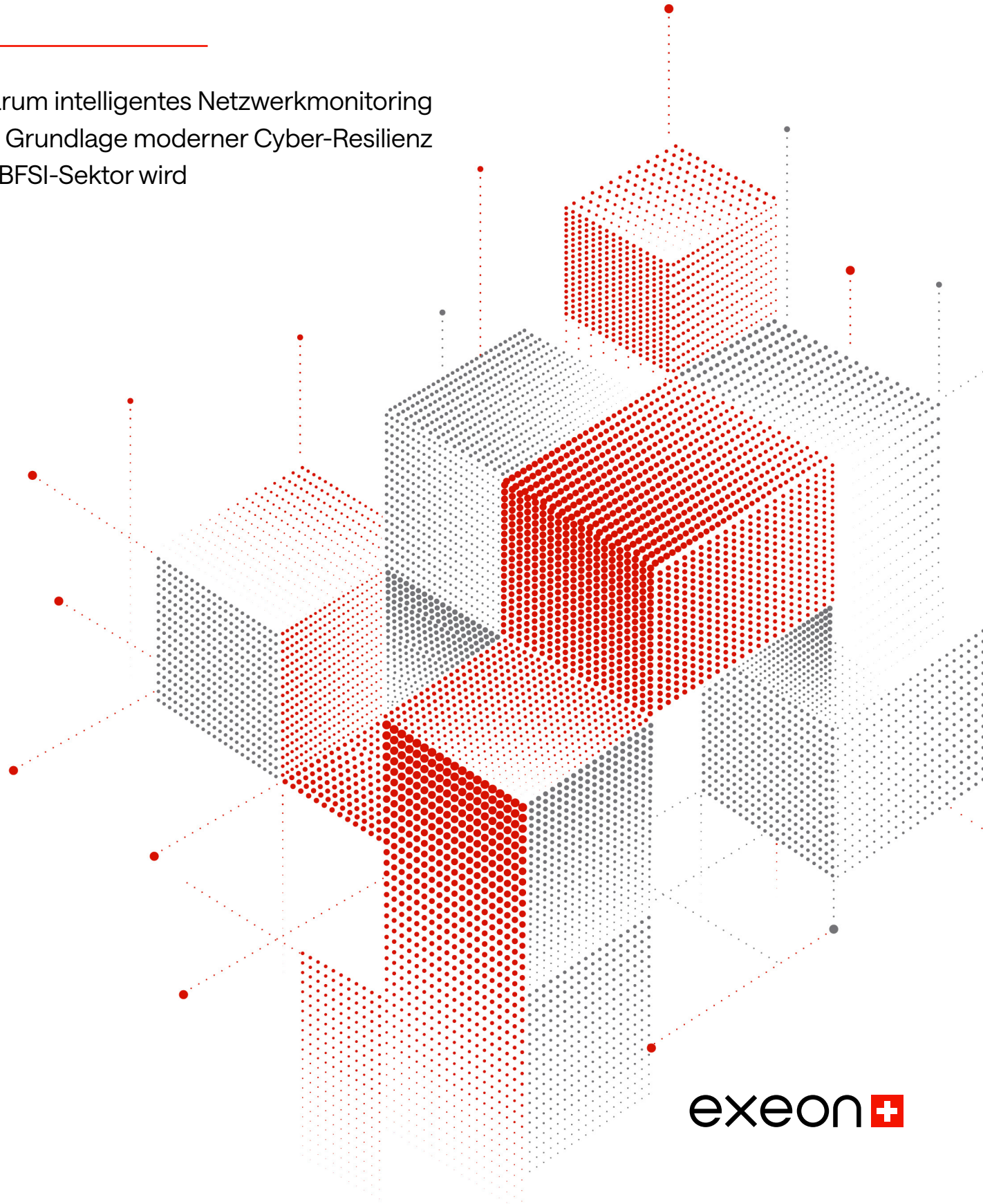
Branchenstatistikbericht 2026–2027 für CISOs, SOC-Leiter, CIOs und Compliance-Verantwortliche

Von Datenüberlastung zu Resilienz

Warum intelligentes Netzwerkmonitoring zur Grundlage moderner Cyber-Resilienz im BFSI-Sektor wird

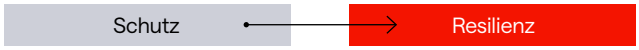


exeon

Executive Introduction

BFSI-Research-Report

Mit der zunehmenden Digitalisierung und Vernetzung des BFSI-Sektors verändern sich auch die Anforderungen an Cyber-Resilienz grundlegend.



