Enterprise Strategy Group | Getting to the bigger truth.™

SOC Modernisierung und die Rolle von XDR

Jon Oltsik, Leitender Analyst, ESG Fellow
Dave Gruber, Hauptanalyst

JUNI 2022

Forschungsziele

Sicherheitsoperationen erfordern eine massive Skalierung, um riesige Datenmengen zu sammeln, zu verarbeiten, zu analysieren und darauf zu reagieren. In den Anfängen von XDR gab es zwei primäre Datenquellen: Endpoints und Netzwerke. Das war zwar eine Verbesserung gegenüber nicht verbundenen EDR- und NDR-Tools, aber die Erkennung und Reaktion auf Bedrohungen in Unternehmen erfordert einen breiteren Ansatz, der auch Cloud-Workloads, Threat-Intelligence-Feeds, SaaS-Anwendungen und die Transparenz des Identitäts- und Zugriffsmanagements einschließt. Gleichzeitig benötigen große Unternehmen zur Modernisierung ihrer Security Operations Center und zur Bewältigung des Volumens an Sicherheitswarnungen fortschrittliche Analysen, um die Aufgaben der Tier-1-Analysten zu automatisieren, z. B. die Einstufung von Warnmeldungen, die Korrelation von Warnmeldungen mit IoCs und die Vorbereitung von Vorfällen für Untersuchungen.

Um einen Einblick in diese Trends zu erhalten, befragte ESG 376 IT- und Cybersicherheitsexperten in nordamerikanischen Unternehmen (USA und Kanada), die persönlich für die Bewertung, den Kauf und die Nutzung von Sicherheitsprodukten und -Services zur Erkennung und Abwehr von Bedrohungen verantwortlich sind.

ZIEL DIESER STUDIE WAR ES:

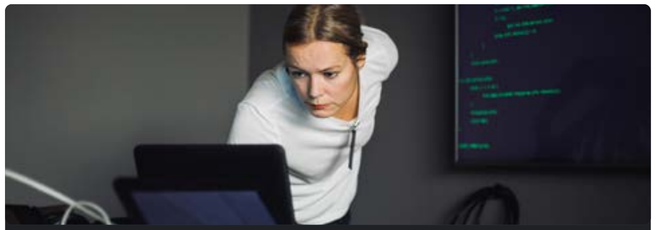
- Menschen, Prozesse und Technologien zu untersuchen, die die Modernisierung der Sicherheitsabläufe unterstützen.
- Die wichtigsten Punkte, die Messgrößen für diese Punkte und die Erwartungen an Produkte und Managed Services für XDR- und SOC-Modernisierung zu identifizieren.
- Ermittlung der aktuellen Wahrnehmung und der Rolle von XDR als Bestandteil der Modernisierungsbemühungen bei Sicherheitsoperationen.
- Mehr über die Strategien zur Automatisierung der Triage, zur Beschleunigung von Untersuchungen und zur Unterstützung von Unternehmen bei der Suche nach unbekannten Bedrohungen zu erfahren.

WESENTLICHE KENNTNISSE

KLICKEN SIE FÜR WEITERE INFOS

Die Sicherheitsmaßnahmen bleiben eine Herausforderung

Die zunehmenden Schwierigkeiten sind auf die wachsende Angriffsfläche, die gefährliche Bedrohungslandschaft und die zunehmende Nutzung von Cloud Computing zurückzuführen.



Sicherheitsexperten wollen mehr Daten und bessere Erkennungsregeln

Trotz der riesigen Menge an Sicherheitsdaten, die bereits verwendet werden, werden mehr und bessere Erkennungsregeln benötigt.

Die Investitionen in die SecOps-Prozessautomatisierung erweisen sich als wertvoll

Obwohl die Umsetzungsstrategien unterschiedlich sind, zahlen sich die Investitionen in die Automatisierung fast immer aus.

Das MITRE ATT&CK-Framework erweist sich für die meisten als nützlich

Viele sind jedoch noch dabei herauszufinden, wie und wo sie ihn einsetzen können, um einen Mehrwert zu erzielen.

Die Dynamik von XDR nimmt weiter zu

Auch wenn oftmals nicht ganz klar ist, was XDR ist, sind die Investitionen in die Erkennung von "Advanced Threats" erheblich.

MDR ist Mainstream und expandiert weiter

Obwohl die Anwendungsfälle unterschiedlich sind, werden MDR Services von Unternehmen aller Größen und Reifegrade in großem Umfang genutzt.

Zurück zum Inhaltsverzeichnis

Die Sicherheitsmaßnahmen bleiben eine Herausforderung.

In den letzten Jahren sind die Sicherheitsmaßnahmen in den meisten Unternehmen schwieriger geworden. Mehr als die Hälfte (52 %) der Befragten ist der Meinung, dass die Sicherheitsumgebung ihres Unternehmens in den letzten zwei Jahren schwieriger zu verwalten geworden ist. Dies ist auf Faktoren wie die zunehmend gefährliche Bedrohungslandschaft, eine wachsende Angriffsfläche, das Volumen und die Komplexität von Sicherheitswarnungen und die Verbreitung der öffentlichen Cloud zurückzuführen. Da diese Herausforderungen in Zukunft nur noch zunehmen werden, erkennen viele CISOs, dass die derzeitigen SOC-Strategien unzureichend sind. Um das wachsende Bedrohungsvolumen und die Ausdehnung der IT zu bewältigen, haben Unternehmen mehrere Initiativen zur SOC-Modernisierung gestartet.

52 %

der Unternehmen sind der Meinung, dass Sicherheitsmaßnahmen heute schwieriger sind als noch vor zwei Jahren.

Sicherheitsoperationen sind heute schwieriger als noch vor zwei Jahren, denn:

Die Bedrohungslandschaft wächst und verändert sich schnell

41 %

Die Angriffsfläche hat sich vergrößert

40 %

Die Angriffsfläche verändert sich ständig und entwickelt sich weiter

39 %

Der Umfang und die Komplexität von Sicherheitswarnungen haben zugenommen

37 %

Die Nutzung von öffentlichen Cloud-Diensten hat zugenommen

34 %

> “Die Unternehmen haben mehrere Initiativen **zur SOC-Modernisierung gestartet.”**

Zurück zum Inhaltsverzeichnis

Der globale Fachkräftemangel wirkt sich auf die Sicherheitsprozesse aus

Zusätzlich zu den allgemeinen Herausforderungen im Bereich der Sicherheitsabläufe ist es erwähnenswert, dass 81 % der Unternehmen der Meinung sind, dass die Sicherheitsabläufe durch den weltweiten Mangel an Fachkräften im Bereich der Cybersicherheit beeinträchtigt wurden. Das führt in der Regel zu einer zunehmenden Arbeitsbelastung des vorhandenen Personals sowie zu Personalabwanderung und Burnout. Sicherheitsexperten weisen auf mehrere Bereiche hin, in denen es besonders an Personal und Fähigkeiten mangelt, darunter Sicherheitsarchitekten, Sicherheitsingenieure, Tier-3-Analysten und Analysten für Schwachstellenbewertung/Priorisierung.

