exeon

Moderne Bedrohungserkennung im BFSI-Sektor

Ein Evaluierungsleitfaden von Exeon Analytics
für Security- und IT-Verantwortliche

exeon.com

Warum 2026 ein Wendepunkt für Cyber-Resilienz im BFSI-Sektor ist

Banken, Finanzdienstleister und Versicherungen stehen zunehmend unter Druck:

- Verschlüsselter Datenverkehr nimmt zu
- Hybride Infrastrukturen wachsen
- Regulatorische Anforderungen wie DORA und NIS2 erhöhen die Anforderungen an Nachvollziehbarkeit und Prüfungsfähigkeit

Gleichzeitig arbeiten viele SOC-Teams mit begrenzten Ressourcen und einer hohen Anzahl an Alarmen mit geringer Relevanz.

Deshalb überprüfen viele Organisationen derzeit ihre Ansätze in den Bereichen:

- Network Detection & Response (NDR)
- SIEM-Architekturen
- Sicherheitsanalytik und Automatisierung

Worauf es bei modernen NDR-Lösungen ankommt

Bei der Bewertung moderner NDR-Lösungen geht es heute nicht mehr nur um zusätzliche Erkennungsfunktionen. Entscheidend ist vielmehr, wie gut sich eine Lösung in bestehende Sicherheits- und Betriebsprozesse integrieren lässt — und ob sie SOC-Teams im Alltag tatsächlich entlastet.

Die folgenden Kriterien orientieren sich an typischen Anforderungen aus regulierten BFSI-Umgebungen und sollen dabei helfen, Lösungen strukturiert zu bewerten und vergleichbar zu machen.

01 **Sichtbarkeit in verschlüsselten & hybriden Umgebungen**

02 **Geringe Komplexität & effizienter Betrieb**

03 **SOC-Produktivität & Erkennungsqualität**

04 **Compliance & Prüfbereitschaft als Grundprinzip**

05 **Messbarer Geschäftsnutzen & ROI**

01 Sichtbarkeit in verschlüsselten & hybriden Umgebungen

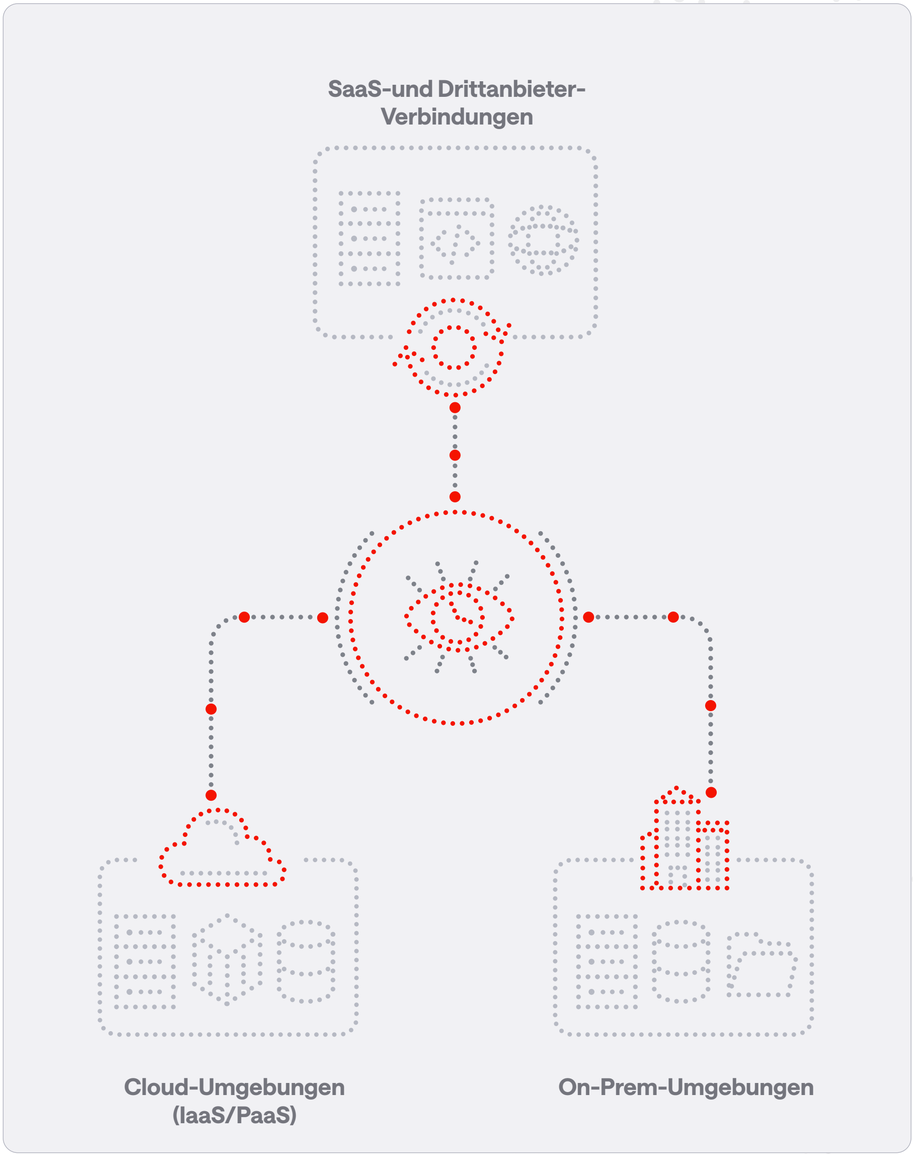
Klassische, rein signaturbasierte Ansätze stossen in modernen BFSI-Umgebungen zunehmend an Grenzen.

