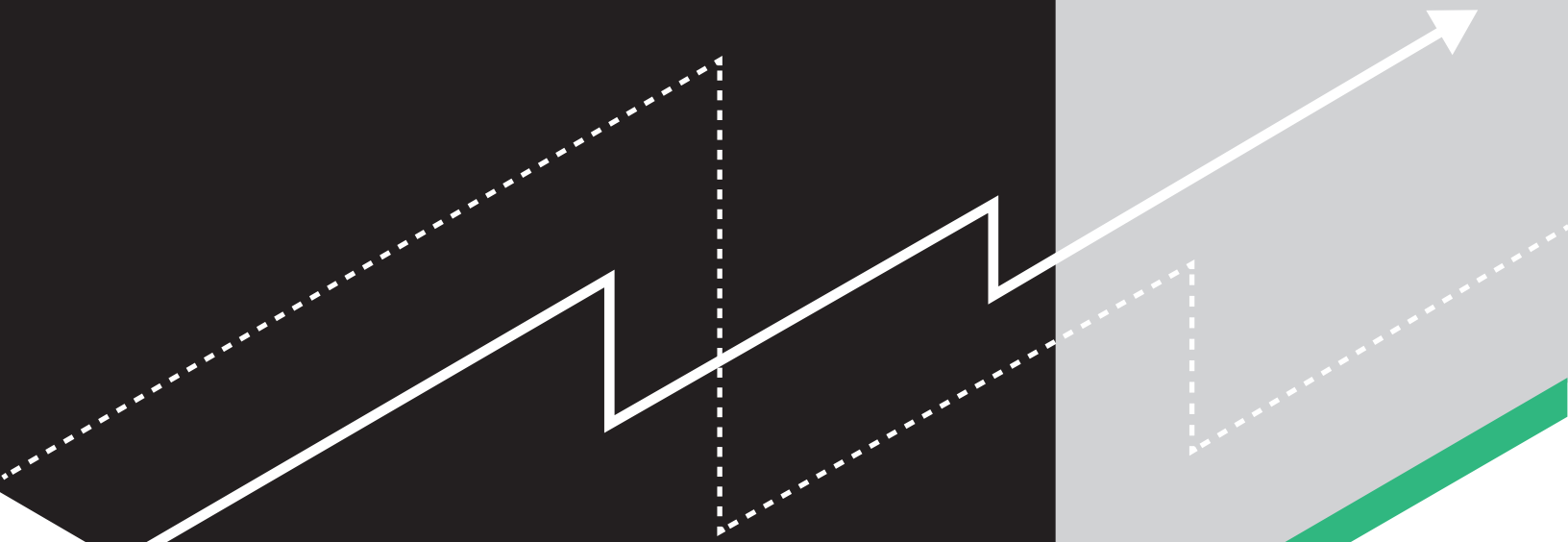
Ein Strategiepapier von
Forrester Consulting im
Auftrag von Palo Alto Networks

April 2020

Der Status quo im Bereich Security Operations 2020

SecOps-Teams tun sich schwer, wesentliche Ziele bei der Bewältigung einer wachsenden Zahl von Sicherheitsmeldungen zu erfüllen



FORRESTER®

Inhalt

Projektleitung:
Ana Brzezinska,
Market Impact Consultant

Studienbeitrag:
Forrester-Team für Sicherheits- und Risikoforschung

ÜBER FORRESTER CONSULTING

Forrester Consulting bietet unabhängige und objektive auf Forschungsergebnisse gestützte Beratungsdienstleistungen und hilft Führungskräften, ihre Organisationen zum Erfolg zu führen. Die Beratungsdienste von Forrester reichen von kurzen Strategiesitzungen bis hin zu kundenspezifischen Projekten. Im direkten Austausch mit Ihnen unterstützen Forschungsanalytiker Sie mit ihrem Fachwissen bei Ihren spezifischen geschäftlichen Herausforderungen. Weitere Informationen finden Sie unter forrester.com/consulting.

FORRESTER®

79 % der Unternehmen waren innerhalb des vergangenen Jahres von einer Datenschutzverletzung betroffen.

Zusammenfassung

Geschwindigkeit und Raffinesse von Datenschutzverstößen nehmen fortlaufend zu. Dies stellt für kleine wie große Unternehmen eine erhebliche Bedrohung dar. Mehr als drei Viertel aller Unternehmen waren innerhalb des vergangenen Jahres von einer Datenschutzverletzung betroffen. Datenschutzverletzungen haben erhebliche geschäftliche Auswirkungen vom Datenverlust bis hin zum verlorengegangenen Kundenvertrauen und zu potenziellen Rechtsstreitigkeiten. Gleichzeitig haben sie aber auch wesentliche Auswirkungen auf die Security-Operations-Teams.

Security-Operations-Teams bekämpfen Datenschutzverstöße häufig an vorderster Front, und Analysten bekommen den zusätzlichen Druck in der sicherheitsorientierten Welt von heute zu spüren. Besorgniserregend ist, dass nur 46 % der Entscheidungsträger im Bereich Security Operations mit ihren derzeitigen Möglichkeiten zur Bedrohungserkennung zufrieden sind. Sie monieren die Zeitverschwendung bei der Verfolgung von Fehlalarmen, schlecht integrierte Sicherheitstools und eine steile Lernkurve, die zur effektiven Nutzung dieser Tools bewältigt werden muss. Dies führt zu Intransparenz und ineffizienten Arbeitsabläufen. Viele Entscheidungsträger im Bereich Security Operations wünschen sich eine Lösung, die eine Verzahnung verschiedener Tools und Datenquellen erlaubt. Dies würde es Analysten gestatten, begründete Warnungen schneller zu identifizieren und Produktivität und Transparenz zu erhöhen.