Anforderungen an Finanzinstitute

Finanzinstitute müssen heute:

- Hybride IT/OT- und Multi-Cloud-Umgebungen absichern
- DORA- und NIS2-Anforderungen erfüllen
- Geopolitische Risiken und Datensouveränität berücksichtigen
- Betriebliche Kontinuität auch unter Sicherheitsvorfällen sicherstellen

2026–2027 markiert einen strategischen Wendepunkt

Sicherheitsverantwortliche werden heute nicht mehr nur daran gemessen, Angriffe zu verhindern – sondern den Geschäftsbetrieb trotz Angriffen aufrechtzuerhalten.

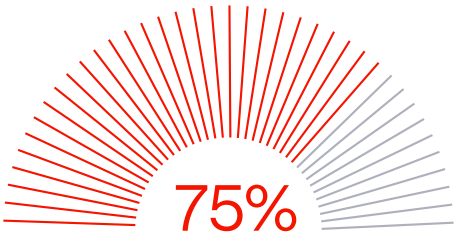
Vertiefende Einblicke

Dieser Bericht fasst aktuelle Daten, Markttrends und strategische Erkenntnisse zusammen, um die Entscheidungsverantwortliche in den Bereichen Sicherheit, IT und Compliance zu unterstützen.

1. Transparenzlücken und operative Komplexität

Am relevantesten für: CIOs / Compliance-Verantwortliche
Auch relevant für: CISOs

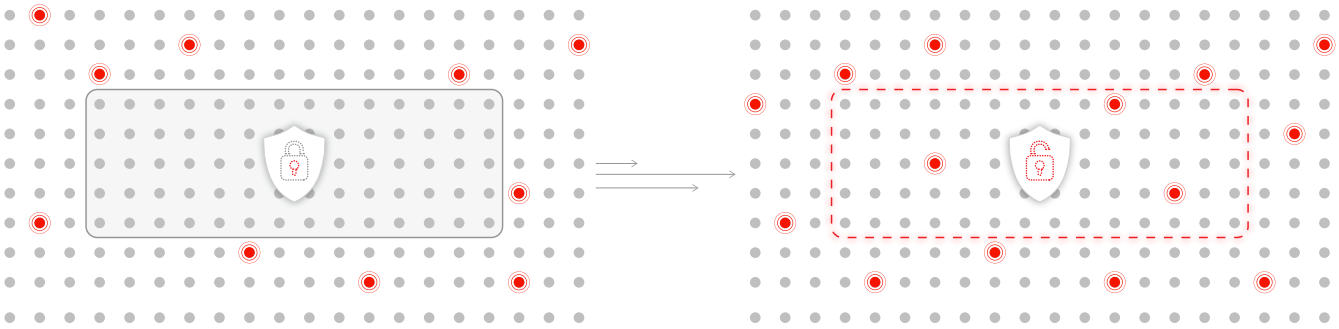
Moderne BFSI-Umgebungen sind zunehmend verteilt, hybrid und schwer überschaubar geworden. Klassische Monitoring-Ansätze stossen dabei häufig an ihre Grenzen.



der BFSI-Unternehmen verzeichneten Compliance-Probleme im Zusammenhang mit Schatten-IT oder nicht verwalteten Assets (KPMG, 2024)

Zentrale Kennzahlen und Trends

68%	der Unternehmen berichten von kritischen Transparenzlücken in hybriden Cloud-Umgebungen (IBM Security, 2024).
75%	der BFSI-Unternehmen verzeichneten Compliance-Probleme im Zusammenhang mit Schatten-IT oder nicht verwalteten Assets (KPMG, 2024).
80%+	des Netzwerkverkehrs sind inzwischen verschlüsselt — weniger als die Hälfte wird effektiv überwacht (Zscaler, 2025).
60%+	der vernetzten OT-/IoT-Geräte in Finanzumgebungen nutzen veraltete oder nicht mehr unterstützte Software (SANS, 2024).
60%+	mehr API-bezogene Angriffe im Finanzsektor im Jahresvergleich (Salt Security, 2025).