Relevante Lösungen sollten daher:

- Aktivitäten in verschlüsseltem Datenverkehr erkennen — ohne Entschlüsselung
- Transparenz über On-Prem-, Cloud- und SaaS-Umgebungen schaffen
- Laterale Bewegungen und ungewöhnliche Kommunikationsmuster frühzeitig erkennen
- Verhaltensbasierte Analysen statt ausschliesslich statischer IoCs nutzen

Darauf sollten Sie achten:

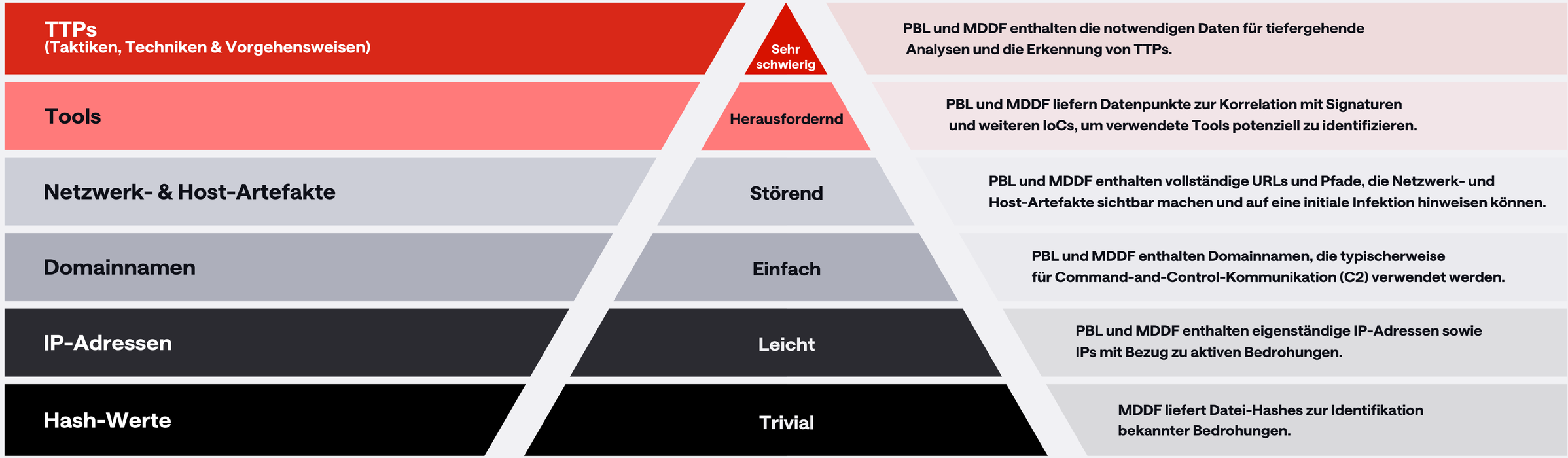
- Können Aktivitäten in verschlüsseltem Verkehr ohne Entschlüsselung erkannt werden?
- Wie werden unbekannte oder schwer erkennbare Aktivitäten identifiziert?
- Welche Datenquellen und Protokolle werden unterstützt?



The Pyramid of Pain
Von IoCs zu verhaltensbasierter Erkennung

Den Fokus von kurzlebigen IoCs auf nachhaltige TTPs verlagern.

IOC-basierte Erkennung: Erkennt bekannte schädliche Artefakte (z. B. spezifische IP-Adressen oder Datei-Hashes).
TTP-basierte Erkennung: Erkennt das Verhalten von Angreifern und erschwert dadurch eine Umgehung deutlich.