Palo Alto Networks beauftragte Forrester Consulting mit einer Untersuchung zum Status quo im Bereich Security Operations in Unternehmen und zum gegenwärtigen Umgang mit Warnungen durch Security-Operations-Teams, um genauer zu erfahren, wo die wesentlichen Herausforderungen bei Sicherheitsabläufen in Unternehmen liegen. Forrester führte im April 2020 eine Onlinebefragung von 315 Teilnehmern aus den USA, Großbritannien, Deutschland, Frankreich, Australien, Neuseeland und Kanada durch, die in ihren Unternehmen Verantwortung für die Bereiche Security Operations und/oder Incident Response tragen.

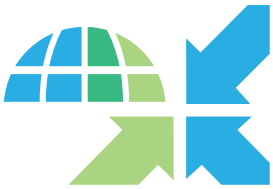
WESENTLICHE ERGEBNISSE

- **Eine Datenschutzverletzung stellt für jedes Unternehmen eine unmittelbare Gefahr dar.** Datenschutzverletzungen betreffen alle Unternehmen ohne Unterschied, und sie können in jedem Unternehmen jederzeit auftreten. Fast 50 % der befragten Unternehmen waren innerhalb der vergangenen sechs Monate und 79 % innerhalb des vergangenen Jahres einem Cyberangriff zum Opfer gefallen.
- **Sicherheitsteams sehen sich mit erheblichen technologischen Herausforderungen konfrontiert.** Security-Operations-Teams arbeiten mit vielen komplexen und isolierten Tools. Dies führt zu Ineffizienzen und verbesserungsfähigen Ergebnissen im Sicherheitsbereich, da die Analysten diese Tools integrieren und steile Lernkurven bewältigen müssen. Aufgrund von Problemen wie der Unklarheit darüber, welcher Endpunktprozess eine Warnmeldung im Netzwerk ausgelöst hat, vergeuden Analysten Zeit damit, falsch positive Meldungen zu verfolgen.
- **Die Investition in eine Lösung, die die Transparenz und Effizienz erhöhen kann, bringt viele Vorteile mit sich.** Weniger als 20 % der Teams setzen eine Lösung ein, die netzwerk-, anwendungs- und endpunktübergreifend Einblick gewährt. Daher leiden die Teams mehrheitlich unter „blinden Flecken“, deren Existenz ihnen zudem nicht bewusst ist. Wem es jedoch gelingt, seine Technologien für die Erkennung von Verstößen und die Einleitung von Gegenmaßnahmen zu verbessern, kann mit Vorteilen wie Produktivitätssteigerungen, höherer Transparenz und einer insgesamt niedrigeren Zahl von falsch positiven Meldungen rechnen.

FORRESTER®

Herausforderungen moderner Security-Operations-Center

Bei der Befragung von 315 Unternehmen zu ihren Herausforderungen im Bereich Security Operations erkannten wir eine Reihe von Gemeinsamkeiten bei der Definition moderner Security-Operations-Center (SOCs). Während die überwiegende Mehrheit (nämlich 94 %) der Unternehmen, die über ein internes SOC verfügen und zugleich einige Sicherheitsaspekte auslagern, einen mehrstufigen Ansatz verfolgt, beschäftigen Organisationen ohne internes SOC stattdessen unternehmensintern ein dediziertes Security-Operations-Team, das im Hinblick auf die Hierarchie heterogener agiert. Und auch wenn in 83 % der Unternehmen rund um die Uhr ein Security-Operations-Support zur Verfügung steht, fehlt es vielen Security-Operations-Teams an der passenden Kombination aus Personal und Technologie, um mit der zunehmenden Anzahl und Komplexität von Cyberangriffen Schritt zu halten: Oft haben sie Schwierigkeiten, die große Zahl eingehender Sicherheitswarnungen zu bearbeiten.

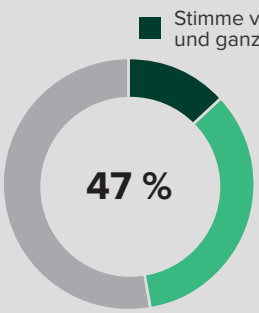


- **Moderne Unternehmen wissen um die Bedrohung durch Cyberangriffe.** 87 % der Entscheidungsträger denken dabei in erster Linie an von außen kommende Cyberangriffe auf ihre Organisation. Bei fast 80 % der befragten Unternehmen ist innerhalb des vergangenen Jahres ein solcher Verstoß aufgetreten, durch den Kundendaten und sensible Unternehmensdaten verloren gegangen und nicht zuletzt finanzielle Verluste eingetreten sind. Forrester Research zufolge kostet eine durchschnittliche Datenschutzverletzung bis zu 7 Mio. US-Dollar pro Vorfall. Die Kosten entstehen durch das Einleiten von Gegenmaßnahmen und das Erfüllen der Mitteilungspflichten, aber auch durch nachfolgende Produktivitätseinbußen und mögliche Rechtsstreitigkeiten und Geldbußen bis hin zu sonstigen Haftungskosten.[1] Und die Zahl der Angriffe nimmt stetig zu. Allein zwischen 2016 und 2017 hat die Zahl der Entscheidungsträger in weltweit tätigen Unternehmen, bei denen anders als im Vorjahr eine Sicherheitsverletzung auftrat, nach Erkenntnissen von Forrester um 5 Prozentpunkte zugenommen.[2]
- **Viel Zeit verbringen Analysten mit einer ineffizienten Bearbeitung von Warnmeldungen.** Jedes Security-Operations-Team erhält Tag für Tag im Schnitt über 11.000 Warnmeldungen, die überwiegend manuell bearbeitet werden müssen. 77 % der Entscheidungsträger stimmen darin überein, dass Warnungstriagen durch manuelles Vorgehen verlangsamt werden (Abbildung 1).

