse zeigen, wird die SOAR-Nutzung im kommenden Jahr weiter zunehmen, da die SOC-Teams neue, innovative Anwendungsbereiche für die Technologie geplant haben. Die COVID-19-Pandemie hat zwar die Lage für die SOC-Teams verschärft, doch gerade jetzt ist ein guter Zeitpunkt, die SOAR-Implementierung anzugehen, um die Effizienz und die Produktivität in Zukunft zu steigern.

Anhang: Demografische Daten der Umfrage

Die Umfrageteilnehmer wurden aus den mehr als 150.000 Sicherheitsfachkräften in der Virtual Intelligence Briefings Community ausgewählt. Abbildung 22 zeigt die Aufschlüsselung der Umfrageteilnehmer nach Unternehmensgröße. Alle Umfrageteilnehmer haben Positionen im Sicherheitsoder Compliancebereich inne.

Von der Umfrage ausgeschlossen wurden Personen, die ...

- in Unternehmen mit weniger als 1.000 Mitarbeitern beschäftigt sind oder deren Unternehmen sämtliche Sicherheitsmaßnahmen ausgelagert haben
- sich nicht sicher waren, ob die Sicherheitsmaßnahmen teilweise oder vollständig ausgelagert wurden
- weder im Sicherheitsbereich arbeiten noch als Manager für den Sicherheitsbereich zuständig sind

Abgedeckt wurden in der Umfrage die Branchen Finanzwesen (17 %), Technologie und/oder technische Services (15 %), Gesundheitswesen (13 %) sowie Einzelhandel und andere Sektoren mit kleineren Prozentzahlen. Auf keine Branche entfallen mehr als 20 Prozent der Umfrageteilnehmer. 24 Prozent der Befragten arbeiten als Sicherheitsexperte (Security Engineer) oder Analyst. Weitere 17 Prozent sind Manager, die für die Cybersicherheit verantwortlich sind, und 14 Prozent sind Sicherheitsarchitekten.

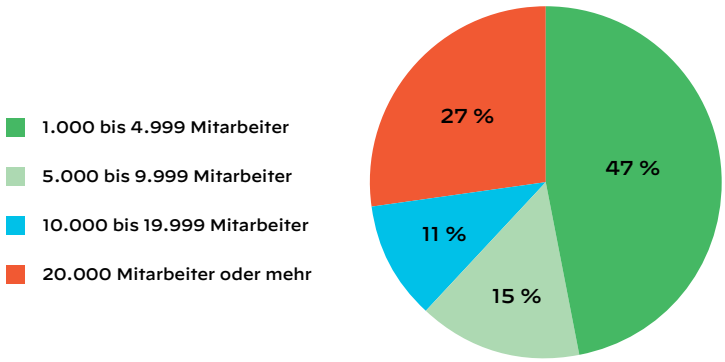

Abbildung 22: Demografische Daten der Unternehmen der Umfrageteilnehmer

paloalto NETWORKS

Oval Tower, De Entrée 99-197
1101 HE Amsterdam, Niederlande

Telefon: +31 20 888 1883
Vertrieb: +800 7239771
Support: +31 20 808 4600

www.paloaltonetworks.de