Worauf Sie bei modernen NDR-, SIEM- oder Intrusion-Detection-Systemen (IDS) achten sollten

Verhaltensbasierte Analysen (ML + statistische Modelle)

Erkennung von TTPs (nicht nur statischen IoCs)

Ebenso wichtig ist die Erkennung von:

- **Lateralen Bewegungen**
- **Verdeckten Kommunikationskanälen**
- **Datenexfiltration**
- **KI-gestützten Angriffsmustern**

Ganzheitliche Sicherheit in verschlüsselten und hybriden Umgebungen erfordert mehr als isolierte Einzeltools.

Verhaltensbasierte Analysen und TTP-Erkennung sind entscheidend — das eigentliche Ziel ist jedoch ein integrierter Sicherheitsansatz, bei dem NDR, SIEM und EDR als Gesamtsystem zusammenarbeiten.

02 Geringe Komplexität und effizienter Betrieb

Komplexe, sensorlastige Architekturen haben sich in modernen BFSI-Umgebungen häufig als schwer skalierbar erwiesen — insbesondere in verteilten Infrastrukturen mit Filialen, Rechenzentren und Cloud-Lösungen. Mit zunehmender Grösse können Betriebsaufwand und versteckte Kosten für die Verwaltung verteilter Sensoren den ursprünglichen Mehrwert deutlich reduzieren. Moderne NDR-Lösungen sollten daher auf Einfachheit und Effizienz ausgelegt sein.

Entscheidend dafür sind:

1 Sensorarme oder sensorfreie Architektur

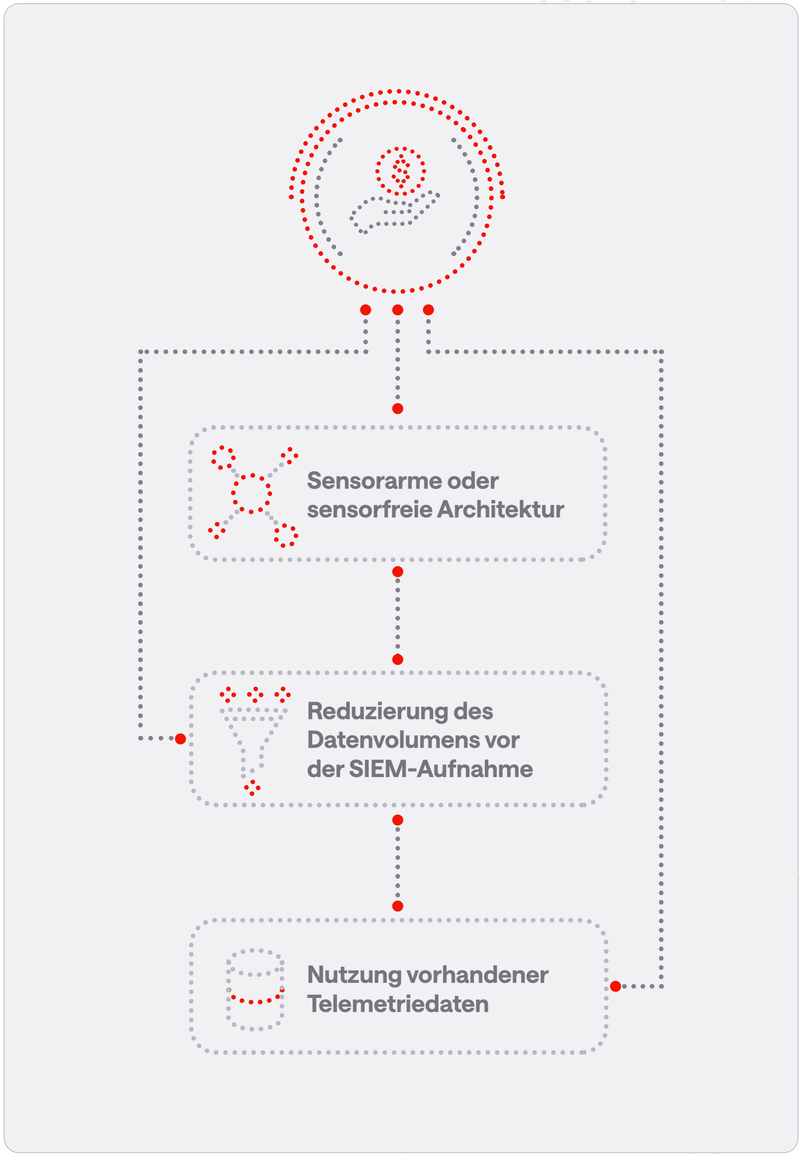
Die Lösung sollte den Bedarf an zusätzlicher Hardware oder verteilten Appliances möglichst reduzieren oder vermeiden. Dadurch lassen sich Bereitstellung, Betrieb und Wartung vereinfachen.