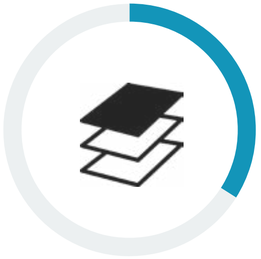
81 %

der Unternehmen sind sich einig, dass ihre Sicherheitsabläufe **durch den Mangel an Fachkräften im Bereich der Cybersicherheit beeinträchtigt wurden.**

Die am stärksten unterbesetzten Bereiche der Sicherheitsoperationen

Sicherheitsarchitekt
37 %

Sicherheitstechniker
35 %



Tier-3 Analysten*
34 %

Analysten, die Schwachstellen bewerten und Prioritäten setzen
33 %

** d. h. ähnlich wie Tier-2-Analysten, aber erfahrener und auf schwierige/kritische Fragen konzentriert.*

Zurück zum Inhaltsverzeichnis

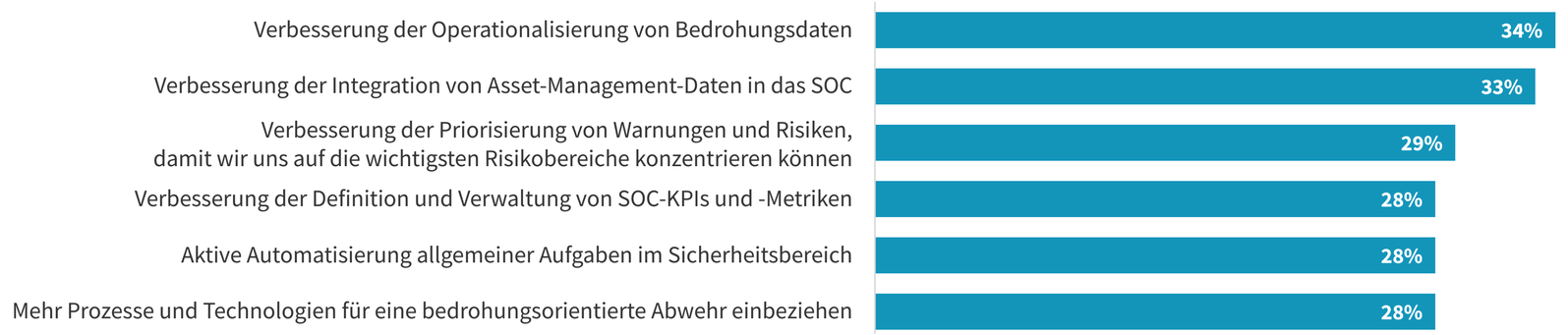
Kurzfristige Prioritäten für die SOC-Modernisierung

Wie planen Unternehmen, mit immer schwierigeren Sicherheitsumgebungen, einschließlich unzureichender Personalausstattung, umzugehen? Die SOC-Modernisierung ist eine der wichtigsten Programminitiativen. 88 % der Unternehmen erhöhen in diesem Jahr ihre Ausgaben für den Sicherheitsbetrieb. In naher Zukunft wollen SOC-Teams ihre Bemühungen auf Bereiche wie die Verbesserung der Operationalisierung von Bedrohungsdaten, die Verbesserung der Integration von Asset-Management-Daten in das SOC, die Verbesserung der Risiko- und Warnpriorisierung, die Verbesserung der Definition und Verwaltung von SOC-KPIs und die Automatisierung allgemeiner Sicherheitsaufgaben konzentrieren.

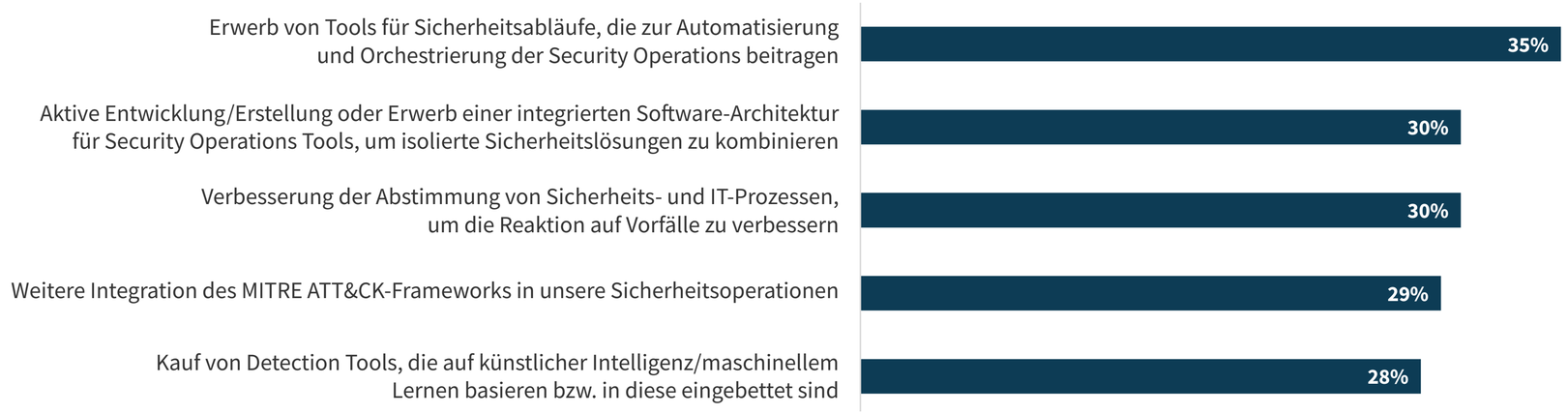
In Zukunft werden Unternehmen viele weitere Schritte zur SOC-Modernisierung unternehmen, wie z. B. die Anschaffung von Tools zur Automatisierung von Sicherheitsprozessen, die Entwicklung/den Aufbau einer integrierten Plattformarchitektur für Sicherheitsabläufe und Analysen (SOAPA), die Verbesserung der Abstimmung von Sicherheits- und IT-Abläufen, die weitere Integration des MITRE ATT&CK-Frameworks in die Sicherheitsabläufe und die Anschaffung fortschrittlicher Analysetools zur Erkennung von Bedrohungen.

Diese Fortschritte werden Zeit brauchen und möglicherweise die Unterstützung von Sicherheitsdiensten erfordern. Dennoch sollten sie als Zwischenstationen auf dem Weg zur Modernisierung der SOC betrachtet werden. Ziel ist es, ein SOC zu schaffen, das den Umfang, die Leistung, die Intelligenz, die Automatisierung und die Verwaltbarkeit bietet, um Bedrohungen zu verhindern, zu erkennen und auf sie zu reagieren, Risiken zu verwalten und die Kernaufgaben des Unternehmens zu unterstützen.

Erwartete SOC-bezogene Ziele für die nächsten 12 Monate



Voraussichtliche Maßnahmen zur Verbesserung der Sicherheitsmaßnahmen in den nächsten 12-18 Monaten



Zurück zum Inhaltsverzeichnis

Sicherheitsexperten wollen mehr Daten und bessere Erkennungsregeln

Trotz der Umstellung auf XDR sind Daten der Endpoints immer noch am wertvollsten

Acht von zehn Unternehmen sammeln, verarbeiten und analysieren Daten zu Sicherheitsvorgängen aus mehr als zehn Datenquellen. Sicherheitsexperten sind der Meinung, dass die wichtigsten Quellen Sicherheitsdaten der Endpoints, Threat Intelligence Feeds, Geräteprotokolle, Cloud Posture Management-Daten und Network Flow Logs sind. Dies scheint zwar eine Menge an Daten zu sein, aber die Befragten wollen tatsächlich mehr Daten für Security Operations nutzen, was den Bedarf an skalierbaren, leistungsstarken, Cloud-basierten Back-End-Datenspeichern erhöht.

