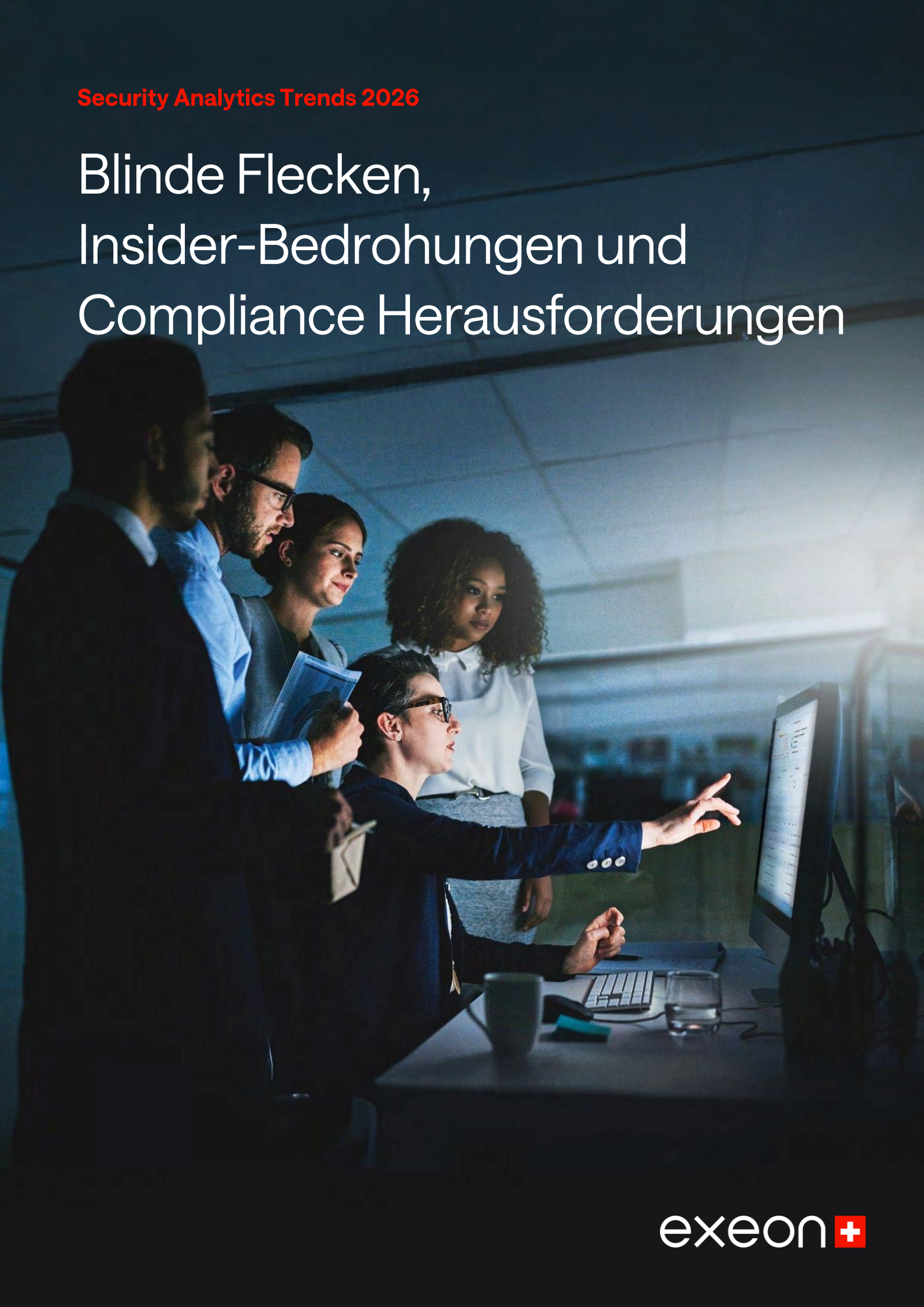
Security Analytics Trends 2026

# Blinde Flecken, Insider-Bedrohungen und Compliance Herausforderungen



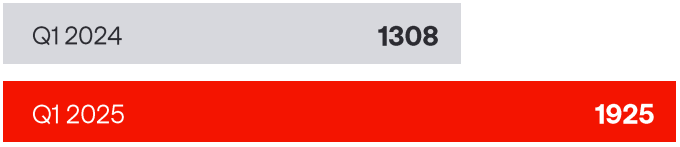
exeon

# Zusammenfassung

## Komplexere Bedrohungen

Cyberangriffe nehmen in Häufigkeit und Raffinesse zu. Anfang 2025 verzeichneten Organisationen durchschnittlich einen **47%igen Anstieg wöchentlicher Cyberangriffe** [1]. Dies unterstreicht den Bedarf an fortschrittlichen Sicherheitsanalysen wie User and Entity Behavior Analytics (UEBA), Identity Threat Detection and Response (ITDR), Network Detection and Response (NDR) und Security Information and Event Management (SIEM)-Lösungen, die subtile Bedrohungen im Rauschen erkennen können. Organisationen in den Bereichen Banking und Finanzdienstleistungen (BFSI), Fertigung, öffentlicher Sektor sowie kritische Infrastruktur wie Energie, Versorgung und Gesundheitswesen überprüfen ihr Sicherheitsmonitoring, da Bedrohungsakteure traditionelle Abwehrmechanismen immer besser umgehen.

**47%** mehr wöchentliche Cyberangriffe pro Organisation




## Shadow IT und Blind Spots

weiter zu Seite 5 →

Vielen Organisationen fehlt die Sichtbarkeit in wesentliche Teile ihrer IT-Umgebung. IT-Abteilungen sind häufig über etwa zwei Drittel der genutzten SaaS-Anwendungen nicht informiert [2], und bis zu 30–40 % der IT-Ausgaben entfallen auf Shadow IT ausserhalb der offiziellen Aufsicht [3]. Eigene geschäftskritische Anwendungen, unverwaltete APIs und Cloud-Dienste fungieren häufig als blinde Flecken – ihre Logs liegen ungenutzt vor oder erreichen das SIEM aufgrund komplexer Formatierungsanforderungen gar nicht. Das Ergebnis ist eine fragmentierte Sichtbarkeit, die Sicherheitsteams im Unklaren lässt, ob sie wirklich alle Bedrohungen erkennen. Tatsächlich glauben **71 % der SOC-Analysten, ihre Organisation könnte bereits ohne ihr Wissen kompromittiert sein** [4].

**71%** der SOC-Analysten glauben, ihre Organisation sei bereits kompromittiert

## Unentdeckte Insider-Bedrohungen

weiter zu Seite 9 →

83% der Organisationen erlebten im vergangenen Jahr einen Insider-Angriff

Insider-Bedrohungen – ob fahrlässige Benutzer, böswillige Insider oder gestohlene Zugangsdaten – sind zu einem der grössten Sicherheitsprobleme geworden. Erschreckende **83 % der Organisationen erlebten im vergangenen Jahr mindestens einen Insider-Angriff** [5], und fast die Hälfte gibt an, dass solche Vorfälle häufiger werden [6]. Dennoch gehen diese Bedrohungen oft in normalen Aktivitäten unter und bleiben unbemerkt: Die durchschnittliche Zeit zur Eindämmung eines Insider-Vorfalls beträgt über 80 Tage [7]. Traditionelle Tools übersehen oft die subtilen Warnsignale im Benutzer- oder Entitätsverhalten. Ohne KI-gestützte Baseline-Erstellung und benutzerdefinierte Verhaltensanalysen können Zugangsdatenmissbrauch und Richtlinienverstösse monatelang unentdeckt auftreten – ein besonders akutes Risiko in datenreichen Branchen wie Finanzwesen und Gesundheitswesen.

## SOC-Überlastung und Ineffizienz

weiter zu Seite 14 →

Security Operations Centers (SOCs) sind mit Daten und Alarmen überflutet, was zu Alarmmüdigkeit und langsamen Reaktionszeiten führt. SOC-Teams bearbeiten durchschnittlich 4.484 Alarme pro Tag, und **67 % dieser Alarme werden aufgrund des Volumens und der Falschmeldungen ignoriert** [8]. Über die Hälfte der Sicherheitsteams fühlt sich von der Alarmmenge überfordert, und 55 % geben zu, nicht sicher in der Priorisierung und Reaktion zu sein [9]. Analysten verschwenden fast ein Viertel ihrer Zeit (27 %) mit der Verfolgung von Falschmeldungen [9] und verzögern damit die echte Vorfallsreaktion. Die Tool-Fragmentierung verschärft das Problem – Unternehmen jonglieren mit Dutzenden disparater Sicherheitstools, wobei die Komplexität selbst heute ein wesentliches Hindernis darstellt (52 % der Führungskräfte sagen, dass die Fragmentierung von Sicherheitslösungen ihre Fähigkeit zur Bedrohungsbekämpfung einschränkt [10]). Das Ergebnis ist ein überlasteter SOC, der Schwierigkeiten hat, schnell (oft zu spät in der Angriffskette) und präzise (hohe Fehlalarmraten) zu reagieren.

67% von 4.484 täglichen Alerts werden aufgrund von Volumen und False Positives ignoriert

## Datenschutz und regulatorischer Druck

weiter zu Seite 19 →

Datensouveränität und Datenschutzbestimmungen schränken ein, wie und wo Sicherheitsdaten analysiert werden, auch wenn neue Gesetze ein robusteres Monitoring fordern. Viele Sicherheitsanalyselösungen – insbesondere UEBA/SIEM-Technologie – setzen auf Cloud-Analysen, aber Organisationen in Regionen wie DACH (Deutschland, Österreich, Schweiz) und anderen Rechtsgebieten unterliegen der DSGVO und Datenspeicherungsanforderungen, die das Senden sensibler Benutzerlogs an ausländische oder öffentliche Clouds einschränken. Dies kann die Analysen einschränken und die operative Kontrolle reduzieren, wenn geeignete EU-basierte oder On-Premises-Optionen nicht verfügbar sind. Gleichzeitig erhöhen Vorschriften die Anforderungen: Der Digital Operational Resilience Act (DORA) der EU (in Kraft seit Januar 2025) verpflichtet Finanzinstitute zur kontinuierlichen Überwachung von IKT-Systemen und zur Meldung schwerwiegender Vorfälle innerhalb von Stunden [11], und die NIS2-Richtlinie wird auf neue Sektoren (Fertigung, Gesundheitswesen usw.) ausgedehnt **mit der Verpflichtung, Vorfälle innerhalb von 24 Stunden nach Erkennung zu melden** [12]. Diese Regeln machen die rechtzeitige Erkennung und Meldung anomaler Aktivitäten (einschliesslich der von UEBA erkannten) zu einer gesetzlichen Verpflichtung. Organisationen ohne automatisierte Echtzeit-Verhaltensanalysen und Berichterstattung sehen sich mit einem hohen manuellen Arbeitsaufwand zur Compliance-Erfüllung konfrontiert.

