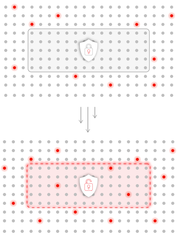
6 zentrale Erkenntnisse für moderne Sicherheitsstrategien im BFSI-Sektor



1. Transparenzlücken erhöhen Risiko und Compliance-Druck

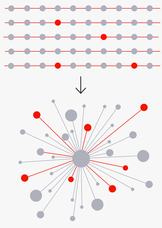
Viele Unternehmen entdecken Schatten-IT und Sicherheitslücken erst nach einem Vorfall. Gleichzeitig erschwert verschlüsselter Datenverkehr die frühzeitige Erkennung von Bedrohungen.

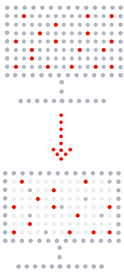
Massnahmen: Verschlüsselungsbasierte Verkehrsanalysen (ETA/TLS) und netzwerkbasierte Asset-Inventare schaffen mehr Transparenz in hybriden und verschlüsselten Umgebungen.

2. Moderne Bedrohungen umgehen klassische Erkennungsregeln

Polymorphe Malware, Ransomware und moderne APTs umgehen klassische signaturbasierte Erkennung zunehmend erfolgreich.

Massnahmen: Verhaltensbasierte ML-Analysen und kontinuierliches Threat Hunting ergänzen klassische Sicherheitsmechanismen und verbessern die Erkennung unbekannter Bedrohungen.





3. Alarmmüdigkeit beeinträchtigt die Effektivität des SOC

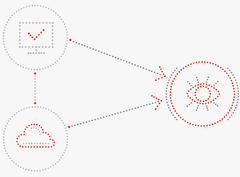
Hohe Analystenbelastung, Fehlalarme und fragmentierte Sicherheitslandschaften verlangsamen Reaktionszeiten und erschweren die Priorisierung.

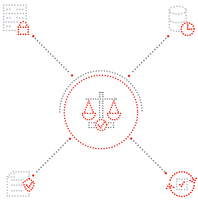
Massnahmen: Konsolidierte Sicherheitslösungen, risikobasierte Erkennungen und automatisierte Tier-1-Triage mit SOAR verbessern Effizienz und Reaktionsfähigkeit im SOC.

4. OT und Cloud bilden den neuen Perimeter

OT, Cloud, SaaS, Filialen und Remote-Arbeitsplätze bilden den neuen Sicherheitsperimeter.

Massnahmen: Integrierte OT-Telemetrie und Cloud-Logs schaffen Transparenz über hybride Umgebungen hinweg.





5. Compliance erfordert Transparenz und Nachweisbarkeit

Regulatorische Anforderungen verlangen schnelle Berichterstattung, Netzwerksegmentierung und eine stärkere Kontrolle von Drittanbietern.

Massnahmen: Automatisierte Nachweis- und Reporting-Prozesse sowie die Verknüpfung bestehender Sicherheitslösungen mit regulatorischen Anforderungen verbessern Compliance und Auditfähigkeit.

6. Weniger Alarmrauschen, schnellere Reaktionsfähigkeit

Analysten benötigen präzise Erkennungen, integrierte Korrelation und sofort einsatzbereite Workflows, um Vorfälle effizient priorisieren und bearbeiten zu können.

Massnahmen: Vollständige Transparenz, integrierte Korrelation, Case Management und SOAR reduzieren Alarmrauschen und verbessern die Reaktionsfähigkeit im SOC.

Vollständigen Report herunterladen

exeon