80 %

der Unternehmen nutzen mehr als 10 Datenquellen im Rahmen von Sicherheitsmaßnahmen.

> Die Befragten wollen **tatsächlich mehr Daten für Sicherheitsmaßnahmen nutzen.”**

Wichtigste Datenquellen für Sicherheitsoperationen

24 %

Datenblatt: Endpoint Security

21 %

Feeds zu Bedrohungsdaten

20 %

Protokolldaten von Sicherheitsgeräten

20 %

Systeme zur Verwaltung der Sicherheitslage in der Cloud

18 %

NetFlow- und/oder IPFIX-Daten und/oder VPC-Flow-Protokolle

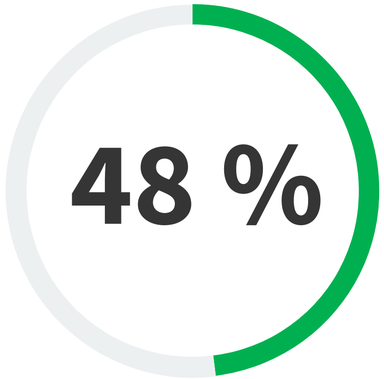
Zurück zum Inhaltsverzeichnis

Die meisten Unternehmen entwickeln ihre eigenen Erkennungsregeln.

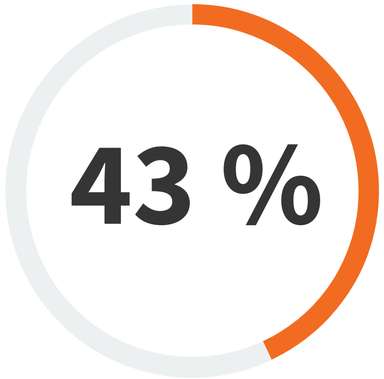
Während die Anbieter immer mehr fertige Inhalte für die Erkennung von Bedrohungen bereitstellen, ergänzen 91 % der Unternehmen diese Bemühungen durch eigene Erkennungstechniken. SOC-Teams sammeln, verarbeiten und analysieren eine Vielzahl von Sicherheitstelemetrien, um Schwachstellen in der Erkennung zu ermitteln, für die individuelle Regeln erforderlich sind. Sicherheitsteams passen die Regelsätze der Anbieter an ihre Bedürfnisse an und entwickeln eigene Regeln, um Bedrohungen zu erkennen, die auf ihre Branche oder ihr Unternehmen abzielen. Um diesen Trend zu unterstützen, müssen die Anbieter die Zusammenarbeit der Benutzernetzwerke erleichtern und gleichzeitig offene Standards wie Sigma und YARA einbeziehen.

Umfang der benutzerdefinierten Regeln zur Erkennung von Bedrohungen

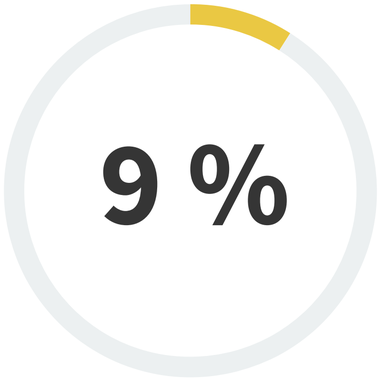
Mein Unternehmen entwickelt eine beträchtliche Anzahl von benutzerdefinierten Regeln, um die von den Anbietern bereitgestellten Erkennungsregeln zu ergänzen.



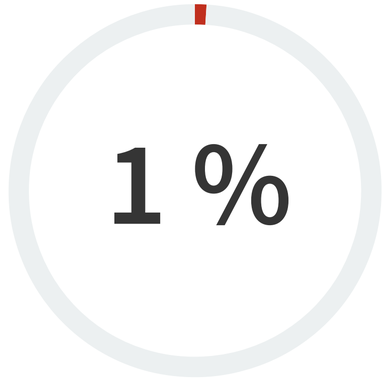
Mein Unternehmen entwickelt einige benutzerdefinierte Regeln, um die von den Anbietern bereitgestellten Erkennungsregeln zu ergänzen.



Mein Unternehmen kann eine kleine Anzahl von benutzerdefinierten Erkennungsregeln entwickeln, verlässt sich aber hauptsächlich auf die von Anbietern bereitgestellten Regeln.



Mein Unternehmen entwickelt keine benutzerdefinierten Erkennungsregeln und verlässt sich vollständig auf die von den Anbietern bereitgestellten Regeln.



Zurück zum Inhaltsverzeichnis

Die Investitionen in die SecOps-Prozessautomatisierung erweisen sich als wertvoll.

Viele Unternehmen haben die Vorteile der Automatisierung von Sicherheitsprozessen erkannt, aber es gibt noch Herausforderungen.

Die Automatisierung von Sicherheitsprozessen ist sehr beliebt, wie die 90 % der Unternehmen zeigen, die derzeit ihre Sicherheitsprozesse automatisieren. 46 % bezeichnen ihre Automatisierungsbemühungen als umfassend. Diejenigen, die Sicherheitsprozesse automatisieren, berichten von Vorteilen wie verbesserter Erkennung von Bedrohungen mithilfe von Playbooks, MTTR und Priorisierung von Vorfällen sowie der Möglichkeit, infizierte Ressourcen schneller zu isolieren. Angesichts der Herausforderungen im Bereich der Security Operations, wie der wachsenden Angriffsfläche, der "Alert Storms" und der gefährlichen Bedrohungslandschaft, wird die Automatisierung von Sicherheitsprozessen weitergehen und wahrscheinlich mit der Automatisierung von IT-Prozessen verschmelzen, um so die Effizienz von IT und IT Security zu steigern.

Die Automatisierung von Sicherheitsprozessen ist zwar nach wie vor beliebt und vorteilhaft, bringt aber auch einige Herausforderungen mit sich. Fast zwei von fünf Unternehmen (39 %) geben an, dass ihr Sicherheitsteam nicht über die richtigen Programmierkenntnisse verfügt, um Runbooks/Workflows in SOAR-Tools zu entwickeln. 21 % sagen, dass ihre Sicherheitsprozesse unausgereift sind und neu entwickelt werden müssen, bevor sie automatisiert werden können. In diesen Fällen müssen die Unternehmen die Prozessabläufe besser bewerten und nach Engpässen suchen, bevor sie zur Automatisierung übergehen. Diejenigen, die nur über begrenzte Programmierkenntnisse verfügen, sollten sogenannte Low Code/No Code SOAR-Optionen in Betracht ziehen oder die in andere Betriebs-Tools integrierten Funktionen zur Prozessautomatisierung nutzen.