**24** Stunden für Unternehmen zur Meldung schwerwiegender Vorfälle gemäss NIS2-Richtlinie

# Die Herausforderungen im Detail

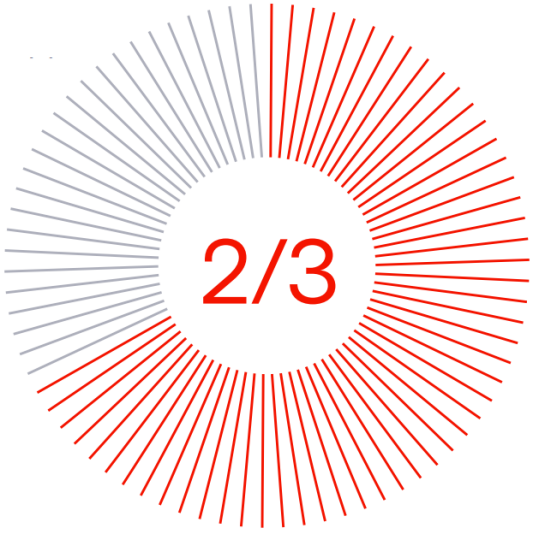
In den folgenden Abschnitten gehen wir tiefer auf diese Trends und Herausforderungen ein – von den versteckten Risiken des Shadow IT bis zur Bedeutung der Erkennung von Insider-Bedrohungen – und untersuchen, wie Unternehmen in BFSI, Fertigung, öffentlichem Sektor, Gesundheitswesen und anderen kritischen Branchen ihre Sicherheitsstrategien für 2026 anpassen.

Jeder Abschnitt liefert datengestützte Erkenntnisse und relevante Statistiken und bietet einen umfassenden Ausblick für Sicherheitsverantwortliche – von CISOs und CIOs bis hin zu SOC-Managern sowie Risiko- und Compliance-Leitern –, um die sich verändernde Landschaft zu verstehen.

# Shadow IT und blinde Flecken im Monitoring

1/3 verwaltete Apps

2/3 nicht verwaltete Apps




IT-Abteilungen sind über fast zwei Drittel der genutzten SaaS-Apps nicht informiert.

Trotz hoher Investitionen in die Cybersicherheit kämpfen Organisationen weiterhin mit **Sichtbarkeitslücken** in ihrer IT-Umgebung.

Eine wesentliche Ursache ist **Shadow IT** – Systeme und Anwendungen, die ausserhalb des Einflussbereichs zentraler IT- oder Sicherheitsteams betrieben werden. Studien zeigen, dass IT-Abteilungen über etwa zwei Drittel der in ihrer Organisation genutzten SaaS-Apps nicht informiert sind [2]. Tatsächlich kann die Anzahl der genutzten Cloud-Dienste

## 3× höher als das, was die IT kennt [2]

Diese unkontrollierte Einführung von Tools (oft durch Geschäftsbereiche, die Komfort suchen) führt zu Daten- und Log-Silos, die möglicherweise nie in das zentrale Sicherheitsmonitoring gelangen. Blinde Flecken entstehen, wenn kritische Systeme – von Legacy-ERP-Datenbanken bis hin zu neuen Cloud-Workloads oder APIs – nicht in die SOC-Monitoring-Fähigkeiten integriert sind. Viele Unternehmen konzentrieren ihre Abwehr immer noch auf Endpunkte oder Netzwerkperimeter-Traffic, während sie Anwendungsschicht-Logs, Benutzeraktivitäts-Feeds oder IoT/OT-Systeme vernachlässigen. Selbst wenn Logs aus diesen Quellen gesammelt werden, „sitzen sie im SIEM" ohne effektive Analyse, aufgrund von Formatierungskomplexitäten oder fehlenden Korrelationsregeln. Beispielsweise könnten eigene Anwendungslogs als Rohdaten aufgenommen, aber nicht in nützliche Verhaltenserkenntnisse oder Alarme umgewandelt werden, weil die Erstellung der erforderlichen Parser und Use Case Regeln zeitaufwändig ist. Infolgedessen könnten Führungskräfte und Sicherheitsteams ein falsches Sicherheitsgefühl haben, während in Wirklichkeit grosse Teile ihrer digitalen Infrastruktur für sie im Dunkeln liegen.

71 %

Über 71 % der SOC-Analysten befürchten, dass ihre Organisation möglicherweise kompromittiert wurde, ohne dass sie es wissen [4].

30 - 40 %

Shadow IT macht 30–40 % aller IT-Ausgaben aus [3].

68 %

Bis zu 68 % der Organisationen haben undokumentierte oder „Shadow"-APIs [14].

## Fragmentierte Sichtbarkeit:

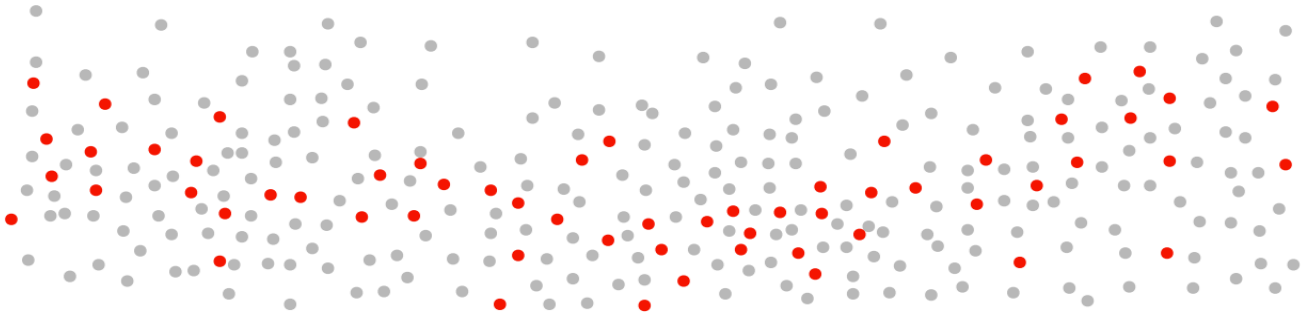
Über **71 % der SOC-Analysten befürchten, dass ihre Organisation möglicherweise kompromittiert wurde** [4], ein aufschlussreicher Indikator für die Sichtbarkeitslücke. Ebenso zeigen Sicherheitsumfragen, dass 76 % der KMU Shadow IT als moderate oder schwerwiegende Bedrohung wahrnehmen [13] – unbekannte Assets sind im Wesentlichen unüberwachte Assets.

Und es sind nicht nur kleine Unternehmen; Gartner schätzt, dass in grossen Unternehmen Shadow IT **30–40 % aller IT-Ausgaben** ausmacht [3], was unterstreicht, wie viel Technologie ausserhalb der offiziellen Aufsicht läuft. Über SaaS-Anwendungen hinaus stellen nicht entdeckte APIs und Service-Accounts einen weiteren blinden Fleck dar.

Bis zu **68 % der Organisationen haben undokumentierte oder „Shadow"-APIs** [14], die Daten preisgeben oder Zugriff ermöglichen könnten, ohne dass das Sicherheitsteam davon weiss. In einer Studie zielten fast 31 % der beobachteten böswilligen Anfragen auf unbekannte oder ungeschützte APIs [15] und nutzten diese Lücken aus. Jede nicht sichtbare Anwendung oder Schnittstelle ist ein potenzieller Brückenkopf für Angreifer und ein Einstiegspunkt für Insider-Missbrauch, der keinen Alarm auslöst, wenn Logs nicht analysiert werden.

> "Erschwerend kommt hinzu, dass Organisationen oft schwierige Entscheidungen über Log-Aufbewahrung und SIEM-Aufnahme aufgrund von Kosten- oder Leistungseinschränkungen treffen müssen"

Die traditionelle SIEM-Lizenzierung basiert typischerweise auf dem aufgenommenen Datenvolumen, was viele Unternehmen dazu veranlasst, ‚weniger wichtige' Logs herauszufiltern oder die Aufbewahrung zur Kostenkontrolle zu verkürzen. Ironischerweise sind einige der als hochvolumig (und damit teuer) eingestuften Logs genau jene, die frühzeitige Warnzeichen eines Angriffs liefern könnten – Identitäts- und Anwendungslogs beispielsweise, bei denen 90–95 % der Ereignisse routinemässig sind, aber die wenigen Anomalien kritisch sind [16]. Laut Branchenanalysten sind **fast 80 % der SIEM-Logs ‚Rauschen' mit geringem Analysewert [17]**, und Sicherheitsteams verbringen erhebliche Zeit damit, dieses Rauschen zu speichern und zu verarbeiten.



## Fast 80 % der SIEM-Logs sind “Rauschen” mit geringem Analysewert [17].

Die versteckten Kosten bestehen darin, dass Teams zur Budgeteinhaltung manchmal hochwertige Datenquellen vollständig fallen lassen und dabei versehentlich gefährliche blinde Flecken schaffen [18][16]. Mit anderen Worten bedeutet kostenbedingtes Datenfiltern, dass Angreifer sich in den Lücken verstecken können – wenn Logs eines ERP-Systems oder eines Okta-Identitätsdienstes nicht aufgenommen werden, könnte ein Insider, der diese Plattformen missbraucht, unbemerkt bleiben.

Der Nettoeffekt von Shadow IT und partiellem Monitoring ist ein **fragmentiertes Sicherheitsbild.** Verschiedene Tools und Silos bieten jeweils eine eingeschränkte Sicht (Endpunkt, Netzwerk, Cloud usw.) ohne einen einzigen Beobachtungspunkt.

Unter diesen Bedingungen können subtile Kompromittierungsindikatoren unbemerkt bleiben, da sie nur dann erkennbar werden, wenn Daten systemübergreifend korreliert werden. Beispielsweise könnte eine verdächtige Nutzung eines privilegierten Kontos in einer Kernbankanwendung nur auffallen, wenn sie neben ungewöhnlichen Netzwerkzugriffsmustern gesehen wird – etwas, das ein silierter Ansatz übersehen würde. Mehrere Umfragen bestätigen diese Herausforderung: **76% der Sicherheitsfachleute sagen, dass zu viele Point-Tools blinde Flecken in ihren Abwehrmechanismen erzeugen** [19]. Der Wechsel zu Cloud und hybrider IT hat diese Komplexität nur erhöht, da die Sichtbarkeit in Cloud-Workloads und SaaS-Nutzung hinter den On-Premises-Fähigkeiten zurückbleibt [20].