2 Reduzierung des Datenvolumens vor der SIEM-Aufnahme

Durch vorgelagerte Aggregation, Anreicherung und Komprimierung von Telemetriedaten können moderne NDR-Lösungen das nachgelagerte Datenvolumen deutlich reduzieren — mit direkten Auswirkungen auf Speicher-, Verarbeitungs- und Lizenzkosten.

3 Nutzung vorhandener Telemetriedaten

Anstatt zusätzliche Datenerfassungsschichten einzuführen, sollte die Lösung bestehende Datenquellen wie NetFlow, Firewall- und Proxy-Logs, DNS-Aktivitäten oder Cloud-native Metadaten nutzen. Das reduziert Komplexität und beschleunigt die Implementierung.



Evaluierungskriterien

Bei der Bewertung von Lösungen lohnt es sich daher, nicht nur auf Funktionen zu achten, sondern auch die langfristigen architektonischen und finanziellen Auswirkungen zu berücksichtigen.

Welche Infrastruktur wird über Filialen, Rechenzentren und Cloud-Umgebungen hinweg benötigt?

Wie hoch sind die tatsächlichen Gesamtbetriebskosten über mehrere Jahre?

Zentrale Erkenntnisse:

Die effektivsten Lösungen reduzieren architektonische Komplexität und bieten gleichzeitig skalierbare Transparenz — und unterstützen damit eine langfristig besser planbare Kostenstruktur.

03 SOC-Produktivität & Erkennungsqualität

Das Ziel sind nicht mehr Alarme – sondern bessere und schnellere Entscheidungen im SOC.

Entscheidend dafür sind:

1 Kontextbasierte Priorisierung

Alarme sollten dynamisch bewertet und kontextualisiert werden — beispielsweise anhand des Schutzbedarfs betroffener Systeme, des Schweregrads des Verhaltens oder des bisherigen Angriffsverlaufs. Dadurch können Analysten priorisieren, welche Aktivitäten tatsächlich relevant sind, anstatt große Mengen unstrukturierter Warnmeldungen abzuarbeiten.

2 Erklärbare Erkennungen (“White-Box”-Analytik)

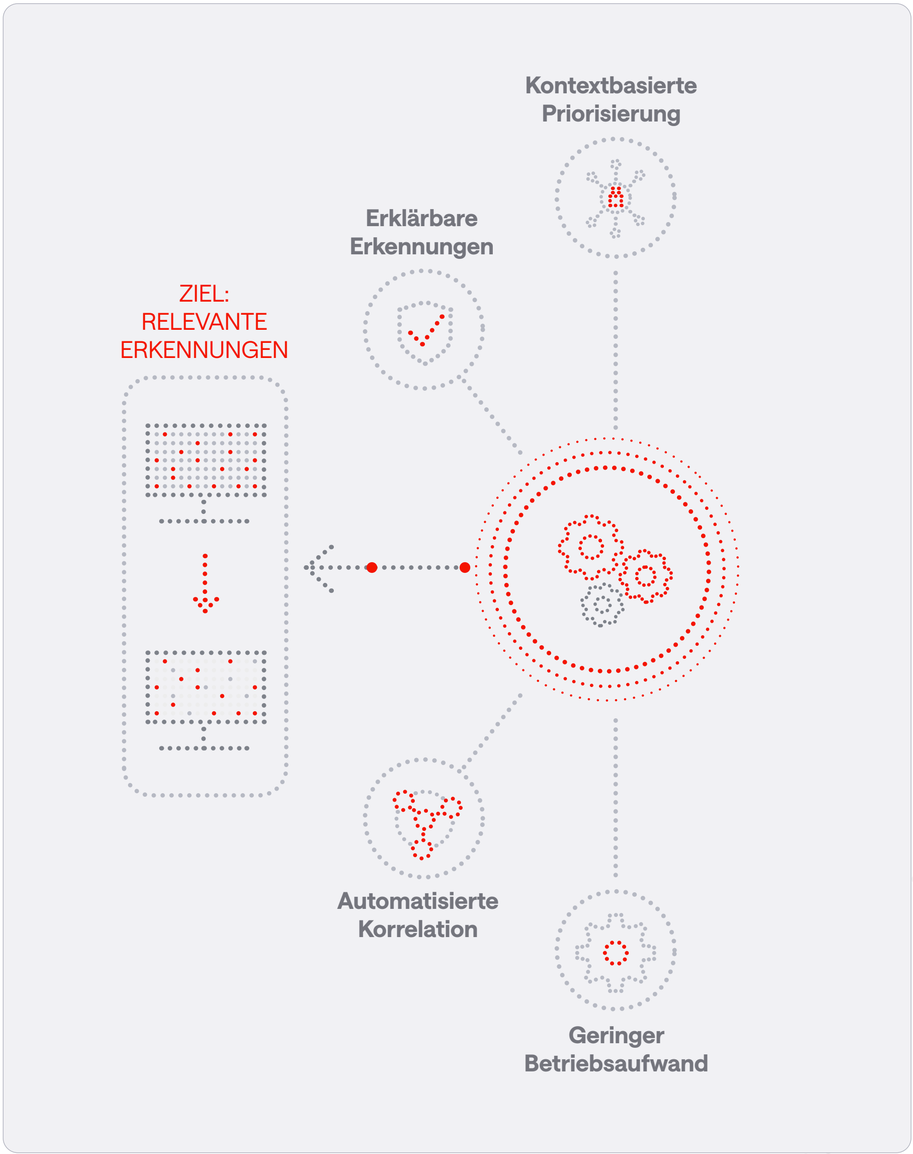
Analysten sollten nachvollziehen können: warum ein Alarm ausgelöst wurde, welche Datenpunkte zur Erkennung beigetragen haben, und wie die Aktivität in ein grösseres Angriffsmuster einzuordnen ist. Nachvollziehbare Erkennungslogik schafft Vertrauen, beschleunigt die Triage und unterstützt Teams dabei, Regeln und Erkennungen gezielt weiterzuentwickeln.