Die am häufigsten realisierten Vorteile der Automatisierung von Sicherheitsprozessen

Verbesserte Erkennung von Bedrohungen durch Playbooks

51 %

Verbesserte durchschnittliche Zeit bis zur Antwort

49 %

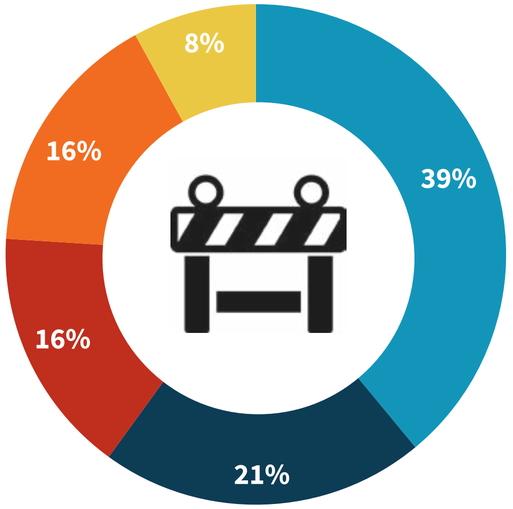
Verbesserte Priorisierung von Vorfällen

44 %

Schnellere Isolierung infizierter Objekte

44 %

Die größten Hindernisse für die Automatisierung von Security Operations



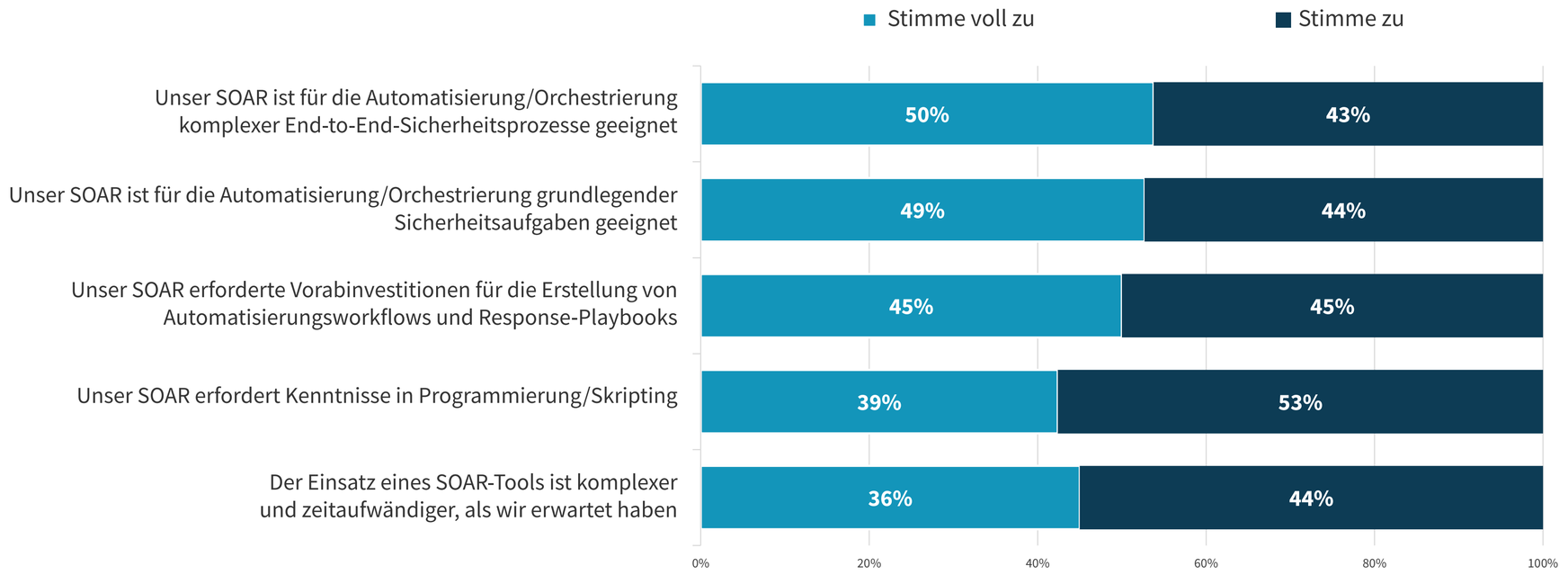
- Kenntnisse in der Software-Entwicklung: Unser Sicherheitsteam verfügt nicht über die Programmierkenntnisse, um Runbooks/ Workflows zu entwickeln.
- Unausgereifte Prozesse: Unsere Sicherheitsprozesse sind relativ unausgereift, so dass wir sie erst überarbeiten müssten, bevor wir mit der Prozessautomatisierung beginnen.
- Zeit: Das Sicherheitsteam hat nicht genügend Zeit, um an der Prozessautomatisierung zu arbeiten.
- Tools: Unser Unternehmen verfügt nicht über Technologien wie SOAR, die für die Automatisierung von Sicherheitsprozessen erforderlich sind.
- Keine Hinderungsgründe

Zurück zum Inhaltsverzeichnis

SOAR-Tools können mit den richtigen Vorabinvestitionen und -erwartungen zu Ergebnissen führen.

Mehr als ein Viertel (29 %) der Unternehmen verwendet eine Art von SOAR-Tool (Security Orchestration, Automation and Response) zur Prozessautomatisierung. Der Einsatz von SOAR kann sich als vorteilhaft erweisen: 93 % der Sicherheitsexperten sind der Meinung, dass ihr SOAR für die Automatisierung komplexer End-to-End-Sicherheitsprozesse und für die Automatisierung/Orchestrierung grundlegender Sicherheitsaufgaben effektiv ist. SOAR gibt es allerdings nicht umsonst. Der Erfolg hängt von einer gewissen Vorausplanung, Investitionen und den richtigen Fähigkeiten ab. So geben beispielsweise 90 % der Sicherheitsexperten an, dass SOAR Vorabinvestitionen für die Erstellung von Automatisierungsworkflows und Reaktions-Playbooks erfordert. 92 % stimmen zu, dass SOAR Programmier-/Skripting-Kenntnisse erfordert und 80 % stimmen zu, dass die Verwendung eines SOAR-Tools komplexer und zeitaufwändiger ist als erwartet. Auf der Grundlage dieser Daten sollten Unternehmen erkennen, dass SOAR als Projekt und nicht als Allheilmittel betrachtet werden sollte. Die Vorteile von SOAR können nur mit dem richtigen Maß an Planung, Schulung und Projektmanagement erreicht werden.

Die Stimmung für SOAR-Tools (Security Orchestration, Automation and Response)



> “Der Einsatz von SOAR kann von Vorteil sein.”

Zurück zum Inhaltsverzeichnis

Das MITRE ATT&CK-Framework erweist sich für die meisten als nützlich.

Die meisten Unternehmen nutzen das MITRE ATT&CK-Framework für Sicherheitsoperationen und sehen darin einen Nutzen

Das MITRE ATT&CK-Framework erfreut sich zunehmender Beliebtheit, so dass heute fast neun von zehn Unternehmen es in gewissem Umfang nutzen. Wenn die SOC-Manager in die Zukunft blicken, sehen sie eine noch stärkere Nutzung von MITRE. Tatsächlich sind 97 % der Sicherheitsexperten der Meinung, dass MITRE ATT&CK (und daraus abgeleitete Projekte) für die Sicherheitsstrategie ihres Unternehmens entscheidend, sehr wichtig oder wichtig sein wird.

Verwendung des MITRE ATT&CK-Frameworks für Sicherheitsoperationen

Verwenden Unternehmen das MITRE ATT&CK-Framework für Sicherheitsoperationen?

