2021

Factsheet

exeon
Smart Cyber Security.

ExeonTrace

01

Smarte Network Detection and Response

Die ExeonTrace Network Detection & Response (NDR) Plattform ist die smarte Art um die Cybersicherheit zu stärken. Leistungsstarke KI und bewährte Algorithmen geben komplette Transparenz über das gesamte Netzwerk. Sie erkennen automatisch verdächtiges Verhalten und unterstützen das jeweilige Sicherheitsteam bei der effizienten Bewertung und Bekämpfung von Cyber-Bedrohungen, bevor Schaden entsteht.

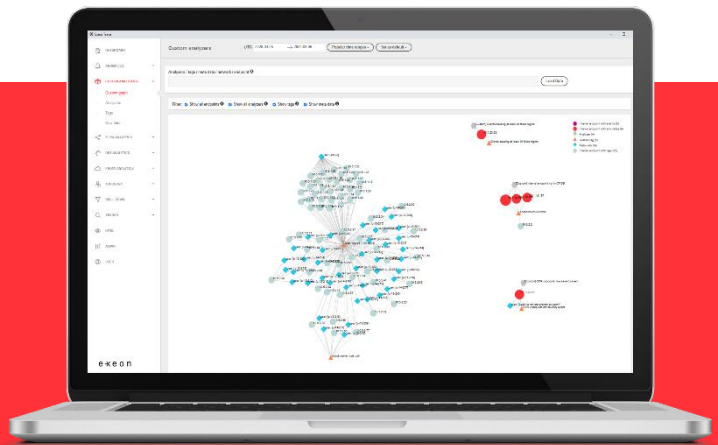
02

Warum ExeonTrace

- **Schnelles Aufsetzen:** Innert Stunden bereit. Keine Sensoren oder Agenten nötig
- **Schlagkräftige Reaktion:** Schnelle Bewertung, Untersuchung und Bekämpfung.
- **Komplette Visibilität:** Vereinte Sicht auf verteilte Netzwerke, Endpunkte und Applikationen.
- **Intelligentes Datenhandling:** Minimaler Speicherbedarf bei voller Datenkontrolle.
- **Schlaue Detektion:** Leistungsstarke KI und bewährte Algorithmen.
- **Zukunftssicher:** Bereit für zunehmenden Datenverkehr und Verschlüsselung

Kunden, die auf ExeonTrace setzen:

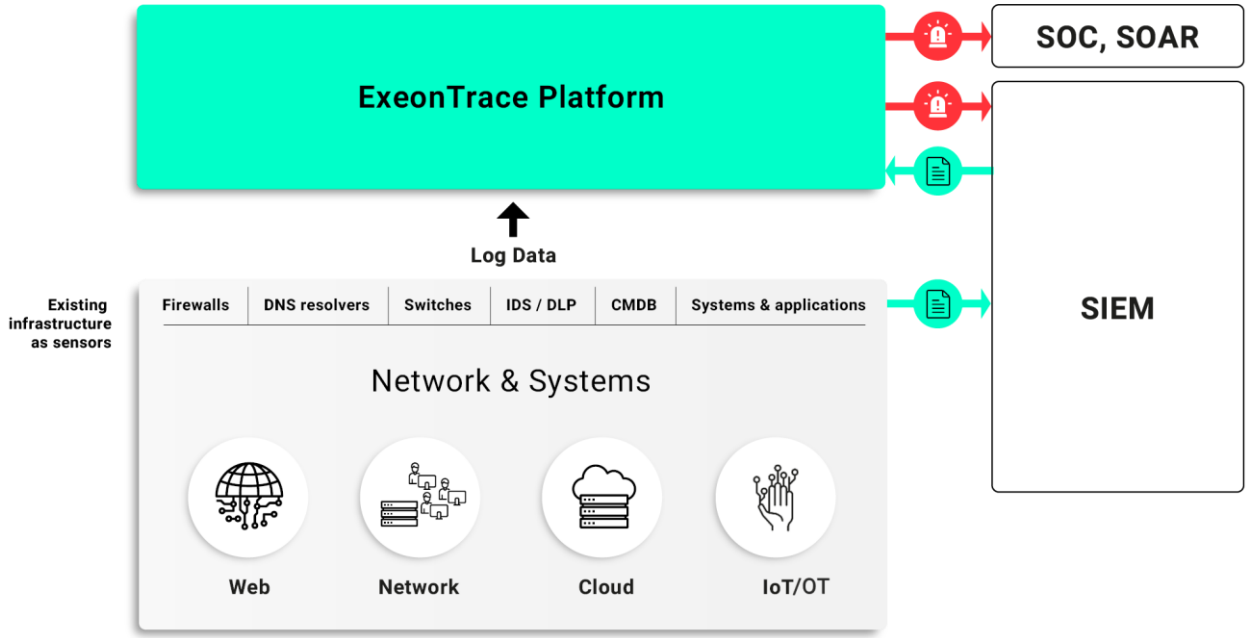
PostFinance
3 Banken IT
HAAG-STREIT DIAGNOSTICS
PLANZER