3 Automatisierte Angriffskorrelation

Anstatt isolierte Ereignisse darzustellen, sollte die Lösung Aktivitäten über mehrere Angriffsphasen hinweg miteinander verknüpfen – beispielsweise initialen Zugriff, laterale Bewegung und Datenexfiltration. Dadurch lassen sich Umfang, Auswirkungen und Priorität eines Vorfalls schneller einschätzen.

4 Geringer Betriebsaufwand

In ressourcenbeschränkten SOC-Umgebungen müssen Lösungen möglichst schnell produktiv einsetzbar sein. Achten Sie auf Lösungen, die: nur geringe manuelle Regelanpassungen erfordern, adaptives Lernen unterstützen, Mechanismen zur Reduzierung wiederkehrender Fehlalarme bieten, langfristig mit überschaubarem Betriebsaufwand betrieben werden können.



Evaluierungskriterien

Messbare Ergebnisse sind wichtiger als reine Funktionslisten — idealerweise validiert im Rahmen eines Piloten oder Proof-of-Concepts.

40–70% Reduzierung von Fehlalarmen

Deutliche Reduzierung irrelevanter Alarme und verbessertes Signal-Rausch-Verhältnis.

Schnellere Untersuchungs-zyklen

Analysten sollten ohne komplexe Abfragen oder Toolwechsel schnell von einem Alarm zu verwertbaren Erkenntnissen gelangen.

Hohe Nutzer-freundlichkeit

Sowohl Junior- als auch Senior-Analysten sollten Erkennungen effizient analysieren und priorisieren können.

Stabiler Betrieb nach der initialen Kalibrierung (30-60 Tage)

Nach einer Einführungs- und Lernphase sollte nur begrenzter manueller Aufwand erforderlich sein, um eine qualitativ hochwertige Erkennungsbasis aufrechtzuerhalten.

Entscheidend ist:

Reduziert die Lösung Fehlalarme nachhaltig und unterstützt sie gleichzeitig schnellere Reaktionszeiten im täglichen SOC-Betrieb?

04 Compliance & Prüfbereitschaft als Grundprinzip

Compliance ist längst keine periodische Aufgabe mehr, sondern eine kontinuierliche betriebliche Anforderung. Erkennungslösungen müssen Bedrohungen erkennen und gleichzeitig prüfungsfähige Nachweise bereitstellen.

Entscheidend dafür sind:

1 Unterstützung für souveräne und On-Prem-Bereitstellungen

Aufgrund strenger Datenschutz- und Compliance-Anforderungen im BFSI-Sektor sollten Lösungen flexible Bereitstellungsoptionen unterstützen, damit sensible Daten innerhalb nationaler oder regionaler Grenzen verarbeitet und gespeichert werden können.