**76%** der Sicherheitsfachleute sagen, zu viele Point-Tools erzeugen blinde Flecken in ihren Abwehrmechanismen [19].

Um diese blinden Flecken zu beheben, verlagern sich Organisationen schrittweise zu einem einheitlicheren Monitoring und einer Datenintegration. Praktiken wie zentralisiertes Log-Management und Sicherheitsdaten-Lakes gewinnen an Bedeutung und ermöglichen es Unternehmen, diverse Datenquellen ohne die hohen Kosten einer traditionellen SIEM aufzunehmen.

Noch wichtiger ist die wachsende Erkenntnis, dass **Verhaltensanalysen** über Endpunkte hinaus auf Benutzer, Anwendungen und sogar Service-Accounts ausgeweitet werden müssen. Der Einsatz fortschrittlicher Sicherheitsanalysetechnologien wie UEBA ist eine Antwort auf diesen Bedarf. UEBA erstellt Baselines für das normale Verhalten von Usern und Maschinen. So werden Rohdaten aus unzureichend überwachten Systemen zu aussagekräftigen Anomalien.

# Der Ausblick 2026

Der Trend 2026 geht zu konvergierten Plattformen, die Netzwerk-, Cloud-, Endpunkt- und Identitätstelemetrie kombinieren, um die Sichtbarkeitslücken zu schliessen. Wie in einem Branchenbericht festgestellt, entwickeln sich moderne SIEM/Analyse-Lösungen zum ‚zentralen Nervensystem' des SOCs, das domänenübergreifend korreliert und KI einsetzt, um Ereignisse hervorzuheben, die in isolierten Silos unsichtbar wären [21][22]. Organisationen, die diese Integration meistern, werden ihre Shadow-IT-Risiken erheblich reduzieren und Bedrohungen aufdecken, die in ehemals blinden Bereichen lauern.

# Übersehene Insider-Bedrohungen und unentdeckte Angriffe

76%

der Organisationen identifizieren wachsende geschäftliche und technologische Komplexität, einschliesslich Faktoren wie Cloud-Einführung, erhöhter Benutzerzugang und IT-Ausbreitung, als wesentliche Treiber des steigenden Insider-Risikos.

Insider-Bedrohungen – ob böswillige Mitarbeiter, kompromittierte Accounts oder Identities oder unbeabsichtigte Fehler – haben sich zu einer der heimtückischsten Sicherheitsherausforderungen entwickelt.

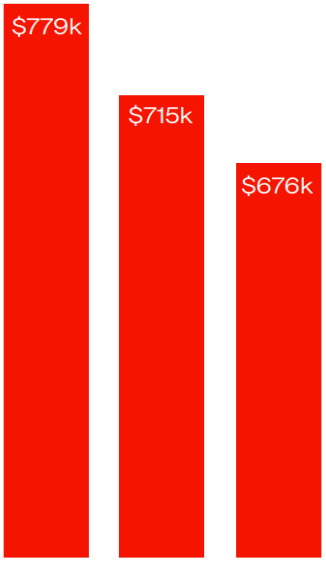
In stark regulierten Branchen wie BFSI oder Pharma haben Insider privilegierten Zugang zu sensiblen Daten und Systemen, was sie einzigartig in der Lage versetzt, Schaden anzurichten. Leider sind viele traditionelle Sicherheitstools schlecht geeignet, Insider-Verhalten zu erkennen, das legitim erscheint. Im Gegensatz zu Malware oder externen Angriffen, die Antivirus- oder Firewall-Alarme auslösen könnten, beinhalten Insider-Angriffe oft einen autorisierten Benutzer, der erlaubte Dinge tut, aber auf anomale Weise oder in unangemessenen Kontexten.

### Die Häufigkeit von Insider-Vorfällen ist stark gestiegen.

Eine globale Umfrage von 2024 ergab, dass **83 % der Organisationen mindestens einen Insider-Sicherheitsverstoss im Vorjahr erlebt haben** [5], gegenüber etwas mehr als der Hälfte der Organisationen vor einigen Jahren. Darüber hinaus glauben 74 % der Organisationen, dass Insider-Angriffe in letzter Zeit häufiger geworden sind [23], angetrieben durch Faktoren wie den Anstieg der Remote-Arbeit, Cloud-Zusammenarbeit und die schiere Komplexität moderner IT (die mehr Versteckmöglichkeiten bietet).

Besonders auffällig ist, dass **76 % der Organisationen wachsende geschäftliche und technologische Komplexität, einschliesslich Faktoren wie Cloud-Einführung, erhöhter Benutzerzugang und IT-Ausbreitung, als wesentliche Treiber des steigenden Insider-Risikos identifizieren** [24]. Da mehr Mitarbeiter von mehr Orten auf Daten zugreifen, wird es ohne fortschrittliche Analysen schwieriger, ‚normales' Verhalten als Baseline zu definieren. Dies ist eine zentrale Herausforderung für ITDR: zu erkennen, wann das Verhalten einer gültigen Identity auf Kompromittierung oder Missbrauch hindeutet.

Bestimmte Branchen sind einem besonderen Insider-Bedrohungsrisiko ausgesetzt. Im Finanzdienstleistungsbereich besteht die Gefahr von internem Betrug oder Datendiebstahl (z. B. ein Mitarbeiter mit Zugang zu Transaktionssystemen, der Zugangsdaten missbraucht). Im Gesundheitswesen könnten Insider elektronische Gesundheitsakten einsehen oder Patientendaten missbrauchen. Fertigung und Pharma befürchten Lieferkettenangriffe und Diebstahl geistigen Eigentums durch Mitarbeiter oder Auftragnehmer. Organisationen im öffentlichen Sektor und in kritischen Infrastrukturen sind potenzieller Sabotage oder Spionage durch Insider ausgesetzt. In allen Fällen können die Auswirkungen eines Insider-Vorfalls enorm sein – eine aktuelle Studie bezifferte die durchschnittlichen jährlichen Kosten von Insider-Bedrohungen auf 17,4 Mio. USD pro Organisation in 2025 (gegenüber 16,2 Mio. USD in 2023) [7]. Diese Kosten entstehen durch Untersuchungen, Systemausfallzeiten, Behebung, regulatorische Bussgelder und Vertrauensverlust. Besonders kostspielig sind **Vorfälle mit kompromittierten Zugangsdaten, die durchschnittlich 779.000 USD pro Vorfall kosten** [25], da sie Angreifern oft ermöglichen, als legitime Benutzer unentdeckt zu agieren.




Zugangsdatendiebstahl ist mit **$779k** am teuersten, gefolgt von böswilligen Handlungen mit **$ 715k** und Fahrlässigkeit mit **$676k**.

## “Im Durchschnitt benötigen Unternehmen über 80 Tage, um einen Insider-Vorfall einzudämmen.”

Das Erkennungsproblem liegt im Kern der Frage, warum Insider-Bedrohungen übersehen werden. Im Durchschnitt benötigen Unternehmen über 80 Tage, um einen Insider-Vorfall einzudämmen [7] – d. h. ein Insider kann fast ein ganzes Quartal lang agieren, bevor er gestoppt wird. Ein Teil dieser Verzögerung liegt darin, dass die erste Erkennung langsam ist.


Bekannte initiale Zugriffsvektoren bei Nicht-Fehler-, Nicht-Missbrauchs-Verletzungen (n=9.891) [26]

Viele Insider-Aktionen lösen keine eindeutigen Alarme aus: Zum Beispiel könnte ein Mitarbeiter, der schrittweise mehr Daten als üblich herunterlädt oder auf Systeme zugreift, die er selten nutzt, keine statischen Regeln auslösen. Ohne Verhaltens-Baseline-Erstellung gehen solche Muster im Hintergrund unter. **Verizons Datenverletzungsforschung hebt hervor, dass der menschliche Faktor bei der Mehrheit der Verletzungen eine Rolle spielt und gestohlene Zugangsdaten bei über 22 % der Verletzungen genutzt werden** [26] – und damit einen externen Angriff durch die Nutzung legitimen Zugangs in einen ‚Insider‘-Vorfall verwandeln. Sobald ein Angreifer mit den Zugangsdaten eines gültigen Benutzers eingeloggt ist, bieten traditionelle Perimeter-Abwehrmechanismen (Firewalls usw.) keine Hilfe [27]. Die Aktionen des Angreifers müssen durch Erkennung abnormaler Nutzung dieses Benutzerkontos aufgedeckt werden – genau das, wofür UEBA entwickelt wurde.

# 5-facher Anstieg

Organisationen mit 11–20 jährlichen Insider-Angriffen verzeichneten einen fünffachen Jahresanstieg

„Ein in ein CRM-System eingebetteter KI-Assistent könnte durch eine geschickt gestaltete Benutzereingabe manipuliert werden, sensible Kundendaten an einen externen Ort zu exportieren.“

**Beispiele für übersehene Insider-Bedrohungsszenarien gibt es zuhauf.**

In vielen Fällen hatten Mitarbeiter wochenlang Richtlinien verletzt oder verdächtiges Verhalten gezeigt, wurden aber erst nach einem schwerwiegenden Vorfall oder Whistleblower-Bericht entdeckt.

**Häufige rote Flaggen, die oft übersehen werden:**

- ein Mitarbeiter, der auf Systeme zugreift, auf die er noch nie zugegriffen hat,
- Anmeldungen zu ungewöhnlichen Zeiten oder von ungewöhnlichen Orten,
- plötzliche Spitzen bei Datenbankabfragen oder Dateidownloads,
- oder mehrere Authentifizierungsfehler auf sensiblen Systemen.

Wenn diese Ereignisse nicht kontextuell korreliert und analysiert werden, könnten sie als normale IT-Probleme abgetan oder in Log-Dateien begraben bleiben. Der Insider-Bedrohungsbericht 2024 vermerkte einen **fünffachen Anstieg bei Organisationen, die ein hohes Volumen (10+ pro Jahr) an Insider-Vorfällen erfahren,** was darauf hindeutet, dass viele kleinere Vorfälle wahrscheinlich unbemerkt bleiben, bis sie sich häufen [6].