Die Bedeutung des MITRE ATT&CK-Frameworks für Sicherheitsoperationen

97 %

der Sicherheitsexperten glauben, dass MITRE ATT&CK (und daraus abgeleitete Projekte) für die Sicherheitsstrategie ihres Unternehmens in begrenztem Umfang entscheidend, sehr wichtig oder wichtig sein wird.

Zurück zum Inhaltsverzeichnis

MITRE ATT&CK Anwendungen florieren

MITRE ATT&CK hat sich auch in einer Reihe von Sicherheitsabläufen bewährt. Von den Unternehmen, die das MITRE ATT&CK-Framework nutzen, setzen es 38 % ein, um Bedrohungsdaten in ihre Alarmtriage oder ihren Ermittlungsprozess einzubeziehen, 37 % nutzen es als Leitfaden für die Sicherheitstechnik. 35 % nutzen MITRE, um die Taktiken, Techniken und Verfahren von Cyberangriffen besser zu verstehen und 34 % nutzen das Framework, um das volle Ausmaß von Angriffen schneller zu erfassen.

Auf diese Weise setzen Unternehmen MITRE ATT&CK in den Bereichen Bedrohungsprävention, -erkennung und -reaktion ein.

Wie Unternehmen das MITRE ATT&CK-Framework nutzen

Damit wir Bedrohungsdaten besser in unsere Warnmeldungen und/oder Ermittlungsverfahren einfließen lassen können

38 %

Als Leitfaden für die Sicherheitstechnik

37 %

Um ein besseres Verständnis der Taktiken, Techniken und Verfahren von Cyberangriffen zu erlangen

35 %

Damit Unternehmen das volle Ausmaß von Angriffen schneller erkennen können

34 %

Um sicherzustellen, dass wir die richtigen Daten aus den richtigen Datenquellen sammeln

33 %

> “MITRE ATT&CK hat sich auch **in einer Reihe von Sicherheitsabläufen bewährt.”**

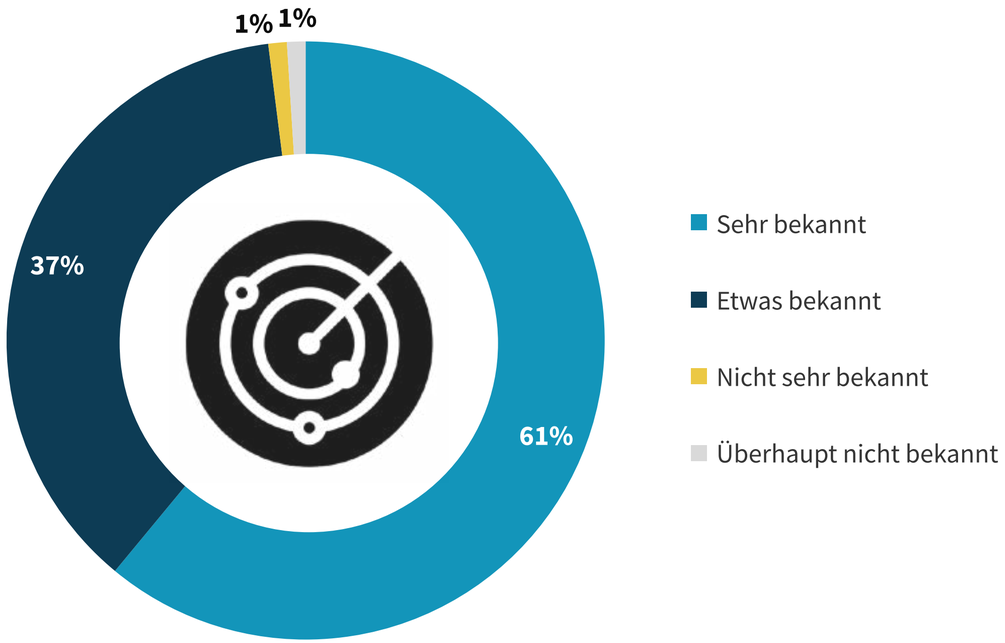
Zurück zum Inhaltsverzeichnis

Die Dynamik von XDR nimmt weiter zu.

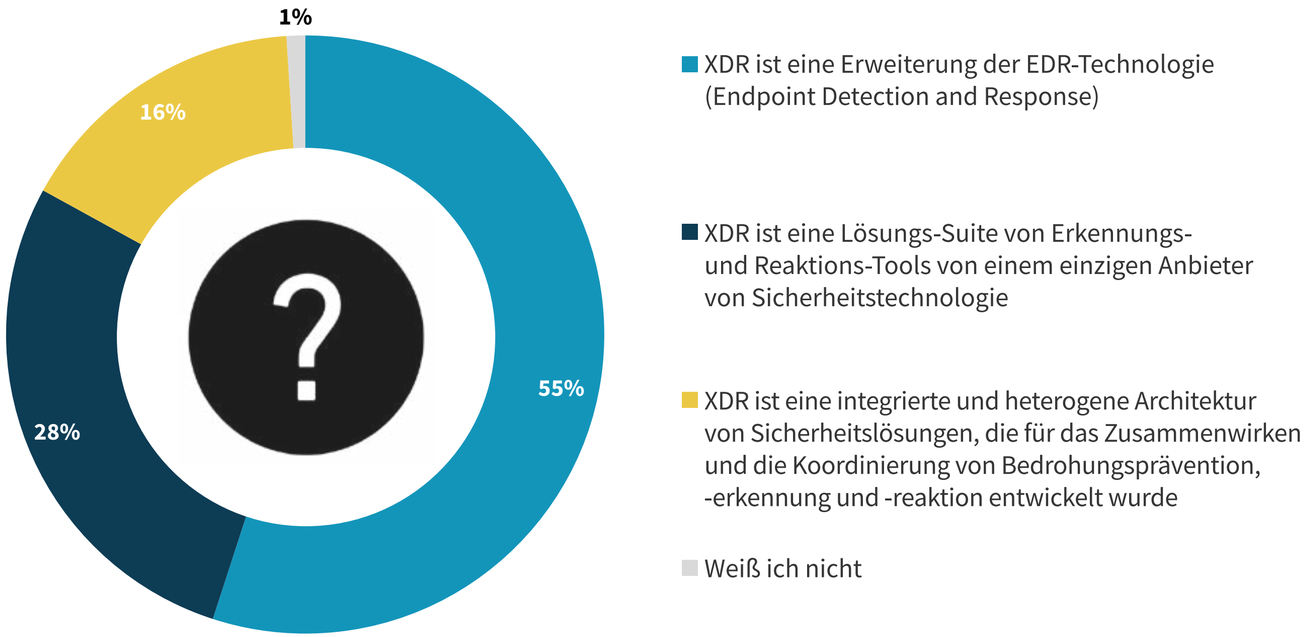
Das Bewusstsein für XDR wächst weiter, obwohl die meisten XDR als Ergänzung oder Konsolidierung von SOC-Technologien sehen.