2 Langfristige Datenspeicherung mit historischen Kontext

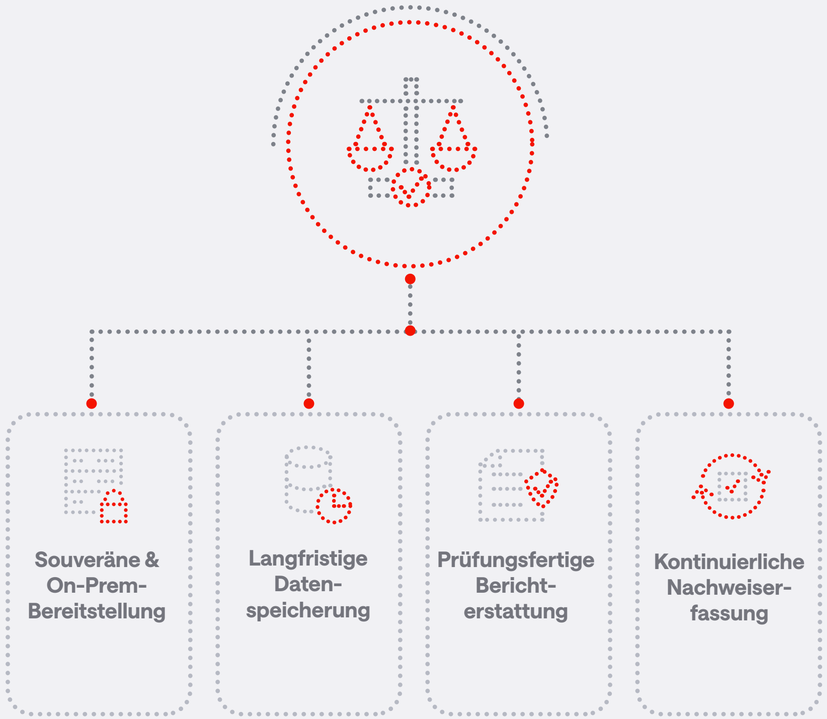
Die Lösung sollte relevante Telemetriedaten langfristig speichern, damit Vorfälle nachvollziehbar bleiben und Compliance-Anforderungen erfüllt werden können.

3 Prüfungsfertige Berichterstattung und Incident-Zeitleisten

Sicherheitsereignisse sollten automatisch in klare Zeitleisten dargestellt werden, einschliesslich betroffener Systeme, Angriffsverlauf und Reaktionsmassnahmen. Dadurch reduziert sich der manuelle Aufwand bei Prüfungen, internen Untersuchungen und regulatorischer Berichterstattung.

4 Automatisierte, kontinuierliche Nachweiserfassung

Die Lösung sollte Nachweise zur Wirksamkeit von Kontrollen automatisch erfassen und kontinuierlich dokumentieren — inklusive Zugriffsprotokollen, Konfigurationsständen und Incident-Zeitleisten.



Native Zuordnung zu regulatorischen Rahmenwerken und Sicherheitsstandards

Erkennungen sollten automatisch bekannten Frameworks wie **MITRE ATT&CK** sowie regulatorische **Anforderungen wie DORA und NIS2 zugeordnet werden können.**

Dadurch lassen sich Vorfälle konsistenter klassifizieren, Berichte schneller erstellen und der manuelle Aufwand bei Audits reduzieren.

Evaluierungskriterien

Bei der Bewertung von Lösungen sollte insbesondere berücksichtigt werden, wie einfach sich technische Erkennungen in prüfungsrelevante Ergebnisse überführen lassen.

Prüfungsrelevante Dashboards

Zugang zu Dashboards und Exportmöglichkeiten für prüfungsrelevante Nachweise und Incident-Dokumentation.

Daten- & Verarbeitungs-souveränität

Unterstützung von Datenhaltungs- und Datenschutzanforder-ungen in regulierten Umgebungen.

Klare Alarmzuordnung

Klare Zuordnung von Alarmen zu regulatorischen Kontrollen und bekannten Frameworks.

Unterstützung regulatorischer Anforderungen

Unterstützung regulatorischer Berichterstattung mit minimalem manuellem Aufwand.

Entscheidend ist:

Unterstützt die Lösung einen kontinuierlichen, prüfungsfähigen Sicherheitsbetrieb — ohne zusätzlichen operativen Aufwand?

05 Messbarer Geschäftsnutzen & ROI

Cybersicherheitsinvestitionen müssen heute nicht nur technisch, sondern auch wirtschaftlich nachvollziehbar sein. Moderne Erkennungslösungen sollten messbar aufzeigen, wie sie Risiken reduzieren, Kosten kontrollieren und die betriebliche Effizienz verbessern.