Strategische Auswirkungen

Die Angriffsfläche geht heute weit über den klassischen ‚Perimeter hinaus und umfasst: Cloud-Workloads, APIs, Partner-Ökosysteme, OT-Systeme, Ost-West-Datenverkehr.

Sichtbarkeit muss heute kontinuierlich und kontextbasiert über hybride Umgebungen hinweg erfolgen.

Massnahmen

Setzen Sie auf KI-gestützte Netzwerkerkennungsplattformen, die:

1 Transparenz über IT-, OT- und Cloud-Assets schaffen

2 Verschlüsselten Datenverkehr kontextbasiert analysieren

3 Transparenz über API- und Ost-West-Verkehr schaffen

2. Moderne Bedrohungen machen Sicherheitsvorfälle unvermeidbar

Am relevantesten für: CISOs / SOC-Leiter
Auch relevant für: CIOs

Angreifer agieren schneller, anpassungsfähiger und nutzen zunehmend KI-gestützte Methoden.

70 %+ der Finanzinstitute sind jährlich von Ransomware betroffen

Zentrale Kennzahlen und Trends

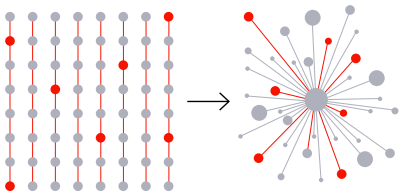
62%	der Malware im Jahr 2025 ist polymorph oder bisher unbekannt (CrowdStrike, 2025).
70%+	der Finanzinstitute sind jährlich von Ransomware betroffen (Sophos, 2025).
~80	Tage bleiben Sicherheitsvorfälle im Finanzsektor durchschnittlich unentdeckt (IBM, 2024).
83%	der Unternehmen verzeichneten 2024–2025 mehr als einen Sicherheitsvorfall (IBM, 2025).

Die Hälfte der CISOs wird Sicherheitsprogramme bis 2028 stärker auf Cyber-Resilienz ausrichten

Gartner-Einblick

Bis 2028 werden laut Gartner rund die Hälfte der CISOs ihre Cybersecurity-Programme stärker an Cyber-Resilienz ausrichten.

Der Fokus verschiebt sich zunehmend: weg von der vollständigen Vermeidung aller Vorfälle hin zur Minimierung operativer Auswirkungen.



Von statischem Schutz zu kontext- und verhaltensbasierter Sicherheit

Strategische Auswirkungen

Sicherheitsvorfälle gelten zunehmend als unvermeidbar – operative Unterbrechungen jedoch nicht.

Unternehmen müssen statische Schutzmechanismen durch verhaltens- und kontextbasierte Erkennung ergänzen.

Massnahmen

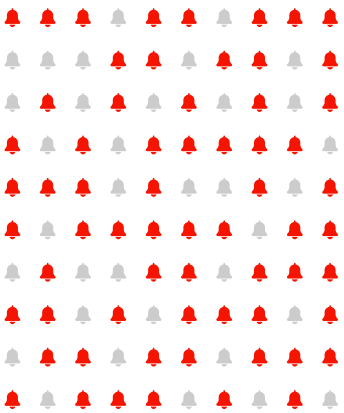
1 Verhaltens- und Anomalieerkennung stärken

2 Kontinuierliches Threat Hunting integrieren

3 Incident Response stärker auf Geschäftskontinuität ausrichten

3. SOC-Effizienz im Zeitalter des Fachkräftemangels

Am relevantesten für: CIOs / SOC-Leiter
Auch relevant für: CISOs



65%

der Alarme sind Fehlalarme
(Palo Alto Networks, 2025)

Sicherheitsteams stehen zunehmend unter Druck – nicht nur durch Bedrohungen, sondern auch durch operative Komplexität und Fachkräftemangel.