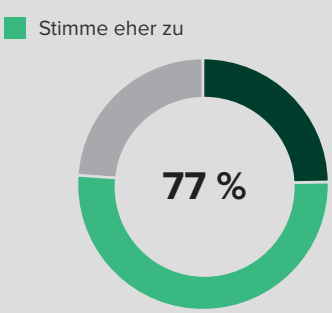
Abbildung 1: Warnmeldungen werden durch manuelle Prozesse verlangsamt und SecOps-Teams können mit der großen Zahl an Warnmeldungen nicht Schritt halten

„Inwieweit stimmen Sie den folgenden Aussagen zu?“

Wir können die meisten oder alle der täglich eingehenden Sicherheitswarnungen bearbeiten.



Unsere Prozesse für die Triage von Warnmeldungen werden durch manuelle Prozesse verlangsamt.



Basis: 315 globale Entscheidungsträger im Bereich Security Operations oder Incident Response
Quelle: Eine im Februar 2020 von Forrester Consulting im Auftrag von Palo Alto Networks durchgeführte Studie

Ein internes Security-Operations-Team erhält täglich im Durchschnitt **11.000** Warnmeldungen.

FORRESTER®

- **Security-Operations-Teams können mit der schieren Anzahl eingehender Warnmeldungen nicht Schritt halten.** Nur 47 % der Organisationen gaben an, dass sie in der Lage sind, die meisten oder alle der an einem Tag erhaltenen Sicherheitswarnungen zu bearbeiten. Fast 20 % der Warnmeldungen werden manuell durch einen Analysten geprüft und triagiert. Bei fast einem Drittel handelt es sich um falsch positive Meldungen, und 28 % werden von den Analysten gänzlich ignoriert, da sie nicht in der Lage sind, das Pensum zu bewältigen.
- **Analysten bekommen die Belastung zu spüren.** Die Folgen von Cyberangriffen gehen über die rein geschäftlichen Verluste hinaus: 96 % der Analysten sind nach einem Cyberangriff von erheblichen persönlichen Auswirkungen betroffen. Die meisten Analysten berichten von Überstunden, zusätzlichem Druck, mehr Nachtschichten und mehr Verantwortung nach einem Angriff (Abbildung 2). Vor allem VPs und C-Level-Führungskräfte machten sich im Nachgang eines Vorfalls Sorgen um ihren Arbeitsplatz.
- **Dies alles führt bei den Entscheidungsträgern zu Frustration und Unzufriedenheit.** Nur 46 % der Entscheidungsträger stimmten der Aussage zu, sie seien mit der Kompetenz ihrer Organisation zu Bedrohungserkennung zufrieden. Viele Entscheidungsträger wiesen auf ihre reaktiven Sicherheitsansätze als wesentliches Problem hin. 82 % der IT-Entscheidungsträger stimmten darin überein, dass ihr Ansatz, auf Bedrohungen zu reagieren, überwiegend oder vollständig reaktiv ist, während sie eigentlich gerne proaktiv handeln würden, und nur 50 % stimmten der Aussage zu, dass sie über die entsprechenden Ressourcen zur proaktiven Suche nach Bedrohungen verfügten.

Abbildung 2: Cyberangriffe haben sowohl finanzielle als auch personelle Auswirkungen

„Welche persönlichen Auswirkungen hatte die in Ihrem Unternehmen zuletzt aufgetretene Cybersicherheitsverletzung auf Sie?“

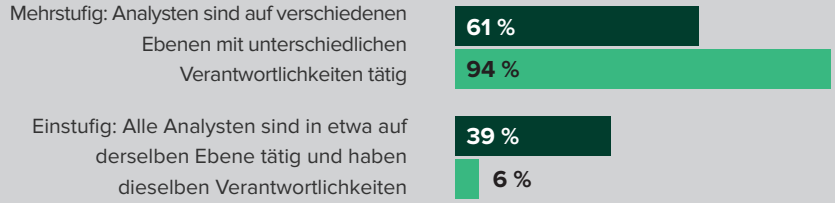
Basis: 313 globale Entscheidungsträger im Bereich Security Operations, bei denen eine Sicherheitsverletzung aufgetreten ist
Quelle: Eine im Februar 2020 von Forrester Consulting im Auftrag von Palo Alto Networks durchgeführte Studie

Obwohl die geschäftlichen Auswirkungen eines Cyberangriffs erheblich sind, müssen die persönlichen Auswirkungen auf die Analysten ebenfalls verstanden werden. **96 %** der Analysten waren von der jüngsten Sicherheitsverletzung in ihrer Organisation persönlich betroffen.