Entscheidend dafür sind:

1 Reduzierung von Sicherheits- und Geschäftsrisiken

Durch verbesserte Sichtbarkeit und schnellere Erkennung sollte die Lösung dazu beitragen, Wahrscheinlichkeit und Auswirkung sicherheitsrelevanter Vorfälle zu reduzieren – insbesondere bei kritischen Systeme wie Zahlungsverkehr- oder Kernbankensystemen.

2 Reduzierung von SIEM- und Datenkosten

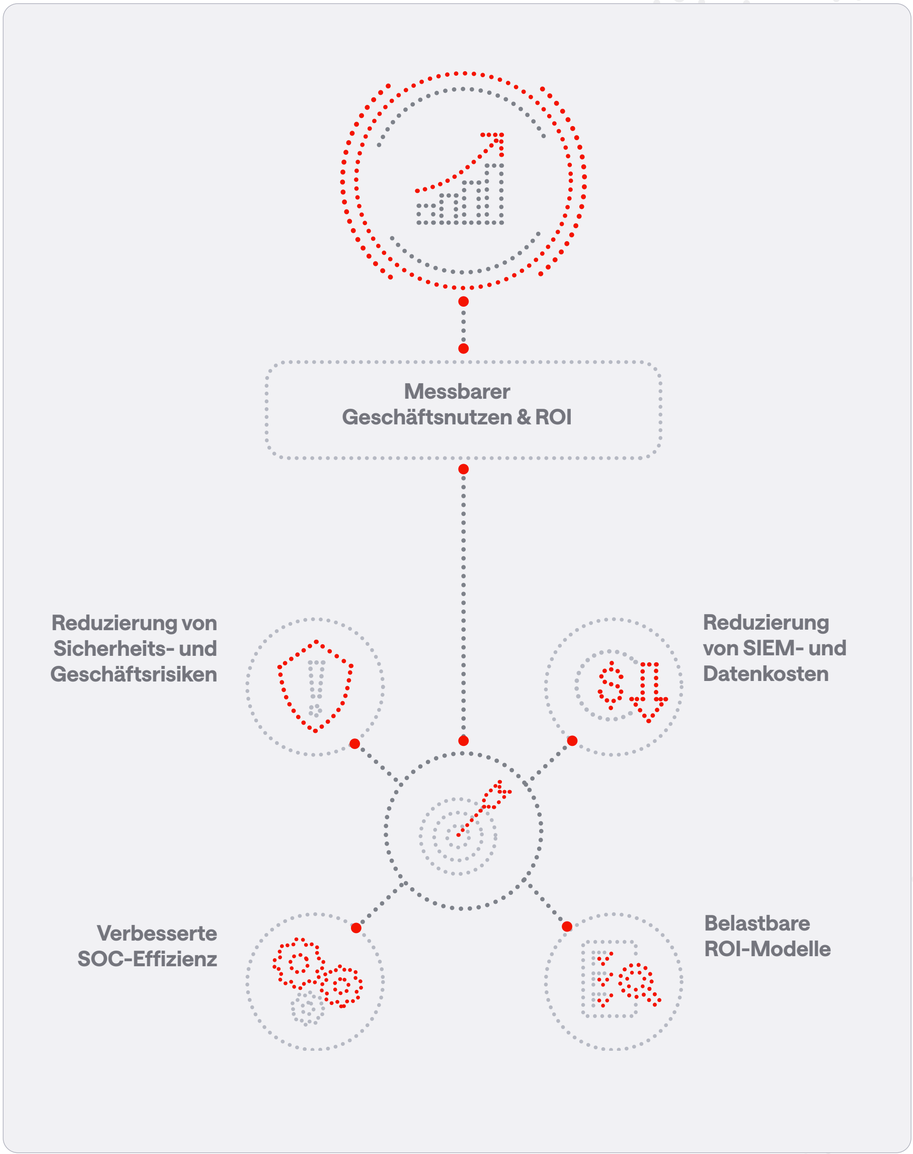
Durch vorgelagerte Datenreduzierung und effizientere Verarbeitung können moderne NDR-Lösungen SIEM-Aufnahmevolumen und langfristige Speicheranforderungen deutlich reduzieren und damit einen wesentlichen Kostentreiber im Sicherheitsbetrieb adressieren.

3 Verbesserte SOC-Effizienz

Durch die Reduzierung von Alarmrauschen und schnellere Untersuchungsprozesse sollten bestehende Teams in der Lage sein, mehr Vorfälle zu bearbeiten, ohne den Personalaufwand proportional erhöhen zu müssen.