Zentrale Kennzahlen und Trends

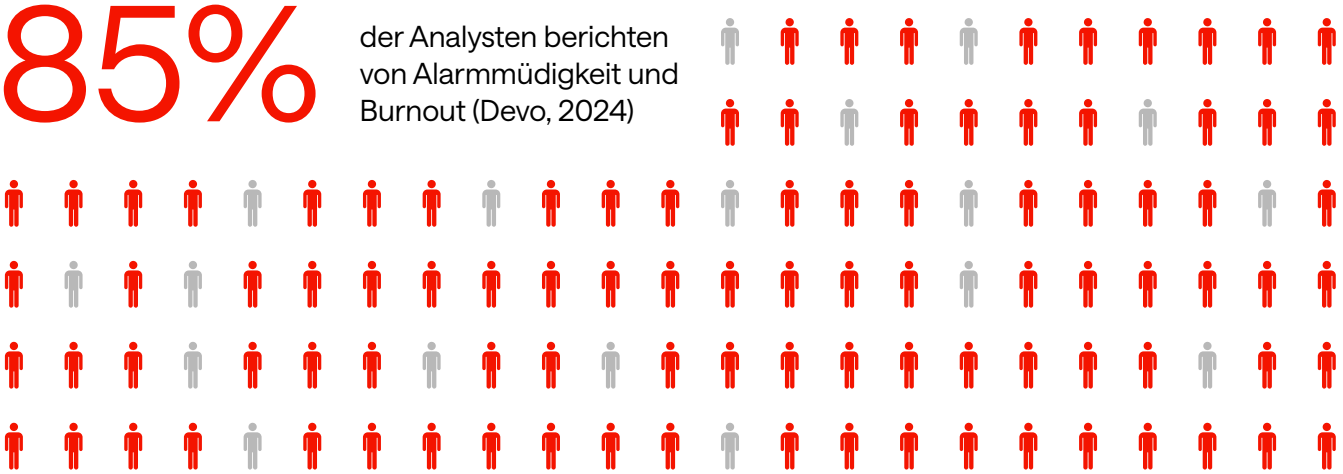
85% der Analysten berichten von Alarmmüdigkeit und Burnout (Devo, 2024).

65% der Alarme sind Fehlalarme (Palo Alto Networks, 2025).

40-50 Sicherheitstools betreiben Unternehmen heute durchschnittlich – oft mit begrenzter Integration (IBM, 2024).

4+ Millionen Cybersecurity-Fachkräfte fehlen weltweit (ISC2, 2024).

85% der Analysten berichten von Alarmmüdigkeit und Burnout (Devo, 2024)



Gartner-Einblick

Bis 2028 werden 40% der Cybersicherheitsverantwortlichen Resilienzmassnahmen stärker auf kritische Geschäftsdienste ausrichten.

Strategische Auswirkungen

Das SOC der Zukunft wird stärker automatisiert und gezielter auf geschäftskritische Risiken ausgerichtet sein.

Massnahmen

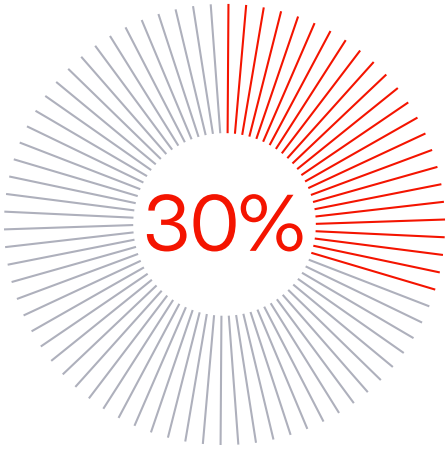
1 Sicherheitswerkzeuge konsolidieren und integrieren (XDR / NDR+)

2 Tier-1-Triage mit SOAR automatisieren

3 Alarme nach geschäftlicher Relevanz priorisieren

4. Regulierung, Souveränität und geopolitische Risiken

Am relevantesten für: CIOs / Compliance-Verantwortliche
Auch relevant für: CISOs



der Unternehmen werden bis 2027 souveräne Cloud-Sicherheitskontrollen benötigen (Gartner)

Cybersicherheit wird zunehmend zu einem strategischen und geopolitischen Thema.