Obwohl XDR in der Branche immer mehr Beachtung findet, bleibt es ein amorphes Konzept mit unterschiedlichen Komponenten und Definitionen. Das spiegelt sich in der Tatsache wieder, dass 61 % der Sicherheitsexperten angeben, dass sie mit der XDR-Technologie sehr vertraut sind. Das ist zwar eine Verbesserung gegenüber der ESG-Studie aus dem Jahr 2020 (damals waren nur 24 % der Sicherheitsexperten sehr gut mit XDR vertraut), aber 39 % sind immer noch nur einigermaßen, nicht sehr gut oder überhaupt nicht mit XDR vertraut. Die Benutzer sind auch verwirrt darüber, was XDR ist. Während 55 % der Befragten sagen, dass XDR eine Erweiterung von EDR ist, glauben 44 %, dass XDR ein Tool zur Erkennung und Reaktion eines einzigen Sicherheitstechnologieanbieters oder eine integrierte und heterogene Architektur von Sicherheitslösungen ist, die darauf ausgelegt ist, bei der Bedrohungsabwehr, -erkennung und -reaktion zusammenzuarbeiten und sich zu koordinieren. Man kann mit Sicherheit sagen, dass XDR noch ein wenig in der Entwicklung steckt.

Vertrautheit mit der XDR-Technologie



Organisatorische Definitionen der XDR-Technologie



Zurück zum Inhaltsverzeichnis

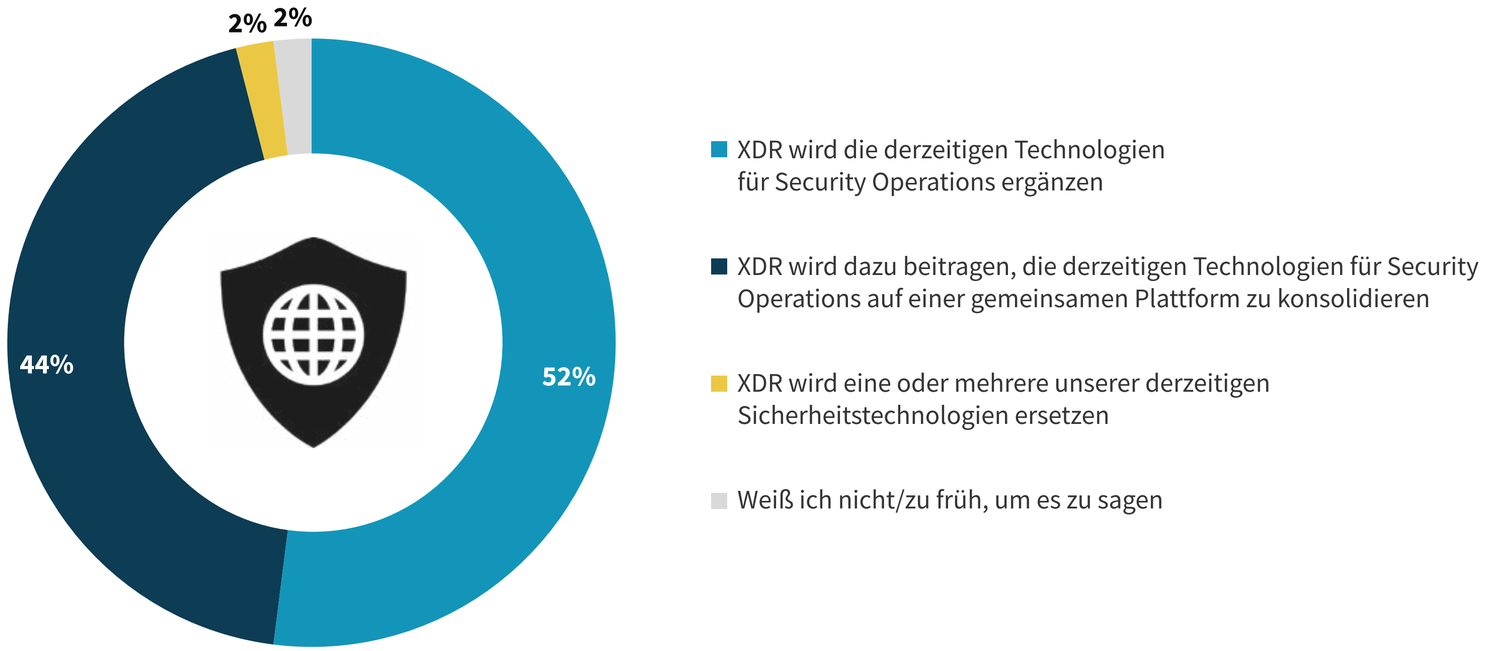
Die meisten sehen XDR als Ergänzung oder Konsolidierung von SOC-Technologien

In diesem Sinne wird XDR zum jetzigen Zeitpunkt nicht als potenzieller Ersatz für SOC-Technologien wie SIEM, SOAR und TIP angesehen. Mehr als die Hälfte (52 %) der Sicherheitsexperten sind der Meinung, dass XDR die vorhandenen Sicherheitstechnologien ergänzen wird, während 44 % der Meinung sind, dass XDR die vorhandenen Sicherheitstechnologien auf einer gemeinsamen Plattform konsolidieren wird. Nur 2 % glauben, dass XDR die derzeitigen Sicherheitstechnologien ersetzen wird.

MEHR ALS DIE HÄLFTE

der Sicherheitsexperten glaubt,
dass XDR die bestehenden Sicherheitstechnologien ergänzen wird.

Erwartete Auswirkung von XDR auf die Umgebung von Security Operations



Zurück zum Inhaltsverzeichnis

Anwender wünschen sich XDR zur Bewältigung allgemeiner Herausforderungen bei der Erkennung von und Reaktion auf Bedrohungen

Unabhängig davon, wie XDR definiert wird, sind Sicherheitsexperten daran interessiert, XDR zu nutzen, um verschiedene Herausforderungen bei der Erkennung von und Reaktion auf Bedrohungen zu bewältigen. XDR scheint eine attraktive Option zu sein, da aktuelle Tools Schwierigkeiten haben, fortschrittlichste Bedrohungen zu erkennen und zu untersuchen, spezielle Fähigkeiten erfordern und nicht in der Lage sind, Warnungen zu korrelieren. Zusammenfassend lässt sich sagen, dass CISOs sich XDR-Tools wünschen, die die Sicherheitseffizienz verbessern können, insbesondere im Hinblick auf die Erkennung fortschrittlichster Bedrohungen. Außerdem soll XDR die Security Operations optimieren und die Produktivität der Mitarbeiter steigern.

Sicherheitsexperten scheinen eine Reihe gängiger XDR-Anwendungsfälle im Kopf zu haben. So wünschen sich beispielsweise 26 % der Sicherheitsexperten, dass XDR dazu beiträgt, Warnungen auf der Grundlage des Risikos nach Prioritäten zu ordnen, 26 % wünschen sich eine verbesserte Erkennung fortschrittlichster Bedrohungen, 25 % wünschen sich effizientere Bedrohungs-/Forensik-Untersuchungen, 25 % wünschen sich eine mehrschichtige Ergänzung zu den bestehenden Tools zur Erkennung von Bedrohungen und 25 % sind der Meinung, dass XDR die Erkennung von Bedrohungen verbessern könnte, um die Sicherheitskontrollen zu verstärken und künftige ähnliche Angriffe zu verhindern. Die Benutzer wollen, dass XDR die Lücken im Sicherheitssystem schließt und gleichzeitig die Wirksamkeit und Effizienz der Bedrohungserkennung und -bekämpfung verbessert.