4 Belastbare ROI-Modelle

Angesichts der potenziell hohen finanziellen Auswirkungen von Sicherheitsvorfällen im im BFSI-Sektor sollte ein belastbarer Business Case Sicherheitsverbesserungen nachvollziehbar mit vermiedenen Kosten und operativen Einsparungen verbinden.



Evaluierungskriterien

Bei der Bewertung von Lösungen sollten Anbieter bevorzugt werden, die ihre Aussagen mit belastbaren Daten und nachvollziehbaren Ergebnissen belegen können.

Transparente ROI-Modelle

Transparente ROI-Modelle, zugeschnitten auf Ihre Umgebung.

Benchmark-Daten

Benchmark-Daten vergleichbarer BFSI-Organisationen.

Dokumentierte Kundenergebnisse

Dokumentierte Kundenergebnisse und Kosteneinsparungen.

Entscheidend ist:

Liefert die Lösung nachvollziehbaren wirtschaftlichen Mehrwert und unterstützt gleichzeitig Risikominderung sowie operative Effizienz?

Eine narrative Checkliste
Fragen, die Sie jedem Anbieter stellen sollten

Nutzen Sie diese Fragen in Demos, Workshops und PoCs:

Sichtbarkeit & Erkennung

Können laterale Bewegungen in verschlüsselten Umgebungen ohne Entschlüsselung erkannt werden?

Wie werden unbekannte Bedrohungen im Vergleich zu bekannten IoCs identifiziert?

Architektur & Bereitstellung

Können vorhandene Datenquellen wie Flows und Protokolle für die Bereitstellung genutzt werden?

Welche Infrastruktur wird in hybriden Umgebungen benötigt?

Erkennung-squalität

Wie entwickelt sich das Verhältnis von Alarmen zu tatsächlichen Vorfällen nach 30–60 Tagen?

Wie hoch ist der manuelle Kalibrierungsaufwand?

Compliance

Wie werden DORA- und NIS2-Anforderungen unterstützt?

Können prüfungsfähige Incident-Zeitleisten und Korrelationen einfach erstellt werden?

Kosten & ROI

Welche Reduzierung von SIEM-Aufnahme- und Speicherkosten ist realistisch?

Wie sieht der 3-Jahres-TCO im Vergleich zur bestehenden Umgebung aus?

Nächste Schritte für Ihre Evaluierungsreise

1 Mit einem Pilotprojekt starten

- Fokus auf kritische Bereiche wie Zahlungsverkehr, SWIFT und Kernbankensysteme
- Erfolgskriterien definieren: Bedrohungen im verschlüsselten Datenverkehr erkennen und Fehlalarme reduzieren

2 Datenvolumen & Kosten messen

- SIEM-Aufnahmevolumen vor und nach der Implementierung vergleichen
- Speicher- und Verarbeitungseinsparungen quantifizieren

3 Compliance-Ziele berücksichtigen

- Erkenntnisse auf DORA- und NIS2-Anforderungen abbilden
- Technische Ergebnisse in prüfungsrelevante Nachweise übersetzen

4 Schrittweise skalieren

Erfolgreiche Pilotprojekte lassen sich häufig innerhalb von 6–10 Wochen produktiv skalieren – unter anderem mit:

- Reduzierter Infrastrukturkomplexität
- Niedrigeren Betriebskosten
- Verbesserter Erkennungsqualität

Warum sich BFSI-Führungskräfte für Exeon entscheiden

Bei europäischen BFSI-Organisationen stehen häufig drei Themen im Vordergrund:

Sensorfreie Sichtbarkeit

- Nutzung vorhandener Datenquellen wie Flows, DNS und Firewall-Protokolle
- Transparenz in verschlüsselten und segmentierten Umgebungen

Erklärbare KI

- Transparente ML-Modelle
- Reduzierung von Alarmrauschen und Analystenmüdigkeit
- Unterstützung von Datensouveränität innerhalb der EU und der Schweiz

Nachweisbarer ROI

- Bis zu 100× Reduzierung des Datenvolumens
- Geringere SIEM-Kosten
- Schnellere Prüfungs- und Compliance-Berichterstattung

Verwenden Sie dieses Framework, um unterschiedliche Anbieter strukturiert und objektiv zu bewerten – **einschliesslich Exeon.**

Erfahren Sie, wie Exeon Transparenz schafft, relevante Bedrohungen frühzeitig erkennt und die Cyber-Resilienz Ihrer Organisation stärkt.

DEMO VEREINBAREN


exeon
Gartner
ATTESTA
ISO 27001
CERTIFIED
CYBERSECURITY™
MADE IN EUROPE