Wichtig ist, dass sich die Vorstellung, wer oder was ein Insider sein kann, weiterentwickelt. Da Organisationen **agentische KI-Systeme** (KI-betriebene Agenten, die autonom über E-Mail, Dateisysteme, Identitätsplattformen und Geschäftsanwendungen agieren können) einsetzen, gewinnen diese Tools System-Level-Zugang, der mit dem menschlicher Benutzer vergleichbar oder grösser ist. Wenn kompromittiert – ob durch Prompt-Injection, Lieferketten-Manipulation oder böswilliges Umtrainieren – könnte ein Agent Privilegien unter dem Deckmantel des ‚Benutzerhelfens' missbrauchen, während er still Daten exfiltriert oder Datensätze modifiziert [60]. Beispielsweise könnte ein KI-Assistent, der in ein CRM-System eingebettet ist, durch eine geschickt gestaltete Benutzereingabe manipuliert werden, sensible Kundendaten an einen externen Ort zu exportieren. Da diese Agenten typischerweise ausserhalb herkömmlicher Identitäts- und Verhaltensüberwachungs-Frameworks fallen, könnte ihre Aktivität weder ordnungsgemäss protokolliert noch auf Anomalien überprüft werden. Das Ergebnis ist eine neue Klasse von nicht-menschlichen Insidern mit umfangreichem Zugang, aber begrenzter Aufsicht.

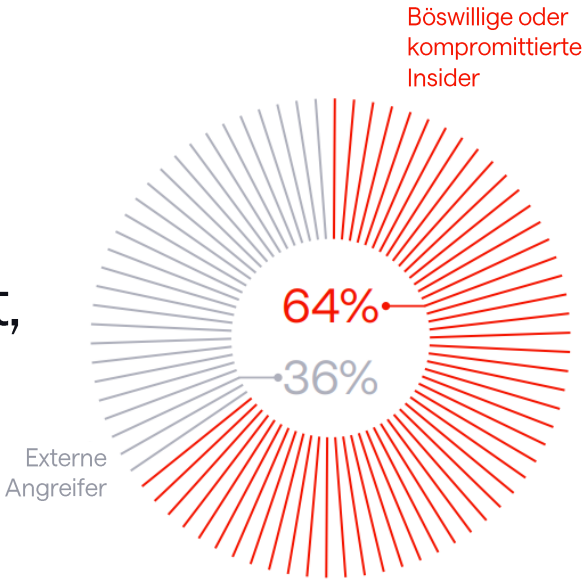
Sicherheitsteams müssen zunehmend **Maschinen- und Agentenverhalten** parallel zu menschlichen Benutzern überwachen. Dies wirft wichtige architektonische Fragen auf: Sollte jeder KI-Agent als eigene Entität innerhalb von Sicherheitsanalysemodellen behandelt werden? Wie definieren wir ‚normales' Verhalten für einen nicht-menschlichen Akteur als Baseline, der vielfältige Aufgaben für viele Benutzer systemübergreifend ausführt? Dies sind dringende Themen für SOCs und Risikoführungskräfte, da die Einführung agentischer KI in Unternehmens-Workflows zunimmt. Sicherheitsanalyse-Systeme, die diese Entitäten nicht berücksichtigen, riskieren blinde Flecken, wo Angreifer durch scheinbar gutartiges Maschinenverhalten schwenken können, das tatsächlich bösartig oder kompromittiert ist.

**Insider-Bedrohungen sind auch nicht auf direkte Mitarbeiter beschränkt.**

Auftragnehmer, Drittanbieter-Partner oder Service-Accounts können als Insider handeln. Beispielsweise könnte ein Support-Auftragnehmer mit VPN-Zugang Daten exfiltrieren, oder ein Angreifer könnte ein Software-Konto eines Drittanbieters kompromittieren, um ins Netzwerk zu gelangen. Diese Szenarien unterstreichen den Bedarf an Entity Behavior Analytics (das ‚E' in UEBA) – nicht nur menschliche Benutzer, sondern auch Service-Accounts, APIs und Maschinen auf Anomalien zu überwachen.

Moderne Sicherheitsanalyselösungen nutzen maschinelles Lernen, um eine Baseline normalen Verhaltens für jeden Benutzer und jede Entität zu erstellen (auf welche Ressourcen sie zugreifen, typische Arbeitszeiten, Netzwerkaktivitätsmuster usw.). Sie können dann subtile Abweichungen markieren: z. B. wenn ein Benutzer, der normalerweise wochentags auf HR-Datensätze zugreift, plötzlich an einem Wochenende eine Kundendatenbank in Bulk herunterlädt, oder wenn ein privilegiertes Konto Abfragen ausführt, die es noch nie zuvor ausgeführt hat. KI-gestütztes UEBA ist zunehmend unverzichtbar, da sich Insider-Angriffe weiterentwickeln und aus Erkennungsmethoden ‚lernen'. Statische Regeln allein (wie feste Schwellenwerte für Downloads) produzieren oft entweder zu viele Falschmeldungen oder übersehen den Kontext, der eine Aktion wirklich verdächtig macht. Sicherheitsanalysetools können sich anpassen, wenn sich das Verhalten im Laufe der Zeit ändert und neue Arten von Insider-Taktiken entstehen.

Tatsächlich zeigen Sicherheitsumfragen, dass **64 % der Cybersicherheitsfachleute böswillige Insider oder kompromittierte Konten als grössere Gefahr** als externe Angreifer betrachten [28], was einen Konsens widerspiegelt, dass fortschrittliche Verhaltensanalyse oberste Priorität hat.




Grösste Cybersicherheitsbedrohung laut Fachleuten.

# Der Ausblick 2026

Zusammenfassend bleiben übersehene Insider-Bedrohungen eine kritische Schwachstelle in allen Branchen. Die Kombination aus komplexeren IT-Umgebungen, entschlosseneren Angreifern (einschliesslich nationalstaatlicher Akteure, die Insider rekrutieren oder gestohlene Zugangsdaten verwenden) und höheren Einsätzen (sowohl finanziell als auch regulatorisch) bedeutet, dass Organisationen ihre Insider-Bedrohungsprogramme stärken müssen.

Dazu gehört nicht nur der Einsatz fortschrittlicher Sicherheitsanalysetechnologien, sondern auch die Etablierung von Insider-Reaktions-Playbooks, die Durchführung regelmässiger Benutzer-Zugangsprüfungen und die Förderung einer Kultur, in der Mitarbeiter sich der Insider-Risiken bewusst sind (z. B. wissen, wie man Social-Engineering-Versuche erkennt, die auf den Diebstahl von Zugangsdaten abzielen). In Zukunft müssen Sicherheitsstrategien KI-Agenten explizit als überwachte Identitäten einschliessen. Bis 2026 erwarten wir, dass Insider-Bedrohungserkennung zu einem Standardbestandteil von Cybersicherheitsstrategien wird – nicht als nachträglicher Gedanke –, insbesondere in Sektoren wie BFSI, Pharma und kritischer Infrastruktur, wo der ‚Insider-Schaden' katastrophal sein kann.

# SOC-Überlastung und operative Ineffizienzen

## 4.484

täglich durchschnittlich von SOC-Teams bearbeitete Alarme.

## 67 %

werden aufgrund des unbeherrschbaren Volumens und häufiger Falschmeldungen einfach ignoriert.

## 70 %

des SOC-Personals berichten, dass die unaufhörliche Alarmüberlastung ihr Wohlbefinden und ihre Work-Life-Balance negativ beeinflusst [29].

Security Teams verarbeiten täglich enorme Mengen an Daten und Alerts. Das führt zu Alert Fatigue, langsameren Reaktionen und übersehenen Signalen. Nirgendwo ist dies deutlicher als im SOC (Security Operations Center), dem Nervenzentrum, wo Bedrohungen erkannt und neutralisiert werden sollen. In allen Branchen berichten SOC-Analysten konstant von hohen Stress- und Burnout-Niveaus, die direkt auf Alarmüberlastung und ineffiziente Prozesse zurückzuführen sind.

Eine globale Studie mit 2.000 SOC-Analysten zeichnete ein drastisches Bild: Ein durchschnittliches Unternehmens-SOC erhält etwa **4.484 Sicherheitsalarme pro Tag, von denen 67 % aufgrund des unbeherrschbaren Volumens und häufiger Falschmeldungen einfach ignoriert werden** [8]. Das bedeutet, dass nur etwa ein Drittel der potenziellen Probleme überhaupt von Menschen überprüft wird – eine Lücke, die Angreifer ausnutzen können. Eine weitere Branchenumfrage ergab, dass 51 % der SecOps-Teams sich von der Alarmmenge, die sie bewältigen müssen, überfordert fühlen, und 55 % sind nicht sicher in ihrer Fähigkeit, effektiv zu priorisieren und zu reagieren [9]. In der Praxis können viele SOCs nur einen Bruchteil der eingehenden Alarme triagieren; der Rest wird in die Warteschlange gestellt oder automatisch geschlossen, was eine gefährliche ‚Alarmmüdigkeit'-Rückkopplungsschleife erzeugt.

Falschmeldungen sind ein grosser Beitragsfaktor zum Rauschen. Mit Legacy-SIEM-Regeln oder signaturbasierter Erkennung ist es üblich, Alarmstürme für gutartige Ereignisse zu erhalten. Analysten verbringen etwa 1/4 ihrer Zeit (27 %) mit der Untersuchung von Falschmeldungen [9] und jagen damit im Wesentlichen Gespenstern. Dies ist verschwendete Mühe, die die Untersuchung echter Bedrohungen verzögert. Es schwächt auch die Moral – das ständige Reagieren auf Fehlalarme kann Teams abstumpfen lassen oder schlimmer noch, Alarme ganz zu ignorieren. Tatsächlich berichten etwa **70 % des SOC-Personals, dass die unaufhörliche Alarmüberlastung ihr Wohlbefinden und ihre Work-Life-Balance negativ beeinflusst** [29].

Es sind Fälle dokumentiert, in denen Analysten absichtlich laute Alarmregeln ausschalten oder sie weniger sensitiv einstellen, nur um den Strom an Benachrichtigungen zu reduzieren [29]. Das Risiko ist natürlich, dass tatsächliche Angriffe dann unbemerkt durchschlüpfen könnten.