Zentrale Kennzahlen & Trends

30% der Unternehmen werden bis 2027 souveräne Cloud-Sicherheitskontrollen benötigen (Gartner).

DORA und NIS2 erfordern unter anderem:

01 Incident Reporting innerhalb von 24-72 Stunden

02 Governance von Drittanbieterrisiken

03 Verpflichtende Resilienztests

70% der Finanzinstitute sehen geopolitische Risiken als wesentlichen Treiber ihrer Cybersecurity-Strategie (World Economic Forum, 2025).

Geopolitischer Kontext

Cybersicherheit wird zunehmend zu einem strategischen und geopolitischen Thema – und ist längst nicht mehr nur eine technische Disziplin.

Steigende geopolitische Spannungen führen zu neuen Anforderungen an Sicherheits- und Datenarchitekturen. Dazu gehören insbesondere:

- Anforderungen zur Datenlokalisierung
- Einschränkungen bei grenzüberschreitenden Datenübertragungen
- Stärkere Kontrolle von Drittanbietern und Lieferketten

Strategische Auswirkungen

Zentrale Anforderungen:

- Kontrolle über Datenstandorte und Sicherheitsoperationen sicherstellen
- Drittanbieter- und Lieferkettenrisiken kontinuierlich überwachen
- Regionale regulatorische Anforderungen erfüllen

Massnahmen

Setzen Sie auf souveränitätsbewusste Architekturen mit:

1 Regionsspezifische Datenverarbeitung

2 Transparente Kontrolle über Protokolle und Telemetriedaten

3 Integriertes Drittanbieter-Risikomanagement

5. Die neue Rolle des CISO

Am relevantesten für: CISOs
Auch relevant für: CIOs / Risikomanagement

Neue Anforderungen an CISOs

- Cyber-Risikomanagement
- Strategische Business-Integration
- Regulatorische Anforderungen & Compliance
- Krisenmanagement
- Incident Response
- Entscheidungsprozesse
- Zero-Trust-Architekturen

Vom Schutzverantwortlichen zur resilienzorientierten Führungskraft – die Erwartungen an CISOs verändern sich grundlegend.

Zentrale Entwicklungsbereiche

Minimum Viable Security: Fokus auf Schadensbegrenzung und betriebliche Kontinuität statt auf perfekten Schutz.
Cyber-Resilienz als Kernauftrag: Cybersicherheit wird enger mit Betriebsstabilität, Wiederherstellung und betrieblicher Resilienz verknüpft.
Wertschöpfung: CISOs unterstützen zunehmend digitale Geschäftsmodelle und Innovationsinitiativen.

“Von CISOs wird heute nicht mehr erwartet, jede Sicherheitsverletzung zu verhindern — sondern den Geschäftsbetrieb trotz Vorfällen aufrechtzuerhalten.”

Gartner-Einblick

50% der CISOs werden bis 2028 neben Incident Response auch Verantwortung für Disaster Recovery übernehmen.

Strategische Auswirkungen

CISOs entwickeln sich zunehmend zu:

1 Resilienzorientierten Führungskräften

2 Funktionsübergreifenden Koordinationsinstanzen

3 Treibern von Vertrauen und Wettbewerbsfähigkeit

Von Datenüberlastung zu Resilienz
Branchenstatistikbericht 2026–2027

Wie sich Netzwerkerkennung & Sicherheitsmonitoring weiterentwickeln

Das moderne Netzwerk

Klassische Perimeter-Modelle verlieren an Relevanz.

Remote-Mitarbeiter, Filialen, Cloud-Workloads, SaaS-Anwendungen und OT-Umgebungen (Operational Technology) kommunizieren heute zunehmend über identitätsbasierte und Zero-Trust-orientierte Architekturen statt über klar abgegrenzte Netzwerke.