FORRESTER®

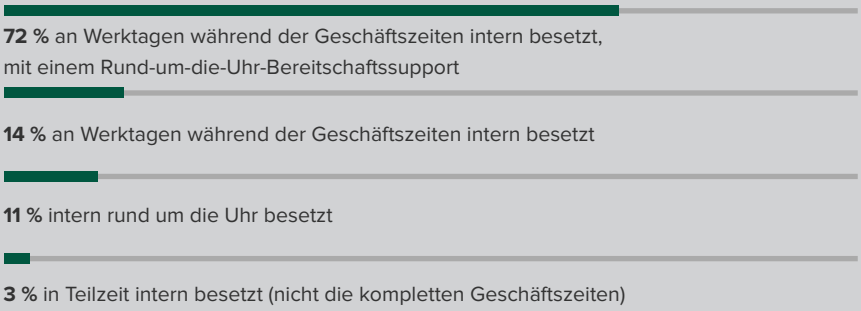
Abbildung 3: Momentaufnahme der Unternehmenssicherheit

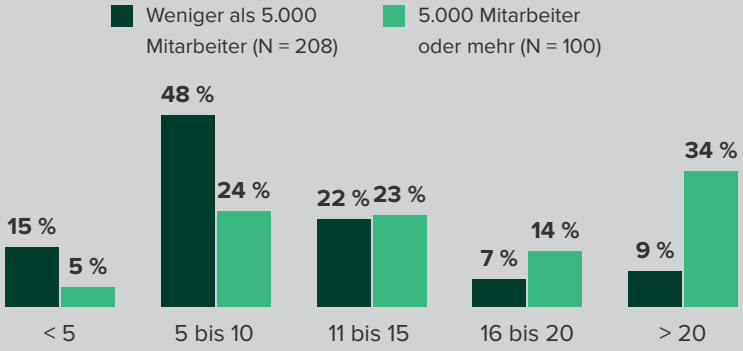
- Nein, wir haben kein internes Security-Operations-Center (SOC), aber wir verfügen über ein unternehmensinternes Security-Operations-Team. (N = 142)
- Ja, wir haben ein internes SOC, aber wir lagern auch gewisse Sicherheitsaspekte aus. (N = 135)



Die meisten Security-Operations-Teams sind mehrstufig. Zudem sind die meisten Security-Operations-Manager dem CIO oder CISO direkt unterstellt.

83 % der Unternehmen verfügen über eine Rund-um-die-Uhr-Abdeckung, wahlweise durch Vollzeitmitarbeiter oder Bereitschaftssupport.





Unternehmen verfügen im Durchschnitt über 14 Vollzeitsicherheits-analysten; kleinere Organisationen verfügen über 11, größere über 20.

Die Prüfung von Warnmeldungen nimmt die meiste Zeit der Analysten in Anspruch, gefolgt von der Triage und der Suche nach Bedrohungen. Nur 10,9 % werden auf Prozessver-besserungen verwendet.

Aufgabe	Durchschnittlicher Anteil der Stunden, die interne SecOps-Ressourcen mit der Aufgabe verbringen
Triage von Warnmeldungen	**21,8 %**
Prüfung von Warnmeldungen	**31,3 %**
Behebung von bzw. Reaktion auf Warnmeldungen	**14,8 %**
Suche nach Bedrohungen	**17,6 %**
Prozessverbesserungen	**10,9 %**

Basis: 315 globale Entscheidungsträger im Bereich Security Operations oder Incident Response
Quelle: Studie von Forrester Consulting, die im März 2020 im Auftrag von Palo Alto Networks durchgeführt wurde.