Die fünf häufigsten Herausforderungen, die das Interesse an XDR wecken

51 %

Derzeitige Tools haben Schwierigkeiten, fortschrittlichste Bedrohungen zu erkennen und zu untersuchen

38 %

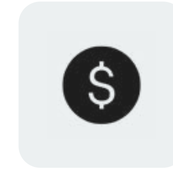
Die derzeitigen Tools erfordern zu viele Spezialkenntnisse

36 %

Derzeitige Tools sind nicht effektiv bei der Korrelation von Warnmeldungen

35 %

Spezifische Lücken bei der Erkennung und Reaktion in der Cloud



32 %

Der derzeitige Einsatz der Tools ist zu teuer

Fünf XDR-Anwendungsfälle mit höchster Priorität

26 %

Eine XDR-Lösung, die helfen könnte, Warnungen auf der Grundlage des Risikos zu priorisieren

26 %

Verbesserte Erkennung der fortschrittlichsten Bedrohungen (Advanced Threats)

25 %

Effizientere Bedrohungs- und forensische Untersuchungen

25 %

Mehrschichtige Ergänzung bestehender Tools zur Erkennung von Bedrohungen helfen dabei, fortschrittlichste und komplexeste Bedrohungen zu identifizieren

25 %

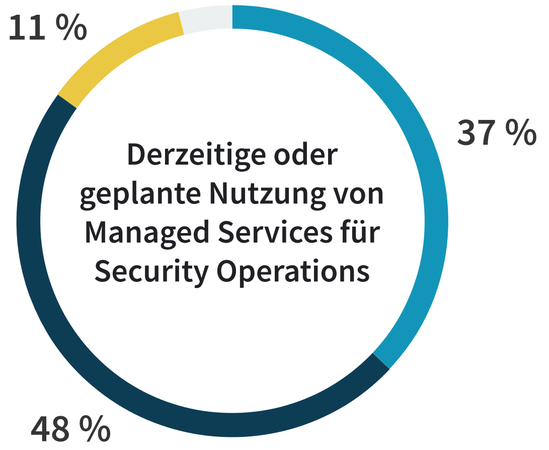
Verbesserte Erkennung von Bedrohungen zur Verstärkung der Sicherheitskontrollen und zur Verhinderung künftiger ähnlicher Angriffe

Zurück zum Inhaltsverzeichnis

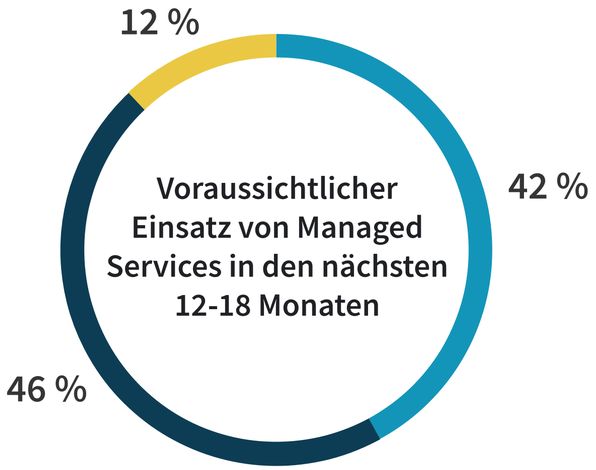
MDR ist Mainstream und expandiert

Die Verwendung von MDR ist Mainstream... und nimmt weiter zu

Unabhängig von Technologiedefinitionen oder Implementierungsstrategien zeigen die Daten von ESG eine nahezu universelle Wahrheit: Unternehmen benötigen für den Sicherheitsbetrieb die Hilfe von Dienstleistern. 85 % der Unternehmen nutzen heute Dienstleister für einen Teil oder die Mehrheit ihrer Security Operations. Und von denjenigen, die Managed Security Services nutzen, werden 88 % in Zukunft noch mehr Managed Security Services einsetzen.



- Wir nutzen MSPs/MSSPs für einen Großteil unserer Security Operations
- Wir nutzen Managed Services für einen Teil unserer Security Operations
- Wir nutzen Managed Services in begrenztem Umfang für Security Operations



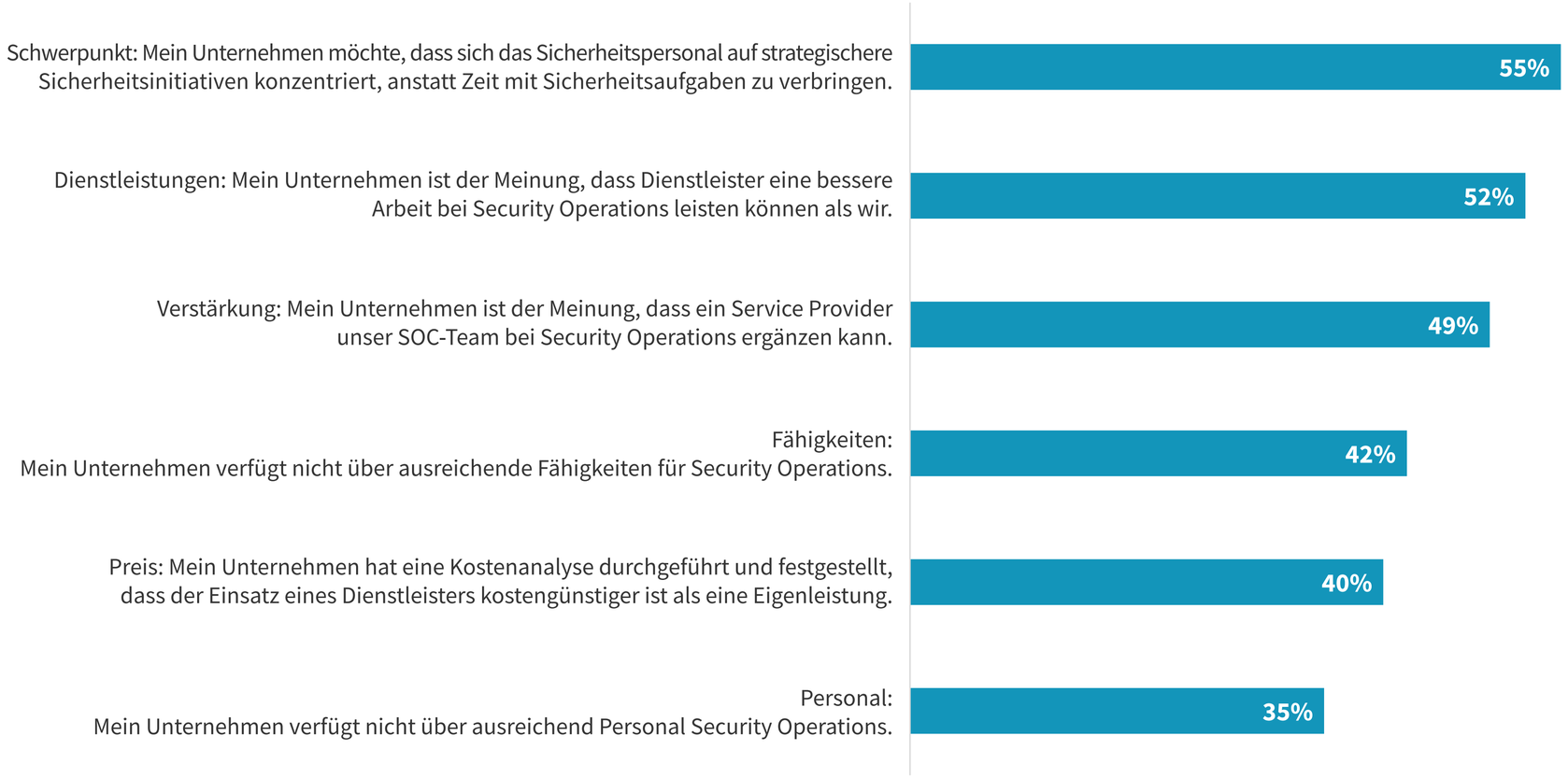
- Wir werden die Nutzung von Managed Services für Security Operations deutlich erhöhen
- Wir werden den Einsatz von Managed Services für Security Operations leicht erhöhen
- Wir werden unsere derzeitige Nutzung von Managed Services für Security Operations beibehalten