Sichtbarkeit über diese verteilten Kommunikationswege hinweg wird immer wichtiger, da Angriffe zunehmend VPNs, SD-WANs, APIs und Ost-West-Cloud-Datenverkehr durchqueren — oft lange bevor sie ein klassisches Gateway erreichen.

Was sich verändert hat

- Netzwerke sind heute identitäts- und zugriffsgesteuert statt rein standortbasiert
- Datenverkehr verläuft zunehmend lateral (Ost-West)
- Nord-Süd-Verkehr ist nicht mehr das dominante Kommunikationsmodell
- Kritische Assets verteilen sich über IT-, Cloud-, SaaS- und OT-Umgebungen hinweg

Neue Anforderungen

Datensouveränität erfordert Transparenz darüber, wo Daten verarbeitet und überwacht werden.

Geopolitische Fragmentierung erhöht den Bedarf an regional kontrollierten Infrastrukturen.
Drittanbieter- und API-Ökosysteme erweitern das effektive Netzwerk über organisatorische Grenzen hinaus.

Strategische Auswirkungen

Sicherheitsteams benötigen **vollständige Transparenz über Kommunikationspfade in hybriden Umgebungen** — einschliesslich verschlüsseltem und lateralem Datenverkehr — und müssen gleichzeitig regulatorische sowie souveränitätsbezogene Anforderungen erfüllen.

Das moderne SIEM

Moderne SIEM-Plattformen gehen heute weit über klassische Protokollverwaltung hinaus.

Moderne SIEM-Plattformen integrieren heute IT- und OT-Telemetrie, Cloud-APIs, Identitätsdaten und Geschäftsprozessinformationen in einer zentralen Plattform für Echtzeiterkennung, Compliance und operative Sicherheitssteuerung.

Automatisierung und SOAR-Orchestrierung ersetzen zunehmend statische Regelwerke durch risikobasierte und kontextorientierte Workflows und helfen Analysten, schneller priorisierte Entscheidungen zu treffen.

Was sich verändert hat

- SIEM entwickelt sich vom Protokoll-Repository zur Daten- und Analyseplattform
- Verhaltensanalysen und Threat Intelligence ergänzen klassische Erkennungsmethoden
- Automatisierung reduziert manuelle Triage-Prozesse und beschleunigt die Reaktion

Neue Anforderungen

Resilienzmetriken wie Reaktionszeit, Eindämmung und Wiederherstellung gewinnen an Bedeutung.
DORA und NIS2-Anforderungen erfordern durchgängige Sichtbarkeit und prüfungsfähige Berichterstattung.
Datenkontrolle und Souveränität erfordern Transparenz über Speicherung und Verarbeitung von SIEM-Daten.

Bedeutung für Security-Teams:

SIEM entwickelt sich vom Protokoll-Repository zur Daten- und Analyseplattform.

Was moderne Sicherheits-plattformen leisten müssen

(Die “NDR+”-Realität)

Analytikerkategorien wie IDS, NDR, NDV, SIEM und SOAR entwickeln sich zunehmend weiter, überschneiden sich funktional und wachsen zusammen.

Die Entwicklung geht klar in Richtung: “NDR is dead, long live NDR+.”

Wichtige Plattformfunktionen

Gemeint ist die Entwicklung hin zu integrierten Plattformen, die folgende Fähigkeiten kombinieren:

- Netzwerksichtbarkeit
- Erweiterte Analytik
- Automatisierte Reaktion
- Operativer Kontext

Kernfähigkeiten moderner Sicherheitsplattformen

- **Vollständige Transparenz** über On-Prem-, Cloud-, SaaS- und OT-Umgebungen hinweg
- **Analyse verschlüsselter** Datenströme ohne Performance- oder Compliance-Einschränkungen
- **Verhaltensbasierte Erkennung** unbekannter und sich entwickelnder Bedrohungen
- **Integrierte Korrelation und Case Management** zur Reduzierung von Tool-Fragmentierung
- **Automatisierte Reaktion** und Playbook-Ausführung zur Verbesserung der SOC-Effizienz