03

So funktioniert ExeonTrace

ExeonTrace analysiert sicherheitsrelevante Log-Daten aus dem Netzwerk und den Systemen. Als reine Softwarelösung nutzt ExeonTrace die bestehende Unternehmensinfrastruktur (d.h. Firewalls, Switches, etc.) als Datensensoren und benötigt keine zusätzlichen Hardware-Appliances oder Sensoren.

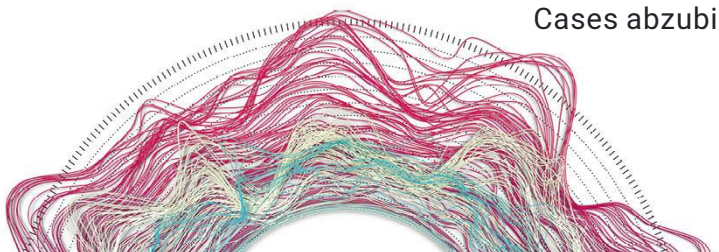


04

Komplette Visibilität – Netzwerkdatenflüsse einfach verstehen

Dank einzigartigen und intuitiven Visualisierungen können grosse und komplexe Netzwerke sofort überwacht und einfach verstanden werden. Data Breaches werden frühzeitig erkannt und die IT Security wird gestärkt ohne die laufenden, wichtigen Geschäftsprozesse zu stören.

- Aufdecken versteckter Datenlecks wie Browser Plug-Ins oder Daten-sammler
- Auffinden ungewöhnlicher Dienste im Netzwerk
- Aufspüren unerwünschter/böswilliger Aufrufe an interne Dienste
- Identifizierung fehlkonfigurierter Geräte
- Nicht autorisierter und veraltete Geräte: Clustering von Machine-to-Machine (M2M)-Geräten zur Ausreisserkennung (interne Schatten-IT)
- Interne Schatten-IT: Korrelation mit CMDB-Information
- Externe Schatten-IT: Aufdeckung von nicht autorisierten Cloud-Diensten oder Uploads
- Korrelation von Netzwerkdaten mit anderen Logdaten-Quellen, um benutzerdefinierte Use Cases abzubilden



05

Detection – Die Alarmanlage für Ihr Netzwerk

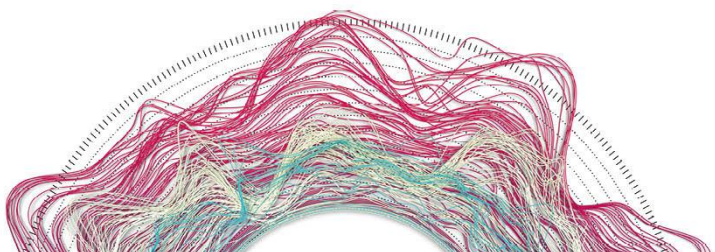
Cyber-Bedrohungen werden sofort erkannt wie z. B. Advanced Persistent Threats (APT), Ransomware, Supply Chain Attacks oder Datenlecks durch exponierte, unsichere Systeme. Schlagkräftige Detektion, auch für Bedrohungen die sich über mehrere Datenquellen erstrecken.