FORRESTER®

Auswirkungen komplexer Sicherheitsanforderungen auf die Geschäftsergebnisse

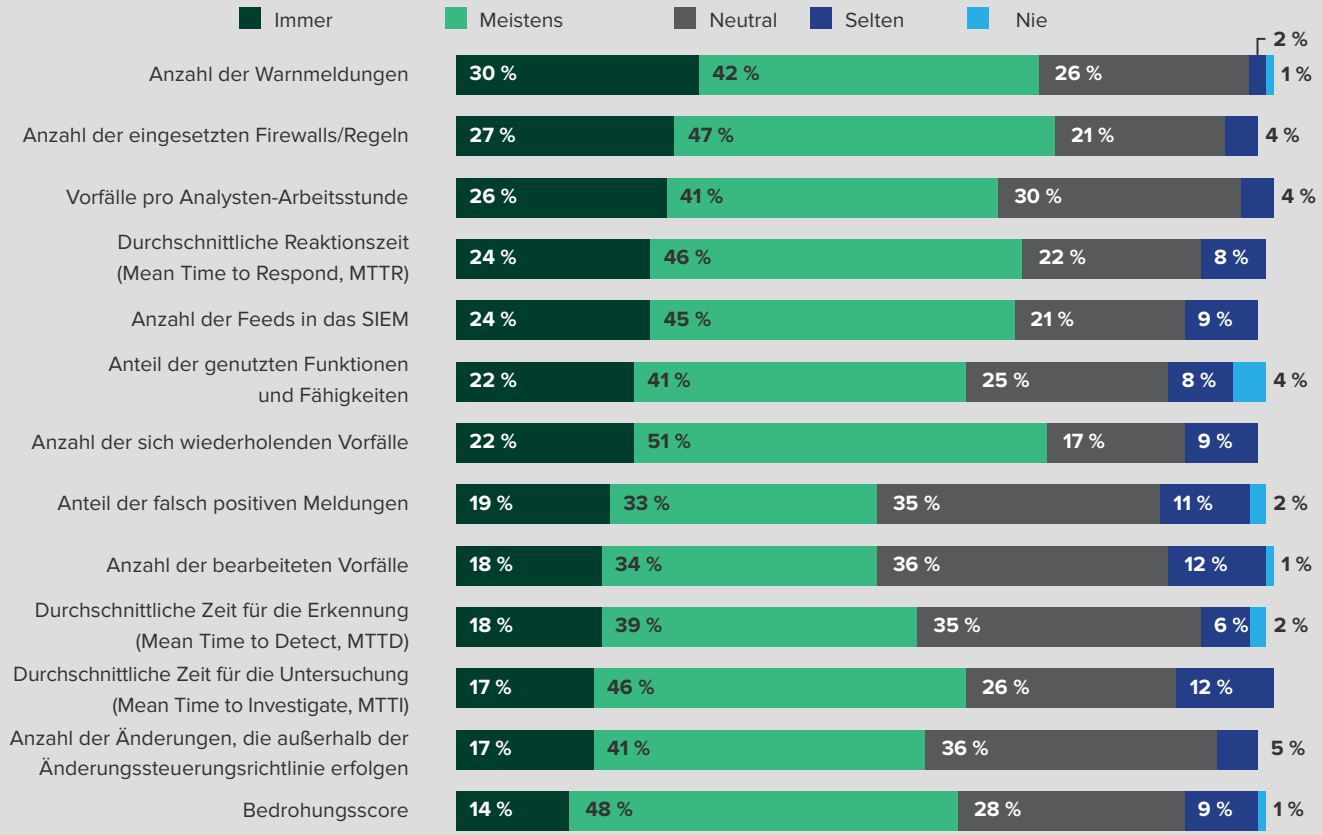
Die aktuelle Situation muss sich grundlegend ändern. Analysten fühlen sich überarbeitet, Unternehmen sind immer häufiger von Sicherheitsverletzungen betroffen und Führungskräfte sind frustriert. Fast 50 % der Befragten gaben an, dass sie nur eingeschränkt in der Lage seien, sich stärker um die Suche nach Sicherheitsrisiken zu kümmern, um so die automatisierte Erkennung zu ergänzen. Sie arbeiten eher reaktiv als proaktiv, was vor allem darin begründet liegt, dass sie sich schwer damit tun, ein stabiles Security-Operations-Team zu unterhalten. Gleichzeitig vergeuden ihre Analysten viel Zeit mit der Verfolgung falsch positiver Meldungen und der weitgehend manuellen Ausführung von Prozessen.

Dies alles hat negative Folgen für den Sicherheitsstatus einer Organisation, denn die Teams erfüllen die Erfolgskriterien nur selten. Security-Operations-Teams werden im Schnitt anhand von fünf Hauptkennzahlen bewertet. Dabei sind die verbreitetsten Kennzahlen die mittlere Untersuchungszeit, die Anzahl bearbeiteter Vorfälle, die mittlere Reaktionszeit, der Bedrohungsscore und die Zahl der Warnmeldungen. Allerdings ist noch nicht einmal die Hälfte der Teams in der Lage, die Sollwerte für diese Kennzahlen im Normalfall zu erreichen, und noch weniger Teams gelingt dies grundsätzlich (Abbildung 4).

Noch nicht einmal die Hälfte der Teams ist in der Lage, diese Kennzahlen im Normalfall zu erreichen, und noch weniger Teams gelingt dies grundsätzlich.

Abbildung 4: Security-Operations-Teams können Sollwerte für wichtige Kennzahlen nicht erfüllen

„Wie häufig hat Ihr internes Security-Operations-Team im vergangenen Jahr die Vorgaben für wichtige Kennzahlen erfüllen können?“



Basis: 83–156 globale Entscheidungsträger im Bereich Security Operations, die formelle Kriterien für die Bewertung des Erfolgs ihres Security-Operations-Teams verwenden
Quelle: Eine im Februar 2020 von Forrester Consulting im Auftrag von Palo Alto Networks durchgeführte Studie