# Mehrere Grundursachen tragen zu dieser operativen Ineffizienz bei:

## Exponentielles Wachstum der Log-Daten:

Da Organisationen das Logging auf mehr Systemen aktivieren und in Cloud, IoT und Remote-Arbeit expandieren, explodiert die Menge an Sicherheitstelemetrie. Aber nicht alle Logs sind intelligente Signale – wie bereits erwähnt, haben bis zu **80 % der aufgenommenen Logs kaum Sicherheitswert** [17], aber sie verbrauchen trotzdem Analysten-Aufmerksamkeit und SIEM-Ressourcen.

**80 %** der aufgenommenen Logs haben kaum Sicherheitswert.

## Fragmentierte Tools und isolierte Systeme:

Viele Unternehmen haben einen Flickenteppich von Point-Sicherheitstools angesammelt (für Endpunkt, Netzwerk, Cloud, Identität usw.), die nicht gut integriert sind. **Die durchschnittliche Organisation nutzt 83 verschiedene Sicherheitslösungen von 29 Anbietern** [10], was einen fragmentierten Workflow für SOC-Analysten erzeugt. Sie müssen zwischen mehreren Konsolen hin- und herwechseln und Daten manuell korrelieren. Über die Hälfte der Sicherheitsführungskräfte (52 %) sagt, diese Komplexität selbst sei das grösste Hindernis für effektive Operationen [10]. Wenn ein Alarm eingeht, könnte das Sammeln von Kontext das Abfragen von drei oder vier separaten Systemen erfordern – ein langsamer und fehleranfälliger Prozess.

**83** Die durchschnittliche Organisation nutzt 83 verschiedene Sicherheitslösungen von 29 Anbietern.

## Mangel an qualifizierten Analysten:

Der Cybersicherheits-Fachkräftemangel verschärft das Problem – es gibt einen geschätzten **Fehlbestand von 3,4 Millionen Personen in der Cyber-Belegschaft** [30], was bedeutet, dass viele SOCs unterbesetzt sind. Die an der Front stehenden müssen zu viele Alarme pro Person jonglieren. Kritische Untersuchungs- und Jagdaufgaben werden aufgeschoben, weil das Team im reaktiven Modus feststeckt.

**3,4 Mio.**

Cybersecurity Fachkräfte, die weltweit fehlen.

## Mangel an Kontext/Anreicherung:

Alarme ohne Kontext (Wer/Was/Wo eines Ereignisses) zwingen Analysten zu zusätzlicher Arbeit. Beispielsweise könnte ein roher Alarm wie ‚übermässige fehlgeschlagene Anmeldungen auf Server X' ein geringfügiges IT-Problem oder ein Brute-Force-Angriff sein – um zu wissen, welches es ist, muss ein Analyst zugehörige Daten suchen (welcher Benutzer? von wo? was haben sie sonst getan?). Ohne Automatisierung zur Anreicherung von Alarmen mit Kontext ist die Triage langsam und viele Alarme bleiben unbearbeitet.

Die Konsequenzen der SOC-Überlastung sind erhebliche Verzögerungen bei der Erkennung und Reaktion. Während einige Organisationen die Komplexität durch die Einführung einheitlicher Sicherheitsplattformen reduzieren, integrieren andere erfolgreich Best-of-Breed-Lösungen durch leichtgewichtige, API-erste Architekturen. Branchenforschung zeigt, dass die Reduzierung von Tool-Fragmentierung – ob durch Konsolidierung oder nahtlose Interoperabilität – die Reaktionszeiten dramatisch verbessern kann.

Eine Studie ergab, dass

# Organisationen mit optimiertem Security Operations entdecken Vorfälle im Durchschnitt 72 Tage schneller und können sie 84 Tage schneller eindämmen, als solche, die isolierte Tools einsetzen. [31][32]

Dies veranschaulicht, wie viel Ineffizienz sich in einem unzusammenhängenden SOC-Workflow verbergen kann. Wenn ein Angriff wie Ransomware eine Umgebung in Stunden verschlüsseln kann, ist es offensichtlich inakzeptabel, Tage oder Wochen mit der Reaktion zu warten.

### Alert Fatigue kann auch zu verpassten Angriffen führen.

Echte Vorfälle erzeugen oft Frühwarnalarme, die möglicherweise niedrig eingestuft oder unter Falschmeldungen begraben sind. Wenn diese Alarme ignoriert werden, schreitet der Angriff fort, bis ein viel offensichtlicheres Symptom (wie ein Serverausfall oder eine grosse Datenexfiltration) bemerkt wird – zu diesem Zeitpunkt ist der Schaden angerichtet. Laut einer Umfrage glauben **71 % der Analysten, dass in ihrer Umgebung möglicherweise bereits Kompromittierungen vorhanden sind, die sie noch nicht entdeckt haben** [4], was mit der Idee übereinstimmt, dass Überlastung eine Vertrauenskrise in die Erkennungsfähigkeiten verursacht.

**71 %**

der Analysten glauben, dass in ihrer Umgebung möglicherweise bereits Kompromittierungen vorhanden sind, die sie noch nicht entdeckt haben [4].

Um diese operativen Herausforderungen zu bekämpfen, verfolgen Organisationen für 2026 mehrere Strategien:


### Investitionen in Automatisierung und KI:

Die Automatisierung von Level-1-Triageaufgaben kann die Arbeitslast drastisch reduzieren. Viele SOCs setzen Security Orchestration, Automation and Response (SOAR)-Tools oder automatisierte Playbooks ein, um Routinealarme zu bearbeiten (wie automatisches Quarantänieren von Malware, Sammeln grundlegender Vorfallsdaten usw.). KI und maschinelles Lernen werden auch eingesetzt, um Falschmeldungen zu reduzieren – zum Beispiel können KI-gesteuerte SIEM/UEBA/NDR lernen, welche Alarme wirklich bedeutsam sind, indem sie Verhaltensmuster querverweisen und so Rauschen herausfiltern. Es gibt auch Interesse an Generative-KI-Assistenten, um Analysten bei der Zusammenfassung von Vorfällen zu helfen oder sogar Behebungsschritte vorzuschlagen, als Kraftmultiplikatoren für jüngere Mitarbeiter.

### Alarmpriorisierung und Risikobewertung:

Moderne Erkennungsplattformen wenden nun oft einen Risikoscore auf Entitäten oder Vorfälle an und helfen Analysten, sich zuerst auf die kritischsten Probleme zu konzentrieren. Durch die Korrelation mehrerer Low-Level-Ereignisse zu einem einzigen Vorfall (zum Beispiel eine Kombination aus einem Alarm für ein ungewöhnliches Login, aus einem ungewöhnlichen Datenzugriff und aus einem Klick auf eine Phishing-E-Mail für denselben Benutzer) können die Systeme eine kohärente Geschichte präsentieren, dass diese Ereigniskette wahrscheinlich auf einen Breach hinweist. Dies reduziert die Anzahl der separaten Alarme und liefert den benötigten Kontext in einem Paket.

### Interoperabilität statt Plattform Lock-In:

Da Sicherheitsteams mit wachsender Arbeitslast und Alarmmüdigkeit konfrontiert sind, suchen Organisationen nach Wegen, die Operationen zu optimieren, ohne Tiefe oder Flexibilität zu opfern. Während einige Full-Stack-Plattformen verfolgen, bevorzugen viele jetzt modulare, interoperable Lösungen, die sich einfach in bestehende Ökosysteme integrieren. Anstelle von monolithischen ‚All-in-one'-Plattformen priorisieren vorausschauende Teams Tools, die einfach zu implementieren (z. B. Log-Weiterleitung, Out-of-the-box-Normalisierung), standardbasiert (API-bereit) und analysereich sind, was schnellen Time-to-Value ohne Vendor-Lock-In ermöglicht. Dieser ‚Best-of-Breed, gut integriert'-Ansatz unterstützt einheitliche Sichtbarkeit bei gleichzeitiger Kontrolle über Architektur und Datenfluss. Der Druck zur Reduzierung von Tool-Fragmentierung ist real: **74 % der Sicherheitsführungskräfte sagen, die Arbeitslast ihrer Teams sei übermässig** [33], und 52 % nennen nicht verbundene Tools als ein wesentliches Hindernis für eine effektive Bedrohungsreaktion [34]. Bis 2026 streben viele Organisationen danach, operative Workflows zu konsolidieren – nicht unbedingt in einem einzigen Anbieter-Stack, sondern in einer kohärenten, interoperablen Erkennungs- und Reaktionsschicht.

### Kontextuelle und frühzeitige Alarmierung:

Anstatt Zehntausender roher Alarme ist das Ziel, weniger, klügere Alarme zu generieren. Verhaltensanalysen spielen hier eine Rolle, indem sie sich auf Anomalien konzentrieren, die wirklich von normalen Baselines abweichen (oft auf eine fortgeschrittene Bedrohung oder einen Insider hinweisend). Darüber hinaus kann kontinuierliche Bedrohungsintelligenz-Integration dem SOC helfen zu wissen, welche Alarme bekannten Bedrohungskampagnen zugeordnet sind. Frühzeitige Erkennung ist der Schlüssel – ein Angreifer in der Aufklärungsphase oder Lateral-Movement-Phase [35] zu erwischen verhindert Schäden in späteren Phasen.

## Letztendlich ist die Bewältigung der SOC-Überlastung genauso sehr eine Frage der Prozesse und Menschen wie der Technologie.

Viele Organisationen überarbeiten ihre Incident-Response-Workflows, implementieren straffere SLAs für die Alarmbearbeitung und bessere Übergabeverfahren (damit kritische Alarme nicht zwischen Schichten verloren gehen). Schulung und Bindung qualifizierter Analysten sind ebenfalls entscheidend – einige Unternehmen rotieren Mitarbeiter, um Burnout zu verhindern, und bieten On-Call-Unterstützung bei schwerwiegenden Vorfällen an, um Ermüdung zu vermeiden. **KPIs wie Mean Time to Detect (MTTD) und Mean Time to Respond (MTTR) werden von CISOs als Schlüsselmetriken der SOC-Effizienz genau beobachtet.**

# Der Ausblick 2026

**Für 2026 ist eine aufkommende Best Practice, das SOC wie eine kontinuierliche Verbesserungsumgebung zu behandeln:** regelmässiges Abstimmen von Erkennungsregeln zur Beseitigung von Rauschen, Ausserbetriebnahme von Tools ohne Mehrwert und periodische Simulation von Hochalarm-Szenarien, um sicherzustellen, dass das Team ohne Zusammenbruch unter Druck bestehen kann.