Zurück zum Inhaltsverzeichnis

MDR hilft Unternehmen, ihre Sicherheitsanstrengungen zu fokussieren und den Mangel an Fachkräften und Personal zu beheben

Warum brauchen Unternehmen Managed Services für den Sicherheitsbetrieb? Mehr als die Hälfte (55 %) wünschen sich Managed Services, damit sie ihr Sicherheitspersonal auf strategische Sicherheitsinitiativen konzentrieren können. Andere glauben, dass MSPs/MSSPs Dinge leisten können, die ihr Unternehmen selbst nicht kann. 52 % sind der Meinung, dass Dienstleister bessere Sicherheitsabläufe bieten können als ihr Unternehmen, 49 % sagen, dass ein MSP/MSSP ihr SOC-Team verstärken kann und 42 % geben zu, dass ihr Unternehmen nicht über ausreichende Fähigkeiten für Security Operations verfügt.

Hauptgründe für die Nutzung von oder Pläne für Managed Services für Security Operations



Zurück zum Inhaltsverzeichnis

kaspersky

Ein zentraler Partner in Fragen der Cybersicherheit, mit dem Sie die Abwehrmöglichkeiten Ihres Teams mit führenden Technologien auf der Basis von erstklassiger Threat Intelligence, Know-how und fachkundiger Anleitung von angesehenen Branchenexperten optimieren.

MEHR ERFAHREN

ÜBER ESG

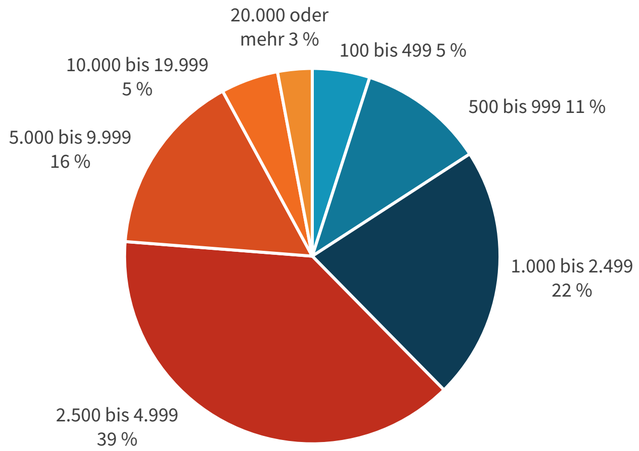
Die Enterprise Strategy Group ist ein integriertes Technologieanalyse-, Forschungs- und Strategieunternehmen, das der globalen Technologiegemeinschaft Marktinformationen, umsetzbare Erkenntnisse und Go-to-Market-Inhaltsdienste bietet.

Forschungsmethodik

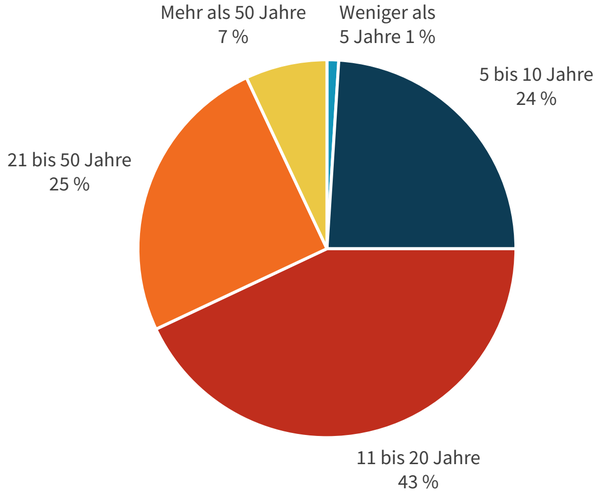
Um Daten für diesen Bericht zu sammeln, führte ESG zwischen dem 4. April 2022 und dem 15. April 2022 eine umfassende Online-Umfrage unter IT- und Cybersicherheitsexperten aus privaten und öffentlichen Unternehmen in Nordamerika durch. Um sich für diese Umfrage zu qualifizieren, mussten die Befragten IT- oder Cybersicherheitsexperten sein, die für die Bewertung, den Kauf und die Nutzung von Sicherheitsprodukten und -dienstleistungen zur Erkennung von und Reaktion auf Bedrohungen verantwortlich sind. Allen Befragten wurde ein Anreiz zur Teilnahme an der Umfrage in Form von Geldprämien und/oder Bargeldäquivalenten geboten.

Nach dem Herausfiltern unqualifizierter Befragter, dem Entfernen doppelter Antworten und dem Screening der verbleibenden ausgefüllten Antworten (anhand einer Reihe von Kriterien) auf Datenintegrität blieb eine endgültige Gesamtstichprobe von 376 IT- und Cybersicherheitsexperten übrig.

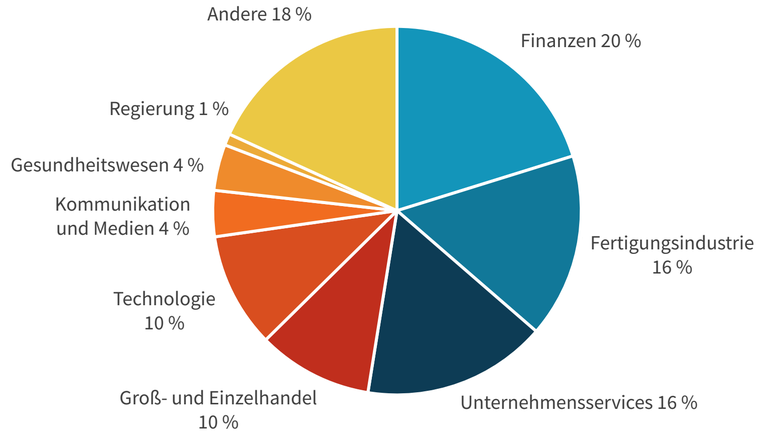
BEFRAGTE NACH ANZAHL DER BESCHÄFTIGTEN



BEFRAGTE NACH ALTER DES UNTERNEHMENS



BEFRAGTE NACH BRANCHE



Zurück zum Inhaltsverzeichnis

Die Enterprise Strategy Group ist ein integriertes Technologieanalyse-, Forschungs- und Strategieunternehmen, das der globalen Technologiegemeinschaft Marktinformationen, umsetzbare Erkenntnisse und Go-to-Market-Inhaltsdienste bietet.