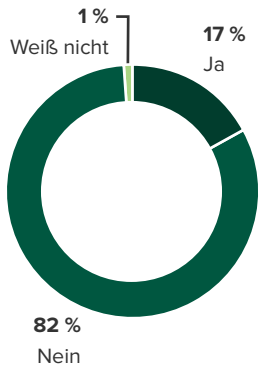
FORRESTER®

- **Unternehmen haben Schwierigkeiten, erfahrene Analysten zu finden und zu binden.** Über 40 % der IT-Entscheidungsträger gaben an, dass sie Probleme haben, erfahrene Mitarbeiter im Bereich Security Operations und genügend Analysten einzustellen, um das Arbeitsaufkommen zu bewältigen. Zudem sagte mehr als ein Drittel der Befragten, dass ihre jeweilige Organisation Schwierigkeiten habe, fähige Mitarbeiter zu halten.
- **Teams verwenden isolierte und schlecht integrierte Tools zur Untersuchung und Behebung von Warnungen.** Die wichtigsten technologischen Herausforderungen, die Entscheidungsträger im Bereich Security Operations daran hindern, Datenschutzverstößen vorzubeugen, sind eine steile Lernkurve bei den vorhandenen Tools und die mangelnde Integration zwischen Sicherheitstools. Nur 17 % der Warnmeldungen werden automatisch erfasst, sodass die Sicherheitsteams bei der Verwaltung der Meldungen auf Sicherheitstools aus im Schnitt zehn verschiedenen Kategorien zurückgreifen müssen. Tatsächlich verwendet nur ein Viertel der Befragten Verhaltensanalytik, was darauf schließen lässt, dass die Teams keine Bedrohungen ohne bekannte Malwaresignatur erkennen können. Nur 49 % stimmen der Aussage zu, dass die Daten und Informationen aus ihren verschiedenen Sicherheitstools gut integriert sind, und über ein Drittel gibt an, dass die Mitarbeiter sehr viel Zeit mit der Prüfung falsch positiver Meldungen verbringen.
- **Nur wenige Organisationen verfügen über eine Lösung für die Probleme, mit denen sie sich im Sicherheitsbereich konfrontiert sehen.** Lediglich 17 % der Organisationen verfügen gegenwärtig über eine Lösung, die netzwerk-, anwendungs- und endpunktübergreifend effektiv für Transparenz sorgt. Zweck dieser Lösungen ist eine Reaktion auf Bedrohungen unter Verwendung von Analytik und Automatisierung (Abbildung 5). Die meisten Organisationen müssen sich aus den vorhandenen Tools eine Lösung zusammenstückeln, wodurch ein Flickenteppich aus manuellen Prozessen für Analysten entsteht.

Nur 17 % der Warnmeldungen werden automatisch erfasst.

Abbildung 5: Aktuelle Lösungen

„Verfügt Ihre Organisation gegenwärtig über eine Lösung, die netzwerk-, anwendungs- und endpunktübergreifend effektiv für Transparenz sorgt sowie Analytik und Automatisierung einsetzt, um auf Bedrohungen zu reagieren?“



Basis: 315 globale Entscheidungsträger im Bereich Security Operations oder Incident Response
Quelle: Eine im Februar 2020 von Forrester Consulting im Auftrag von Palo Alto Networks durchgeführte Studie

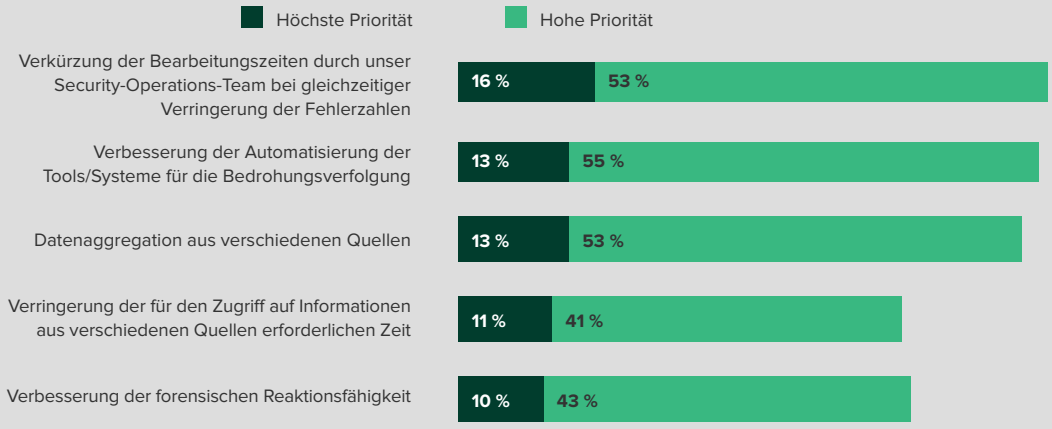
Optimierungsmöglichkeiten im Bereich Security Operations

Die meisten Entscheidungsträger im Bereich Security Operations sind sich der Tatsache bewusst, dass ihre derzeitigen Ansätze zur Erkennung, Untersuchung und Behebung von Bedrohungen erhebliche Mängel aufweisen. Den Führungskräften ist klar, dass sie sich auf die Behebung sowohl kurz- als auch langfristiger Probleme konzentrieren müssen (Abbildung 6), um 2020 ihre wichtigsten Ziele – kürzere Bearbeitungszeiten bei gleichzeitiger Verringerung der Fehlerzahlen und stärkere Automatisierung ihrer Tools und Systeme zur Suche nach Bedrohungen – zu erreichen. Dabei kommt es zu positiven Wechselwirkungen. Die Verbesserung der Effizienz und Transparenz steigert Zufriedenheit und Produktivität der Analysten, wodurch diese für das Unternehmen bessere Ergebnisse im Sicherheitsbereich erzielen und so effizienter arbeiten können.

- **Die meisten Teams schöpfen das Automatisierungspotenzial nicht vollständig aus.** Nur 13 % der Organisationen verwenden Automatisierung oder maschinelles Lernen (ML) für den gesamten Lebenszyklus einer Warnmeldung (Triage, Analyse, Reaktion). 17 % setzen Automatisierung/ML dagegen überhaupt nicht ein.
- **XDR (Extended Detection and Response) wird als Lösung angesehen, die der Ermüdung der Analysten und der Ineffizienz der Tools entgegenwirken und für die Sicherheitsergebnisse insgesamt hilfreich sein kann.** Bei XDR handelt es sich um eine Anzahl von Funktionen, die Daten aus verschiedenen Quellen – Netzwerk, Endpunkte und Anwendungsstacks – aggregieren, um Erkennung und Reaktion zu verbessern. Insgesamt lassen sich mit XDR-Lösungen viele der größten Herausforderungen angehen, mit denen Analysten und Security-Operations-Teams konfrontiert sind. XDR integriert Datenquellen und Funktionen isolierter Tools, sodass Unternehmen auf allen Geräten − ob verwaltet oder nicht − und bei allen Datenquellen Bedrohungen erkennen und darauf reagieren können. Dies vermittelt Sicherheitsteams mehr Transparenz und verbessert die Effizienz von Analysten. Hierdurch nehmen Zufriedenheit und Produktivität der Analysten zu, wodurch die Sicherheit für die Organisationen optimiert wird.