Zusammenfassend kämpfen SOCs in BFSI, Fertigung, Regierung und anderen Sektoren alle mit diesen operativen Problemen – das SOC einer Bank könnte in Betrugsalarmdaten ertrinken, während das SOC eines Versorgungsunternehmens sowohl IT- als auch Legacy (OT)-Apps überwachen muss, ohne den Überblick zu verlieren. Die Lösungen liegen in intelligenterer Technologie (Verhaltensanalysen, KI/ML, integrierte Plattformen) und intelligenteren Operationen (Workflow-Automatisierung, Tool-Rationalisierung). Die Organisationen, die dies meistern, werden einen erheblichen Vorteil erlangen: schnellere und präzisere Vorfallsreaktion, was wiederum den Unterschied bedeuten kann zwischen dem schnellen Vereiteln eines Angriffs oder dem Erleiden kostspieliger Schäden.

# Datenschutz und regulatorische Herausforderungen für Analysen

Während Organisationen darum bemüht sind, ihre Bedrohungserkennung und -reaktion zu verbessern, müssen sie dies unter den Einschränkungen des Datenschutzes, der Datensouveränität und der regulatorischen Compliance tun. Diese Faktoren sind besonders relevant in Regionen wie Europa und dem Nahen Osten sowie in Branchen wie Finanzwesen, kritischer Infrastruktur und Regierung, wo Daten hochsensibel und stark reguliert sind.

**Zwei miteinander verknüpfte – und potenziell widersprüchliche – Herausforderungen stechen hervor:**

1. Einschränkungen bei der Datenhosting/-verarbeitung (die beeinflussen, wie Sicherheitsanalysen eingesetzt werden können),

2. Neue Vorschriften, die eine stärkere operative Resilienz und Berichterstattung vorschreiben.

**Einschränkungen beim Daten-Hosting & Souveränität:**

Viele Sicherheitsanalyselösungen nutzen Cloud-Infrastruktur für Skalierbarkeit und fortschrittliche Analysen. Cloud-basierte Analysen können Vorteile bei der Verarbeitung von Big Data bieten (KI auf massive Log-Volumina anwenden usw.). Für Unternehmen in Rechtssystemen mit strengen Datenschutzgesetzen wirft das Senden interner Benutzerverhaltensdaten oder Systemlogs in eine öffentliche Cloud (insbesondere eine in einem anderen Land gehostete) jedoch rote Flaggen auf.

“Organisationen müssen ihre Bedrohungserkennung und -reaktion verbessern und dabei Datenschutz-, Souveränitäts- und regulatorische Compliance-Einschränkungen einhalten.”

**Europäische Datenschutzgesetze (DSGVO)** erfordern beispielsweise, dass personenbezogene Daten (die Benutzer-IDs, IP-Adressen, Authentifizierungslogs usw. umfassen könnten) sorgfältig behandelt und nicht in Regionen ohne äquivalente Schutzmassnahmen übertragen werden. Organisationen in DACH, anderen europäischen Ländern und im Nahen Osten haben oft Richtlinien oder Vorschriften, die verlangen, dass sensible Log-Daten (wie Mitarbeiter- oder Kundeninformationen in Sicherheitslogs) innerhalb nationaler oder EU-Grenzen verbleiben. Daher

entspricht das ‚cloud-only' Liefermodell einiger Sicherheitsanalyse-Anbieter nicht diesen Anforderungen, was Sicherheitsteams dazu zwingt, entweder On-Premises- oder EU-lokale Lösungen zu suchen oder reduzierte Funktionalität zu akzeptieren.

Darüber hinaus haben bestimmte Sektoren explizite Souveränitätsregeln: Regierungsbehörden und Betreiber kritischer Infrastruktur können verpflichtet sein, inländische Clouds oder On-Premises-Systeme für das Sicherheitsmonitoring zu nutzen, um Spionagerisiken zu vermeiden. Im Finanzsektor schreiben Vorschriften wie die EZB-Leitlinien zum Cloud-Outsourcing und andere die Aufsicht und Auditierbarkeit jedes Cloud-Dienstes vor – was einige Banken dazu bewegt, selbst gehostete Analysen zu bevorzugen. Wenn ein Sicherheitsanalysetool das Hochladen aller Active-Directory-Logs in eine US-basierte Cloud zur Analyse erfordert, werden viele europäische Banken es schlicht nicht in Betracht ziehen, egal wie effektiv die Analysen sein mögen.

**Das schafft einen Trade-off:**

Einige der fortschrittlichsten Analysetools könnten aufgrund von Datenschutzbedenken nicht verfügbar sein. Organisationen enden mit eingeschränkten Analysen, wenn sie Cloud-KI/ML nicht im grossen Massstab nutzen können. Selbst wenn Cloud verwendet wird, treiben Datenschutzbedenken die Nachfrage nach Datenanonymisierung oder Pseudonymisierung in Logs (was die Analyse durch Entfernen von Benutzer-Identifikatoren komplizieren kann). Anbieter reagieren mit EU-basierten Cloud-Instanzen oder Hybrid-Deployments (bei denen sensible Daten vor Ort bleiben und nur anonymisierte Funktionen in die Cloud gehen). Nichtsdestotrotz bleibt es eine Einschränkung – die Flexibilität, die Lösung dort zu hosten, wo der Kunde sie benötigt, ist heute ein Wettbewerbsfaktor. Anbieter, die On-Premises- oder Private-Cloud-Deployments unterstützen, sehen in stark regulierten Märkten Nachfrage, während reine Cloud-Lösungen auf Zurückhaltung stossen. Kurz gesagt wird ‚Analyse-Souveränität' wichtig:

Organisationen wollen leistungsstarke Analysen und Kontrolle darüber, wo die Daten liegen.

Gleichzeitig entstehen datenschutzerhaltende Analysetechniken. Es gibt Interesse an Methoden wie föderiertem Lernen (bei dem Modelle auf lokalen Daten trainieren und nur Modell-Updates teilen, nicht rohe Logs) oder fortschrittlicher Verschlüsselung, die Cloud-Analyse ohne Offenlegung von Klartext-Daten ermöglicht. Diese befinden sich noch in der Entwicklung, aber der Schlüsselpunkt ist, dass Benutzerverhaltensdaten sensibel sind und Analyseplattformen sich anpassen, um Datenschutzgesetzen zu entsprechen. Wie eine Marktanalyse feststellte, integrieren die meisten Sicherheitsanalyse-Anbieter Datenschutzmassnahmen zur Einhaltung globaler Datenschutzgesetze, während sie weiterhin grosse Mengen von Verhaltensdaten analysieren [36]. Dies kann Funktionen wie rollenbasierte Zugriffskontrollen, Datenminimierung und klare, vorschriftskonforme Datenspeicherungsrichtlinien umfassen.

## Regulatorische Anforderungen – DORA, NIS2 und mehr

Auf der anderen Seite der Einschränkungen treiben Regulatoren Organisationen auch dazu an, ihre Sicherheitsmonitoring- und Vorfallsmeldungsfähigkeiten zu verbessern. Insbesondere hat die EU neue Regeln eingeführt, die explizit oder implizit kontinuierliche Bedrohungserkennung erfordern, einschliesslich des Einsatzes fortschrittlicher Sicherheitsanalysen:

# DORA (Digital Operational Resilience Act):

## 5 Säulen der DORA-Regulierung

| | |
|---|---|
| 01 | IKT-Risikomanagement |
| 02 | Vorfallsmeldung |
| 03 | Digitale Resilience-Tests |
| 04 | IKT-Drittparteien-Risikomanagement |
| 05 | Informationsaustausch |

Fokussiert auf EU-Finanzentitäten (Banken, Versicherer, Investmentfirmen), trat DORA mit vollständiger Anwendbarkeit im Januar 2025 in Kraft [37]. Es schreibt vor, dass Unternehmen robustes Sicherheitsmonitoring und Vorfallsbehandlung als Teil der operativen Resilienz aufrechterhalten.

Eine der strengen Anforderungen ist, dass **schwerwiegende Cyber-Vorfälle den Regulatoren innerhalb von Stunden nach der Klassifizierung als schwerwiegend gemeldet werden müssen** [11]. Das bedeutet, dass Banken und Finanzinstitute die Fähigkeit benötigen, Anomalien schnell zu erkennen und ihre Auswirkungen zu bewerten. Ohne automatisiertes Monitoring, das verdächtige Aktivitäten aufgreift, könnte eine Organisation nicht einmal bemerken, dass sie angegriffen wird, bis es zu spät ist, die Meldefrist einzuhalten. DORA zwingt BFSI-Unternehmen im Wesentlichen dazu, in Echtzeit-Erkennung zu investieren, weil manuelles oder Ad-hoc-Monitoring Vorfälle nicht schnell genug erkennen wird, um die Compliance zu erfüllen [11]. Darüber hinaus erwartet DORA, dass Unternehmen **umfassende IKT-Risikomanagement-Frameworks** haben, was impliziert, dass Logs aller kritischen Systeme überwacht werden sollten. Die Ära, bestimmte Legacy-System-Logs zu ignorieren, ist vorbei – wenn diese Systeme für den Betrieb wesentlich sind, fallen sie unter das Resilience-Framework und benötigen Anomalie-Monitoring.

DORA bringt auch Kontrolle über Drittanbieter (einschliesslich Cloud-Dienste) [38]. Finanzunternehmen müssen sicherstellen, dass ihre Sicherheitsdaten in der Cloud geschützt sind und dass sie Kontinuitätspläne haben, wenn ein Anbieter ausfällt.

Das deckt sich mit dem Datenschutzproblem: Regulatoren würden es nicht gern sehen, wenn eine Bank keine Rechenschaft über Sicherheitsdaten ablegen kann, die an eine externe Analyse-Cloud gesendet werden [39]. DORA drängt also sowohl auf verbesserte Analysen als auch auf sorgfältiges Anbieter-Management – eine schwierige Balance.

# NIS2 (EU-Netz- und Informationssicherheitsrichtlinie 2):

## 24h

Innerhalb von 24 Stunden müssen Organisationen eine ‚Frühwarnung' geben, dass ein schwerwiegender Cybersicherheitsvorfall vermutet wird.

## 72h

Innerhalb von 72 Stunden müssen Organisationen einen detaillierten Bericht über den Vorfall vorlegen.

## 1 Monat

Innerhalb von 1 Monat müssen Organisationen einen Abschlussbericht vorlegen, der den Vorfall, die Ursache und die Eindämmungsmassnahmen beschreibt.