Neue Anforderungen

Resilienzorientierte Architektur: Lösungen müssen nicht nur Erkennung, sondern auch Eindämmung und Wiederherstellung unterstützen.
Souveränitätsbewusstes Design: Unternehmen benötigen Kontrolle über Datenspeicherort, Verarbeitung und Zugriff.
Priorisierung nach Geschäftskontext: Der Fokus verlagert sich vom Schutz aller Assets hin zum Schutz kritischer Geschäftsprozesse und Dienste.
Intelligente Spezialisierung statt Konsolidierung: Anstatt sämtliche Funktionen in einer einzigen Plattform zu bündeln, setzen Unternehmen zunehmend auf spezialisierte Systeme wie NDR oder UEBA, die ergänzend zum SIEM eingesetzt werden, um:

- Hochvolumige Telemetriedaten effizient zu filtern und anzureichern
- Spezifische Bedrohungsklassen präziser zu erkennen
- Alarmrauschen und Datenaufnahmekosten zu reduzieren
- Nur hochwertige, kontextreiche Erkennung an SIEM- und SOAR-Plattformen weiterzuleiten

Bedeutung für moderne Sicherheitsarchitekturen:

Die Zukunft liegt nicht in vollständiger Zentralisierung, sondern in schlanken, integrierten Sicherheitsarchitekturen, in denen spezialisierte Erkennungssysteme die Signalqualität verbessern und nahtlos mit bestehenden SIEM-, SOAR- und Endpoint-Lösungen zusammenarbeiten.

Fazit: Von Erkennung zu Resilienz

Cybersicherheit im BFSI-Sektor bedeutet heute nicht mehr ausschliesslich, Angriffe zu verhindern — sondern auch unter Sicherheitsvorfällen die betriebliche Kontinuität aufrechtzuerhalten.

Erweiterte Analyseplattformen und automatisierte Bedrohungserkennung helfen Unternehmen, Risiken zu reduzieren, Alarmrauschen zu minimieren, Sicherheitsoperationen effizienter zu gestalten und Betriebsstabilität zu stärken.