Abbildung 6: Eine höhere Geschwindigkeit und stärkere Automatisierung sind die wichtigsten Ziele für die nächsten 12 Monate

„Welchen der folgenden Verbesserungen im Bereich Security Operations räumt Ihre Organisation für die nächsten 12 Monate Priorität ein?“



Basis: 315 globale Entscheidungsträger im Bereich Security Operations oder Incident Response
Quelle: Eine im Februar 2020 von Forrester Consulting im Auftrag von Palo Alto Networks durchgeführte Studie

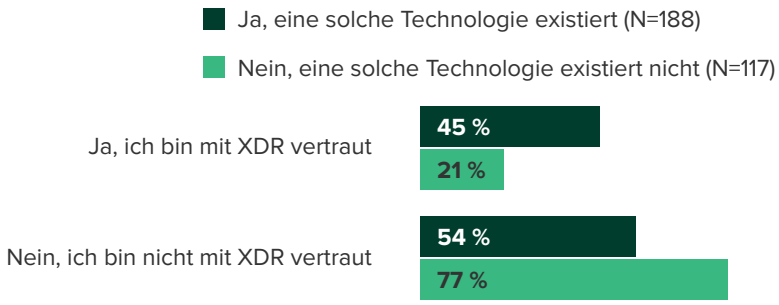
FORRESTER®

- **Entscheidungsträger, die mit XDR vertraut sind, sind doppelt so häufig der Meinung, dass es eine Sicherheitstechnologie gibt, die ihre Anforderungen erfüllt.** Von denen, die mit XDR vertraut sind, glauben 45 %, dass derzeit eine Technologie auf dem Markt verfügbar ist, die ihre Anforderungen im Bereich Security Operations erfüllen würde. Verglichen damit sind 21 % nicht davon überzeugt, dass eine solche Technologielösung existiert (Abbildung 7).
- **Diejenigen, die in die Verbesserung ihrer Technologien für die Erkennung von Verstößen und die Einleitung von Gegenmaßnahmen investieren, erwarten einen erheblichen Nutzen.** Die Befragten gehen davon aus, dass bessere Funktionen für die Erkennung von Verstößen und die entsprechende Reaktion die Produktivität ihrer weniger erfahrenen Analysten steigern, die quellenübergreifende Transparenz verstärken und eine schnellere Identifizierung von Bedrohungen gestatten sowie die Zahl der falsch positiven Meldungen senken, mit deren Verfolgung Analysten Zeit vergeuden.

Abbildung 7: Kenntnis von XDR sorgt für Vertrauen in Technologielösungen

„Wissen Sie, was die XDR-Technologie ist?“

„Sind Ihrer Meinung nach derzeit Technologien verfügbar, die Ihre Anforderungen im Bereich Security Operations erfüllen?“



Basis: 305 globale Entscheidungsträger im Bereich Security Operations oder Incident Response
Quelle: Eine im Februar 2020 von Forrester Consulting im Auftrag von Palo Alto Networks durchgeführte Studie

Diejenigen, die mit der XDR-Technologie vertraut sind, sind doppelt so häufig der Meinung, dass derzeit eine Technologie existiert, die ihre Anforderungen im Bereich Security Operations erfüllen kann.

Wichtige Empfehlungen

Sicherheitsteams benötigen eine einheitliche Sicht auf die in ihrer Organisation eingesetzten Technologien zur Bedrohungsabwehr, um die Mitarbeiter, Prozesse und Technologien innerhalb der Organisation auf das alleinige Ziel der Verteidigung dieser Organisation auszurichten. Es hat sich gezeigt, dass Organisationen, die mit dem XDR-Konzept vertraut sind, davon überzeugt sind, dass dies die geeignete Lösung zur Bewältigung der größten Herausforderungen ist.

Die von Forrester durchgeführte Befragung von 315 IT-Entscheidungsträgern aus aller Welt zum Thema Security-Operations-Teams ergab eine Reihe wichtiger Empfehlungen:

Die Transparenz sollte mit einer vereinheitlichenden Technologie, die Daten aus verschiedenen Quellen nahtlos integriert, verbessert werden. Organisationen müssen dafür sorgen, dass Daten netzwerk-, anwendungs- und endpunktübergreifend in einem einzigen skalierbaren Data Lake aggregiert werden können, um eine effektivere Verfolgung und Erkennung zu ermöglichen.

Security-Analytics-Funktionen wie maschinelles Lernen sollten genutzt werden, um nachvollziehbare Muster für die Erkennung herauszukristallisieren. Viele SOCs reagieren in erster Linie auf Warnmeldungen. Die Korrelation dieser Vorfälle bietet die Möglichkeit, Warnmeldungen mit geringer Zuverlässigkeit, die zunächst möglicherweise ignoriert oder übersehen worden waren, beim zweiten oder dritten Mal genauer zu prüfen.