NIS2, 2022 verabschiedet und bis 2025 von den Mitgliedstaaten umzusetzen, erweitert den Geltungsbereich verpflichtender Cybersicherheitspraktiken und Vorfallsmeldungen auf viele Sektoren. Sie erfasst nun mittlere/grosse Organisationen in Sektoren wie Fertigung, Gesundheitswesen, Energie, Transport, Finanzmarktinfrastruktur, öffentliche Verwaltung und mehr [40][41]. Eine Schlüsselanforderung ist die **24-Stunden-Erstbenachrichtigung** für schwerwiegende Vorfälle [12]. Das ist ein noch engeres Zeitfenster als viele gewohnt waren (das ursprüngliche NIS gab 72 Stunden). Um einen Vorfall innerhalb von 24 Stunden nach Bekanntwerden zu melden, müssen Organisationen fast sofort wissen, wenn etwas nicht stimmt – was wiederum kontinuierliches Monitoring unterstreicht.

NIS2 fordert explizit die Notwendigkeit angemessener **Risikomanagementmassnahmen, einschliesslich Erkennungsfähigkeiten und schneller Reaktion** [42].

Es legt sogar nahe, dass Entitäten SIEM-Lösungen in Betracht ziehen sollten, um Daten netzwerkübergreifend zu aggregieren und zu analysieren [43] – und ermutigt damit im Wesentlichen zur Einführung fortschrittlicher Sicherheitsanalysen für die Compliance.

Für Branchen wie Gesundheitswesen und Fertigung, die möglicherweise nicht die gleiche SOC-Reife wie Banken hatten, ist NIS2 ein Weckruf. Krankenhäuser müssen beispielsweise jetzt auf verdächtige Netzwerkaktivitäten überwachen, die auf Ransomware hinweisen könnten, und schnell melden. Dies kann angesichts der Ressourceneinschränkungen eine Herausforderung sein, daher ist Automatisierung der Schlüssel. Im Allgemeinen drängt NIS2 Unternehmen dazu, ‚dem Stand der Technik' entsprechende Cybersicherheitsmassnahmen zu implementieren – sicherlich passt die Nutzung KI-gesteuerter Sicherheitsanalysen in diese Beschreibung [44][45].

Organisationen betrachten Automatisierung als Compliance-Lebensader [46][47]: Tools einzusetzen, die Vorfälle mit minimaler menschlicher Intervention erkennen und sogar melden können, um die engen Zeitpläne nachhaltig einzuhalten.

# Andere Vorschriften und Standards:

Über DORA und NIS2 hinaus gibt es zahlreiche sektorspezifische oder nationale Regeln, die die Sicherheitsanforderungen erhöhen. In Deutschland beispielsweise schreiben das IT-Sicherheitsgesetz und BSI-Richtlinien für KRITIS (kritische Infrastruktur)-Betreiber kontinuierliches Monitoring und Vorfallsmeldung vor. Die USA haben Direktiven für Pipeline- und Versorgungssicherheit, die Anomalieerkennung erfordern. Der globale Bankensektor betont über Basel/IOSCO operative Resilienz, zu der auch Cyber-Angriffserkennung gehört. Selbst Datenschutzbestimmungen wie die DSGVO erfordern indirekt gutes Sicherheitsmonitoring – eine Verletzung personenbezogener Daten muss innerhalb von 72 Stunden gemäss DSGVO gemeldet werden, was wiederum impliziert, dass Sie innerhalb dieses Zeitrahmens wissen müssen, dass eine Verletzung vorlag. All dies schafft ein regulatorisches Umfeld in 2026, in dem das Fehlen fortschrittlicher Bedrohungserkennung nicht nur ein Sicherheitsrisiko, sondern auch ein Compliance-Risiko ist.

**Eine besondere Herausforderung ist die Ressourcenbelastung durch Compliance-Berichterstattung.** Vorschriften wie DORA und NIS2 erfordern detaillierte Berichterstattung und manchmal kontinuierliche Aktualisierungen. Wenn Organisationen keine Tools haben, um die relevanten Daten (z. B. Logs, Indikatoren, betroffene Systeme) für einen Vorfallsbericht automatisch zusammenzustellen, müssen sie dies möglicherweise manuell unter engen Fristen zusammenstellen. Dies kann extrem arbeitsintensiv sein – Log-Dateien zusammenstellen, Ereignisse korrelieren, Vorfallsbeschreibungen verfassen – und potenziell das SOC davon ablenken, tatsächlich auf die Bedrohung zu reagieren. Beispielsweise erfordert NIS2 einen Folgebericht innerhalb von 72 Stunden und einen Abschlussbericht innerhalb eines Monats [48][49], was mehrere Dokumentationsphasen bedeutet. Unternehmen sind daher zunehmend an Lösungen interessiert, die compliance-fähige Berichte oder Audit-Logs als Nebenprodukt ihres Monitorings generieren können. Tatsächlich bieten einige Anbieter jetzt Funktionen wie ‚Ein-Klick-Regulatorische-Berichterstattung' für Vorfälle [50], die die Details ausgeben können, die zur Benachrichtigung der Behörden benötigt werden. Automatisierung in diesem Bereich ist entscheidend – andernfalls könnte der Aufwand zur manuellen Compliance-Einhaltung viele Personalressourcen ‚binden'. Sicherheitsteams könnten sich dabei ertappen, mehr Berichte zu schreiben als Bedrohungen zu jagen, wenn man nicht aufpasst.

Automatisierung ist entscheidend, sonst bindet manuelle Compliance wertvolle Ressourcen.

# Der Ausblick 2026

Zusammenfassend sind regulatorische und datenschutzrechtliche Faktoren ein zweischneidiges Schwert: Sie zwingen Organisationen dazu, Sicherheitsoperationen zu verbessern (gut zur Motivierung von Investitionen), schränken aber auch ein, wie diese Operationen umgesetzt werden können, und fügen Overhead hinzu. Die führenden Organisationen gehen dies proaktiv an – zum Beispiel haben viele europäische Banken die letzten 2 Jahre damit verbracht, ihr SIEM und ihre Analysen zu aktualisieren, in Kenntnis dessen, dass DORA in Kraft treten würde. Ebenso führen Unternehmen unter NIS2 Lückenanalysen durch, um sicherzustellen, dass sie die Monitoring-Tools und Incident-Response-Pläne haben, die zur Erfüllung der 24-Stunden-Regel erforderlich sind [42].

Wir sehen auch zunehmende funktionsübergreifende Zusammenarbeit: Compliance-Beauftragte, Datenschutzbeauftragte und CISOs arbeiten zusammen, um Lösungen auszuwählen, die sowohl Sicherheitsziele als auch rechtliche Anforderungen erfüllen. Ein positives Ergebnis dieser Druckfaktoren ist, dass sie Standardisierung und Dokumentation fördern. Mit dem Übergang zu 2026 können wir erwarten, dass die regulatorische Kontrolle der Cybersicherheit nur zunimmt – aber Organisationen, die Compliance als Chance nutzen, um eine starke, datenschutzbewusste Sicherheitsanalyse-Fähigkeit aufzubauen, profitieren nicht nur durch Vermeidung von Bussgeldern, sondern auch durch besseren Schutz der Daten und des Vertrauens ihrer Stakeholder.

# Fazit und Ausblick für 2026

Da sich Unternehmen in allen Sektoren auf die sich entwickelnde Cyber-Bedrohungslandschaft vorbereiten, ist klar, dass traditionelle Sicherheitsansätze intelligenteren, integrierten Strategien weichen müssen. Die besprochenen Trends – von Shadow IT und Insider-Bedrohungen bis hin zu SOC-Überlastung und neuen Vorschriften – zeigen alle auf ein gemeinsames Thema hin: den Bedarf an umfassendem, adaptivem Sicherheitsmonitoring. Organisationen in BFSI, Fertigung, Gesundheitswesen, Regierung und darüber hinaus erkennen, dass Sicherheit nicht mehr nur darum geht, die Angreifer am Perimeter abzuwehren; es geht darum, kontinuierlich zu beobachten, was im Inneren passiert, riesige Datenmengen in Echtzeit zu verstehen und schnell auf die geringsten Anzeichen von Problemen zu reagieren.

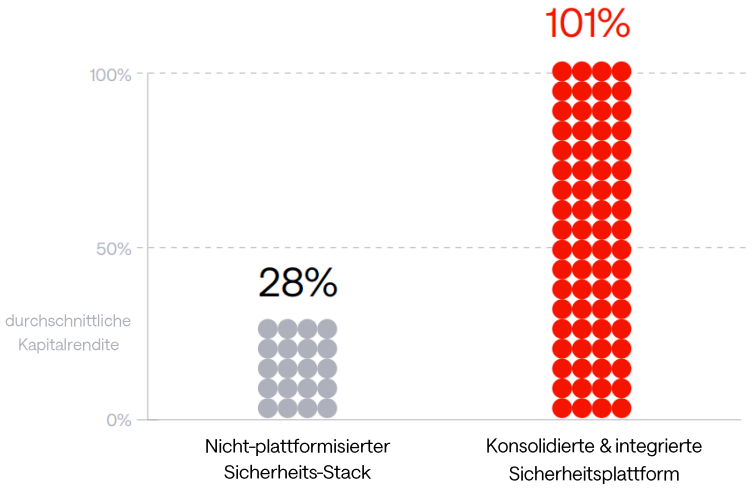
## Für 2026 sind mehrere wichtige Entwicklungen zu erwarten:

### Breitere Einführung KI-gestützter Analysen

KI und maschinelles Lernen werden eine noch grössere Rolle in Cybersicherheitsoperationen spielen. Wir erwarten einen verstärkten Einsatz von Verhaltensanalysen nicht als eigenständige Tools, sondern eingebettet in breitere Plattformen. Fortschrittliche Algorithmen, einschliesslich neuer GenAI-Techniken, helfen dabei, Angriffsmuster zu erkennen und Anomalien schneller zu priorisieren. Beispielsweise könnte KI ein zuvor ungesehenes Muster von Insider-Exfiltration identifizieren, indem es mit erlerntem Verhalten über viele Abteilungen innerhalb der Organisation vergleicht. Das Katz-und-Maus-Spiel wird weitergehen – Angreifer rüsten sich ebenfalls mit KI – aber defensiv eingesetzte KI bietet die Chance, das Spielfeld zu ebnen, insbesondere für ressourcenschwache Teams.