Für CISOs & SOC-Leiter

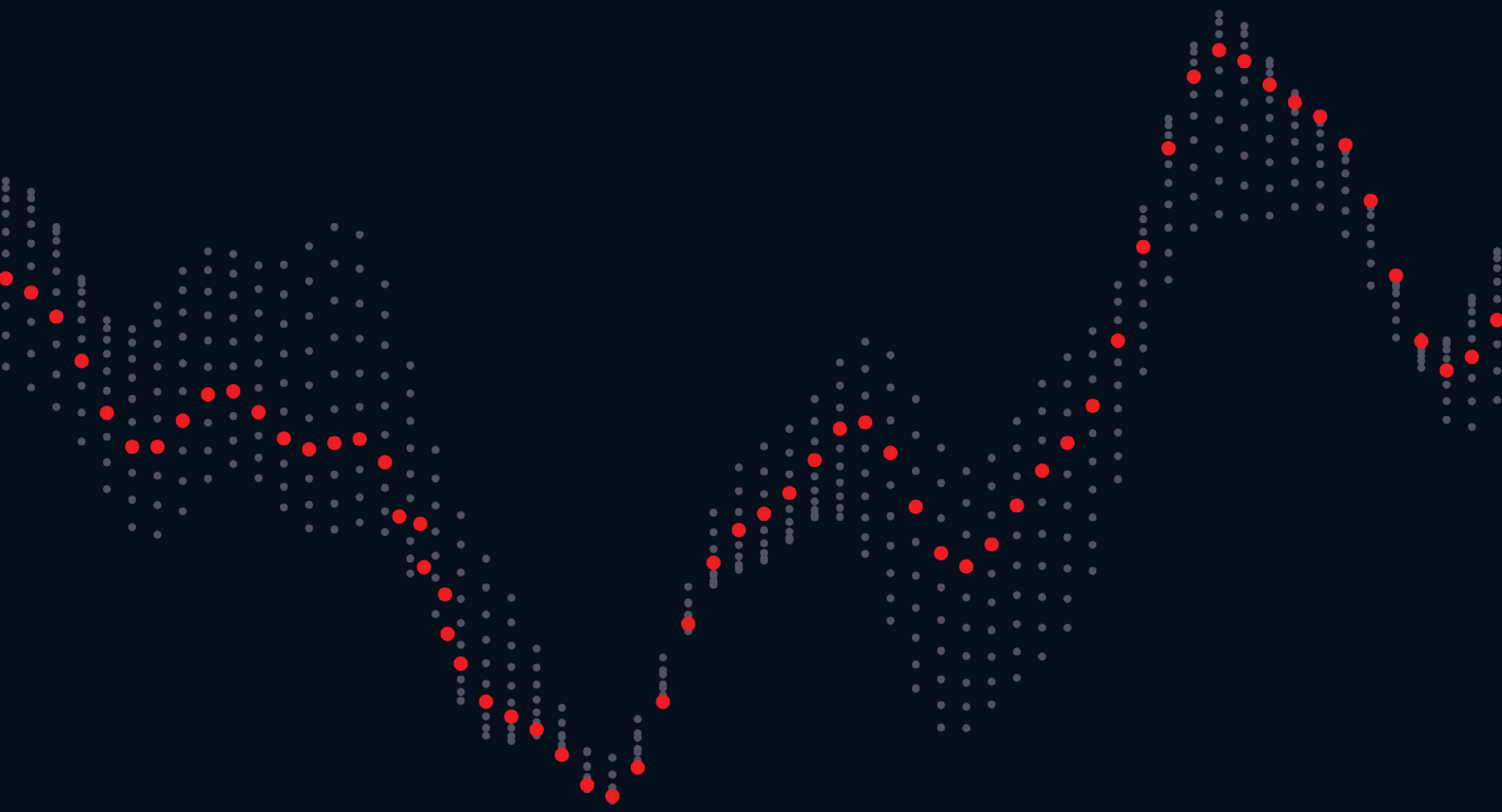
- Schnellere Erkennung und Reaktion durch KI-gestützte Plattformen mit korrelierter und priorisierter Analyse über hybride Umgebungen hinweg
- Reduzierung von Alarmrauschen durch verhaltens- und kontextbasierte Bedrohungserkennung sowie Stärkung der Resilienz durch Fokus auf Eindämmung, Schadensbegrenzung und Kontinuität kritischer Dienste
- Höhere SOC-Effizienz durch automatisierte Triage, intuitive Dashboards und optimierte Workflows

Für CIOs & Compliance-Verantwortliche

- Echtzeit-Sichtbarkeit über IT-, Cloud- und OT-Umgebungen hinweg zur Reduzierung von blinden Flecken
- Unterstützung regulatorischer Anforderungen wie DORA und NIS2 durch bessere Transparenz und nachvollziehbare Sicherheitsprozesse
- Verbesserung des ROI durch umfassendes Monitoring — einschliesslich verschlüsseltem Datenverkehr — ohne zusätzliche operative Komplexität
- Stärkung von Governance und Prüfbereitschaft durch zentrale Protokollierung, Berichterstattung und Integration in bestehende Ökosysteme
- Langfristige Kontrolle durch souveränitätsorientierte Architekturen und transparente Datenverarbeitung

Abschliessender Gedanke

Klarheit schafft Resilienz. **Resilienz** schafft Vertrauen. **Im BFSI-Sektor entscheidet Vertrauen.**



Quellen

01. **IBM Cost of a Data Breach Report**
(2024–2025)

02. **Gartner Cyber Resilience & CISO Role Evolution**
(2024–2025)

03. **CrowdStrike Global Threat Report**
(2025)

04. **Sophos State of Ransomware**
(2025)

05. **Zscaler ThreatLabz Report**
(2025)

06. **Cybersecurity considerations 2024: Financial services sector**
(2024)

07. **SANS OT/IoT Security Reports**
(2024)

08. **Salt Security API Security Report**
(2025)

09. **Devo Security Operations Report**
(2024)

10. **Palo Alto Networks Unit 42 Threat Report**
(2025)

11. **ISC2 Cybersecurity Workforce Study**
(2024)

12. **World Economic Forum Global Cybersecurity Outlook**
(2025)


exeon