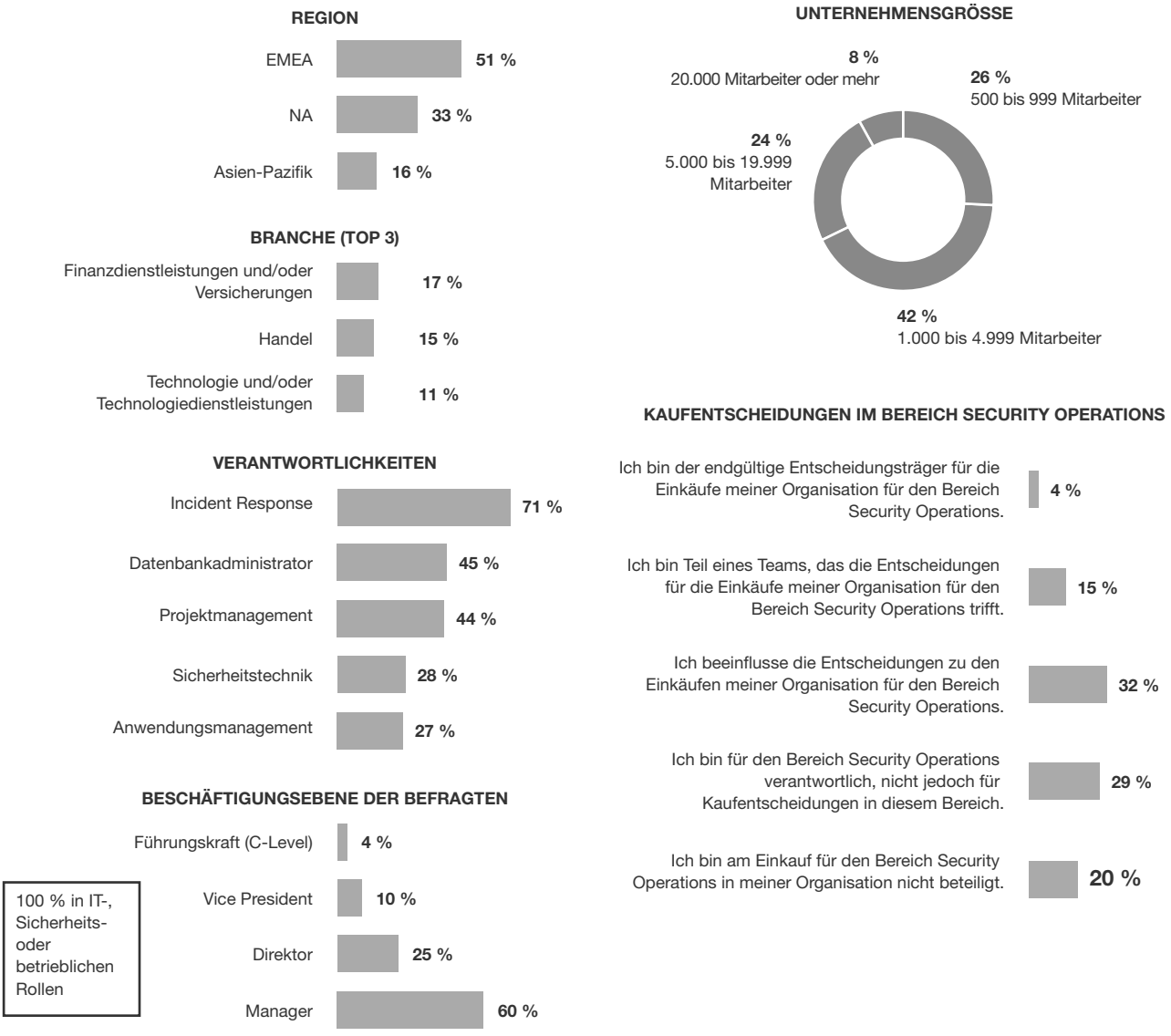
Es sollte in Funktionen investiert werden, die die Ursachenanalyse automatisieren. Die Dauer der Triage im SOC kann mit ausgereiften Analytics-Funktionen verkürzt werden, die miteinander verbundene Vorfälle sichtbar machen und die Untersuchung automatisieren. Die Korrelation dieser Vorfälle bietet die Möglichkeit, frühere Warnmeldungen mit niedrigerem Konfidenzwert, die zuvor möglicherweise ignoriert oder übersehen worden waren, noch ein zweites oder gar drittes Mal unter die Lupe zu nehmen.

FORRESTER®

Anhang A: Methodik

Für diese Studie führte Forrester eine Onlinebefragung von 315 IT-Entscheidungsträgern durch, um deren aktuelle Ansätze für die Verwaltung des Bereichs Security Operations in ihrer Organisation zu bewerten. Die Befragten waren Entscheidungsträger in den Bereichen IT, Sicherheit und Betrieb, die direkt mit Security Operations und/oder Incident Response zu tun haben. Die Mitwirkenden erhielten zum Dank für ihre Teilnahme an der Befragung eine kleine Anerkennung. Die Studie wurde im Februar und März 2020 durchgeführt.

Anhang B: Demografie/Daten



Basis: 315 globale Entscheidungsträger im Bereich Security Operations oder Incident Response
Quelle: Eine im Februar 2020 von Forrester Consulting im Auftrag von Palo Alto Networks durchgeführte Studie

Anhang C: Anmerkungen

[1] Quelle: „Your Guide To Cyberinsurance“, Forrester Research, Inc., 6. Juni 2018.

[2] Quelle: „Planning For Failure: How To Survive A Breach,“ Forrester Research, Inc., 6. Juli 2018.

FORRESTER®