## Konvergenz von Sicherheitstools

Die Ära isolierter Sicherheitsprodukte geht zu Ende. Unternehmen werden zunehmend **smarte Integrationen** fordern, die Logging, Erkennung (SIEM/UEBA/NDR), Reaktion (SOAR) und sogar Wiederherstellungs-Workflows optimieren und vereinfachen. Diese Konsolidierung wird nicht nur durch Effizienzanforderungen, sondern auch durch ROI angetrieben – Studien zeigen, dass Organisationen, die Sicherheitstools konsolidieren und integrieren, deutlich höhere Renditen auf Sicherheitsinvestitionen und eine schnellere Vorfallsbearbeitung sehen [31][32]. Man kann sich eine zukünftige SOC-Plattform vorstellen, wo ein Alarm automatisch eine Anreicherung aus Bedrohungsintelligenz auslöst, Compliance-Berichterstattungsvorlagen überprüft und Behebungsschritte vorschlägt – alles in einer Oberfläche. Die grossen Akteure der Branche bewegen sich bereits in diese Richtung, und bis 2026 werden viele mittelgrosse bis grosse Unternehmen wahrscheinlich zu einer integrierten Sicherheitsarchitektur migriert sein. Dies sollte schrittweise die Probleme der Alarmmüdigkeit und blinden Flecken reduzieren, da alles in ein Gehirn eingespeist wird, sozusagen.




Organisationen mit konsolidierten Sicherheitsplattformen sehen einen durchschnittlichen ROI, der 4-mal besser ist als bei Nicht-Anwendern.

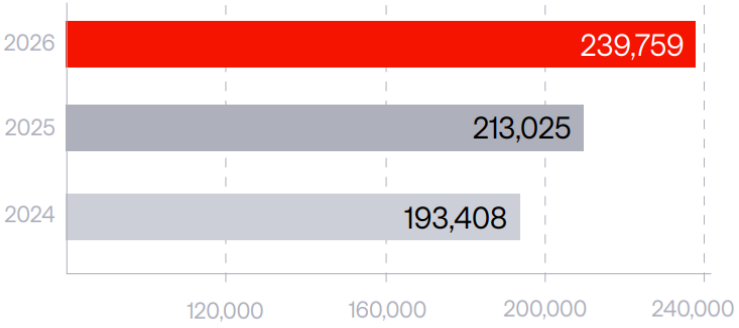
## Zero Trust und identitätsfokussierte Sicherheit

Da Insider und Zugangsdatenmissbrauch zu den grössten Bedrohungen gehören, werden Organisationen die Zero-Trust-Prinzipien verstärken. Identität wird der neue Perimeter sein, was bedeutet, dass kontinuierliches Monitoring von Benutzer- und Service-Account-Aktivitäten entscheidend ist. UEBA liefert den Verhaltenskontext für Identity Threat Detection and Response (ITDR) sowie Zero Trust und zeigt, ob sich eine gültige Identität wie erwartet verhält. In der Praxis werden wir mehr Einsatz von Identitätsanalysen, privilegiertem Zugriffsmonitoring und bedingten Zugriffskontrollen sehen, die sich basierend auf der Risikobewertung des des Benutzerverhaltens in Echtzeit anpassen. Dies knüpft an unsere Diskussion über übersehene Insider-Bedrohungen an – bis 2026 zielen viele Unternehmen darauf ab, abnormale Benutzeraktionen zu erkennen, bevor sie eskalieren. Diese proaktive Haltung minimiert Schäden durch Insider-Bedrohungen.

## Compliance als Katalysator für Verbesserung

Die neuen regulatorischen Anforderungen (DORA, NIS2 usw.), die in Kraft treten, werden bis 2025–2026 ihre Durchsetzungsphase erreichen. Wir antizipieren einige hochkarätige regulatorische Massnahmen (Bussgelder oder Sanktionen) gegen Organisationen, die Vorfälle erleiden und als nicht konform befunden werden, was als abschreckende Beispiele dienen wird. Umgekehrt werden Organisationen Zertifizierungen oder Bescheinigungen der Resilienz als Wettbewerbsdifferenziator anstreben – zum Beispiel könnte eine Bank, die sagen kann, dass sie DORA erfüllt und über ein modernes Monitoring verfügt, mehr Vertrauen von Kunden und Partnern gewinnen. Im breiteren Markt werden die Ausgaben für Cybersicherheit voraussichtlich weiter steigen (die globalen Sicherheitsausgaben werden voraussichtlich 213 Mrd. USD in 2025 erreichen, gegenüber 193 Mrd. USD in 2024 [51]). Der Fokus dieser Ausgaben wird sich wahrscheinlich auf Lösungen verlagern, die nicht nur Verstösse verhindern, sondern auch die Compliance optimieren. Automatisierung der Berichterstattung, audit-fähige Protokollierung und klare Metriken werden Verkaufsargumente sein. Unternehmen werden Anbieter bevorzugen, die **Datenresidenz-Optionen** anbieten und nachweisen können, dass ihre Tools nicht gegen Datenschutzgesetze verstossen.

Die Ausgaben werden voraussichtlich um 12,5 % in 2026 auf insgesamt 240 Mrd. USD steigen.




Ausgaben für Informationssicherheit weltweit 2024-2026 (Millionen US-Dollar)

## Menschliches Element und Prozess

Trotz aller Technologie bleibt das menschliche Element entscheidend. Es wächst die Erkenntnis, dass **die Kultivierung qualifizierter Cyber-Talente** und die Vermeidung von Analysten-Burnout Teil der Resilienz sind. In 2026 und darüber hinaus können Unternehmen erwartet werden, in das Wohlbefinden ihrer Sicherheitsteams zu investieren – sei es durch bessere Ausbildung, Arbeitslastmanagement oder sogar psychische Gesundheitsunterstützung angesichts der berichteten Stressniveaus. Eine Sicherheitskultur wird Organisationen tiefer durchdringen, mit regelmässigen Übungen, unternehmensweitem Bewusstsein und Überwachung des Cyber-Risikos auf Vorstandsebene (Vorstände in DACH und anderswo sind aufgrund des regulatorischen Drucks bereits stärker engagiert [52][53]).

# Fazit

Die kommenden Jahre werden von tiefgreifenden Veränderungen in Cybersicherheitspraktiken geprägt sein. Unternehmen, die sich proaktiv anpassen – indem sie bisher unbekannte Bereiche ihrer IT-Umgebung ins Rampenlicht rücken, auf intelligente Automatisierung setzen und sich neuen Vorschriften anpassen –, werden nicht nur Bedrohungen wirksamer abwehren, sondern auch effizienter arbeiten. Diejenigen, die hinterherhinken, werden feststellen, dass sowohl Angreifer als auch Aufsichtsbehörden an ihre Tür klopfen.

**Für einen CISO oder Leiter IT-Risiko, der dies liest, ist die Botschaft klar:** Jetzt ist die Zeit, blinden Flecken zu eliminieren, Insider Threats frühzeitig zu erkennen, das SOC zu entrümpeln und sicherzustellen, dass die Abwehr (und Vorfallsberichte) für alles bereit sind, was als nächstes kommt.

Finanzielle Verluste, Reputationsschäden und Compliance-Strafen erhöhen den Handlungsdruck. Gleichzeitig bieten intelligente Security Analytics und ein klarer strategischer Fokus die Chance, die Cyber-Resilienz nachhaltig zu stärken.

# Quellen


01. **Auvik, 50 wesentliche Shadow-IT-Statistiken für 2024 – Verbreitung und Risiken von Shadow IT** (nicht genehmigte SaaS-Apps, Ausgaben) [2][3][14].

02. **Vectra AI, Bericht zum Stand der Bedrohungserkennung 2023 – SOC-Alarmvolumen und blinde Flecken** (durchschnittliche tägliche Alarme, % ignoriert; Sichtbarkeitsbedenken) [8][54].

03. **DeepStrike (Khalil, 2025), Insider-Bedrohungsstatistiken 2025 – Häufigkeit und Kosten von Insider-Bedrohungen** (83% Erfahrungsrate, durchschnittliche Kosten 17,4 Mio. USD, 81-Tage-Eindämmung, Ursachen) [7][5].

04. **Cybersecurity Insiders, Insider-Bedrohungsbericht 2024 (via Gurucul) – Zunahme der Insider-Vorfälle** (48% sahen Anstieg im letzten Jahr und Komplexität als Treiber) [24].

05. **Trend Micro Umfrage (via IT Europa, 2021) – SOC-Überlastungsstatistiken** (51 % Teams von Alarmen überwältigt, 55 % nicht sicher in der Reaktion, 27 % Zeit für Falschmeldungen) [9].

06. **IBM Institute for Business Value, Security Platformization Report (2024) – Tool-Fragmentierung und Komplexität** (83 Sicherheitslösungen im Durchschnitt; 52% sagen Komplexität behindert Betrieb; 74% sagen Arbeitslast übermässig) [10][33].

07. **Observo Blog (Turriff, 2023), SIEM-Kosten senken & Datenrauschen reduzieren – Log-Wert und blinde Flecken** (80% der Logs mit geringem Wert; Entfernen von Quellen aufgrund von Kosten erzeugt blinde Flecken) [17][55][16].

08. **Check Point Research, Q1 2025 Cyber-Angriffsreport – Bedrohungsanstiegraten** (47% jährlicher Anstieg der Angriffe pro Organisation, 1925 wöchentlicher Durchschnitt) [1].

09. **InnReg, DORA-Regulierung erklärt (2023) – DORA-Anforderungen** (Januar 2025 in Kraft; Vorfallsmeldung innerhalb von Stunden; Bedarf an robustem Monitoring) [37][11].

10. **Snare Solutions, Überprüfung der NIS2-Richtlinie (2023) – NIS2-Anforderungen** (24-Stunden-Vorfallsbenachrichtigung vs. 72h; Mandat für bessere Erkennungstools wie SIEM) [56][12][43].

11. **FutureMarketReport, UEBA Software Marktausblick 2032 – UEBA-Trends** (Cloud vs. On-Premises-Einführung, datenschutzerhaltende Analysen für Compliance, branchenspezifische Bedürfnisse) [57][36].

12. **ManageEngine, Evolution von SIEM in 2025 (2025) – Moderne SIEM-Fähigkeiten** (KI-gesteuerte Analysen, Integration von UEBA für fortgeschrittene Bedrohungserkennung) [58][59].

13. **Check Point, 2025 Cybersicherheitsreport – Globale Ausgaben und Prioritäten** (Prognostizierte 213 Mrd. USD Sicherheitsausgaben in 2025; KI und einheitliche Plattformen entstehend) [51].

14. **Wing Security, Bekämpfung von KI-Sicherheitsbedrohungen in SaaS-Umgebungen von Lia Ciner, Okt 2023** [60].


exeon