- Detektion von versteckten HTTP(S)-basierten Angreifern von Befehls- und Kontrollkanälen
- Detektion von lateralen Bewegungen, z.B. die Verbreitung von Ransomeware in Ihrem Unternehmensnetzwerk
- Detektion von Malware mithilfe von Domain Generation Algorithmen (DGAs)
- Detektion von horizontalem und vertikalem Scannen innerhalb Ihres Netzwerkes
- Detektion verdeckter DNS-Kanäle: Versteckte Datenlecks über das Domain Name System (DNS)
- Detektion von Richtlinien-Verstössen
- Blacklist-Abgleich: Korrelation mit externer Intelligenz

06

Response – Effiziente Untersuchung von Sicherheitsvorfällen

- Sicherheitswarnungen können durch die sofortige Anzeige aller relevanten Informationen schneller und besser bearbeitet werden. Unsere Algorithmen minimieren Fehlalarme und priorisieren Vorfälle automatisch nach Bedrohungs-ebenen.
- Entscheidende Zeit bei Sicherheitsvorfällen sparen und so die Arbeitsbelastung des Sicherheitsteams reduzieren.
- Intuitive grafische Darstellung von Sicherheitsvorfällen für eine effektive Untersuchung des Netzwerks
- Algorithmus-gesteuerte Bedrohungs-bewertung für eine effiziente Priorisierung der Vorfälle
- Schnelle Queries: Sekunden statt Minuten für TB an Logdaten
- Korrelation von Daten aus verschiedenen Daten-quellen, um schnell ein vollständiges Bild zu erhalten



07

ExeonTrace Subscription

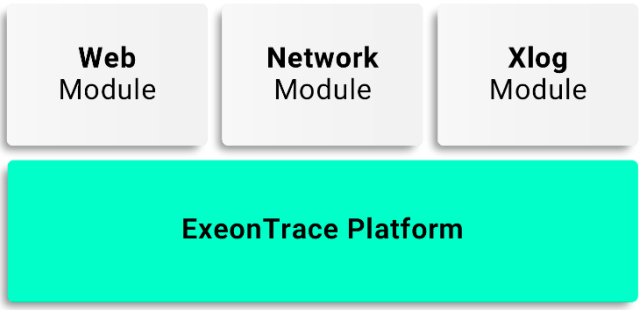
Schützen Sie das IT-Netzwerk Ihres Unternehmens mit ExeonTrace. Unser Jahresabonnement beinhaltet die Softwarelizenz und ein Supportpaket für die Einrichtung, Schulung und Support durch unsere Techniker. Die Preisgestaltung ist abhängig von den gewählten Analysepaketen und der Anzahl der aktiven, internen IP-Adressen.

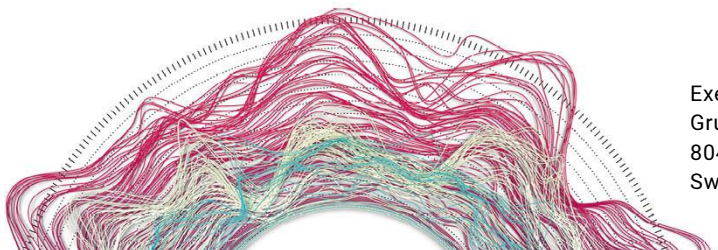
Bitte kontaktieren Sie uns für weitere Informationen oder eine Live-Demonstration von ExeonTrace: contact@exeon.com

Web Modul: Abdeckung der Web-Aktivitäten interner Geräte
Für Proxy-Protokolle von SSL/TLS-abfangenden Secure Web Gateways

Netwerk Modul: Abdeckung des internen & externen Netzwerkverkehrs
Für NetFlow, IPFIX, Corelight & DNS

Xlog Modul: Datenübergreifende Bedrohungserkennung
Für die Korrelation und Analyse zusätzlicher sicherheitsrelevanter Protokolldaten, wie z. B. allgemeine Ereignisprotokolle (System- und Anwendungsprotokolle, Active-Directory-Protokolle), Informationen der Configuration Management Database (CMDB), Sicherheitsanwendungsprotokolle (Ereignisse, die von Ihrer EDR-, IDS-, Antivirensoftware usw. erzeugt werden) oder Cloud-Anwendungsprotokolle.





Exeon Analytics AG
Grubenstrasse 12
8045 Zürich
Switzerland

contact@exeon.com