Exeon.NDR

Moderne Netzwerksicherheit gegen hybride, verschlüsselte und neuartige Bedrohungen

Hybride und verschlüsselte Netzwerke verursachen blinde Flecken bei herkömmliche Sicherheitslösungen. Gleichzeitig bewegen sich Angreifer schneller und unauffälliger durch IT-, OT- und Cloud-Umgebungen.

Exeon.NDR bietet sensorlose, metadatenbasierte Netzwerksichtbarkeit, um verborgene Bedrohungen früh zu erkennen, die Effizienz des SOC zu steigern und die Compliance zu unterstützen.

Ihre Vorteile mit Exeon.NDR

Vollständige Netzwerk-sichtbarkeit

Sehen Sie **alle Assets und Datenströme** in IT-, OT- und hybriden Umgebungen – selbst bei verschlüsseltem Datenverkehr.

Früherkennung bei versteckten Bedrohungen

Identifizieren Sie Lateral Movements, APTs und Zero-Day-Angriffe mittels **KI-gestützter Verhaltensanalyse und Expertenregeln.**

Weniger Fehlalarme, bessere SOC-Effizienz

Intelligente Alarmkorrelation und intuitive Netzwerk-visualisierung **beschleunigen Investigation** und Response.

Geringere Gesamt-betriebskosten (TCO)

Keine Wartung von Sensoren oder Agenten, kombiniert mit **starker Datenreduktion, die SIEM-Kosten senkt.**

Schnelle Bereitstellung & Integration

Keine Sensoren nötig. Inte-grierte Erkennungsregeln und offene APIs ermöglichen eine **schnelle Integration** in SIEM-, SOAR- und SOC-Systeme.

Compliance, Daten-souveränität & DSGVO

Unterstützt **NIS2-/DORA-Vorgaben. On-Prem**-Bereitstellung und metadatenbasierte Analysen gewährleisten **Datenschutz.**

Trusted by

PostFinance · SWISS · cargolux · LGT · Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra · BonnNetz Ein Unternehmen der Stadtwerke Bonn

Wieso jetzt reagieren

Verlust von Sichtbarkeit

90%+ des internen Netzwerkverkehrs ist mittlerweile verschlüsselt.

Quelle: Microsoft Digital Defense Report 2024

Schnellere Angriffe

Die durchschnittliche Verweilzeit von Ransomware beträgt **~24 Stunden**.

Quelle: Secureworks

Nicht verwaltete Assets

Über **90%** der Ransomware-Angriffe stammen von nicht verwalteten Assets.

Quelle: Microsoft Digital Defense Report 2024

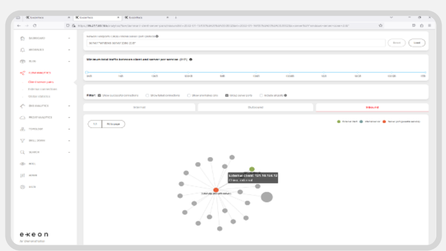
Steigende Regulatorien

DORA/NIS2 erfordern nachweisbare, kontinuierliche Netzwerküberwachung.

Quelle: EU Digital Operational Resilience Act (DORA); EU Network and Information Security Directive (NIS2)

Das 4-Phasen-Modell: So arbeitet Exeon.NDR

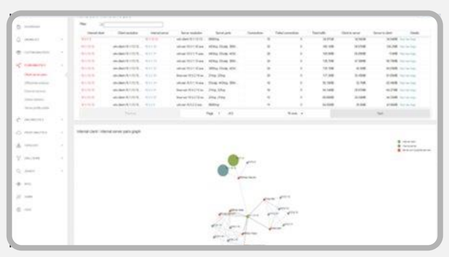
Log-Quellen



- Sammlung der Logdaten mittels sensorlosem, meta-daten-basiertem Ansatz

- Bereitstellung in Tagen, nicht Monaten
- Keine Installation von Sensoren

Log-Prozessierung



- Reduzierung der Logdaten durch intelligente Datenverarbeitung
- Visualisierung aller Datenströme

- Holistische Netzwerkübersicht
- Vollständige IT/OT/Cloud-Abdeckung

Detektion

- Mehrschichtiges System zur Erkennung von versteckten & neuartigen Bedrohungen

- KI + Expertenregeln führt zu hoher Genauigkeit
- Erkennung von Zero-Days & APTs

Visualisierung & Response

- Hochwertige und handlungsrelevante Alarme
- Intuitive GUI und umfassende REST-API

- Schnellere & zuverlässigere Reaktion
- Nahtlose SIEM- / SOAR-Integration

Sie möchten Exeon.NDR testen?

Exeon Analytics AG

exeon.ai

+41 44 500 77 21

contact@exeon.com

CYBERSECURITY MADE IN EUROPE™

Gartner Peer Insights™