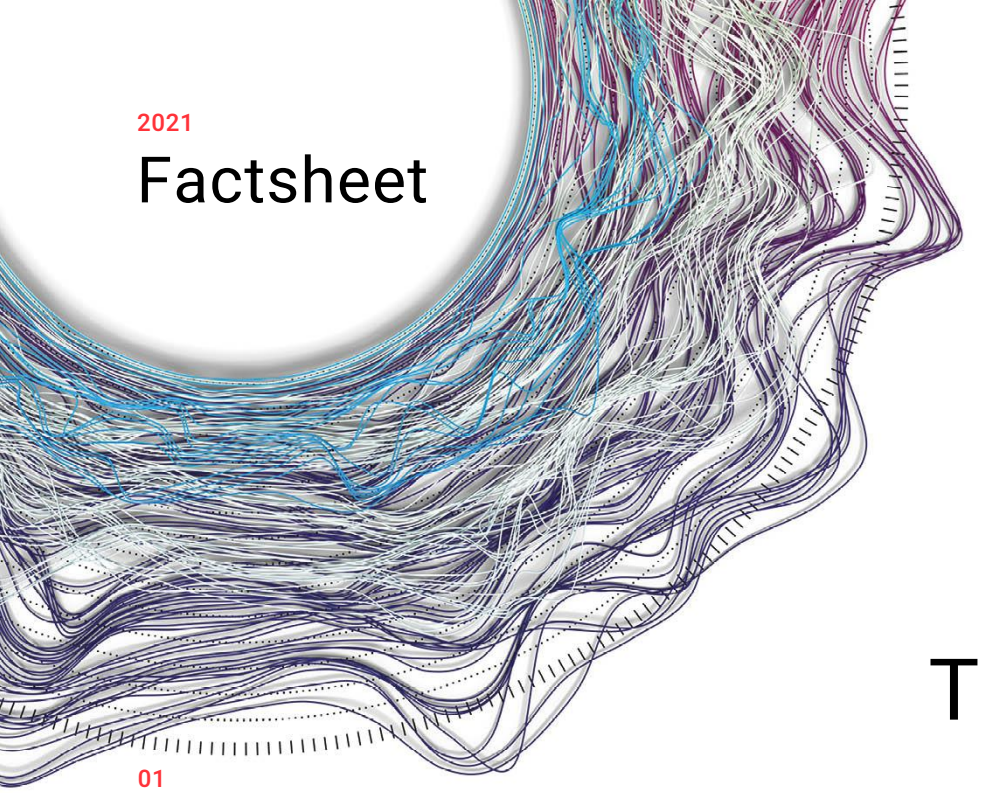
2021

Factsheet

exeon

Smart Cyber Security.



Exeon ThreatReport

01

Wir ermitteln versteckte Cyber-Bedrohungen

Cyber-Angreifer und böswillige Insider umgehen regelmässig IT-Sicherheits-massnahmen und kompromittieren hochsensible Daten. Derartige Angriffe bleiben über Monate hinweg unentdeckt, da sie in den Millionen von regulären IT-Aktivitäten schlichtweg untergehen.

Die durchschnittliche Erkennungszeit für Daten-Kompromittierungen beträgt derzeit mehr als 24 Tage. Es kann aber auch viel länger dauern, wie die Hotelkette «Marriott international» feststellen musste. Diese entdeckte einen Cyber-Angriff erst nach vier Jahren und der Offenlegung von über 300 Millionen Kunden-daten. Exeon ist darauf spezialisiert, verborgene Datenabflüsse und fortschrittliche Cyber- Angriffe aufzudecken. Mit ExeonTrace, unserer Analyse- und Visualisierungs Visualisierungssoftware, finden wir die sogenannte Nadel im Heuhaufen. ExeonTrace basiert auf preis-gekrönten Algorithmen, identifiziert effektiv Lücken in IT-Sicherheitsperimetern und erkennt Anomalien in Millionen von Datenpunkten (Logdaten). Für unsere ExeonThreatReport Sicherheitsüberprüfung verwenden wir ExeonTrace, um aus den Netzwerkprotokolldaten unserer Kunden konkrete Sicherheits-erkenntnisse abzuleiten.

02

Sicherheitsüberprüfung bestellen

Der ExeonThreatReport spürt die potentielle Nadel im Heuhaufen auf. Während eines Sicherheitschecks überprüfen unsere Experten den Sicherheitsstatus des Netzwerkes, indem sie mithilfe der Algorithmen von ExeonTrace die Logdaten analysieren.

Aufsetzen und Konfiguration von ExeonTrace

Unsere Experten analysieren über eine Woche hinweg die gesammelten Logdaten

Unsere Spezialisten dokumentieren die Ergebnisse in einem Bericht.

Der interne Zeitaufwand beträgt ein bis zwei Arbeitstage.

03

Analysepakete

Der ExeonThreatReport bietet zwei Analysepakete. Die Pakete können gemeinsam oder separat gewählt werden. Paket 1 analysiert Proxy-Logdaten und Paket 2 Flow- und DNS-Logdaten.

Paket 1
Proxy/Secure Web Gateway Analyse

Analyse der **Web-Aktivitäten** interner Geräte.

Ermittlung von APT Attacken:

- Ermittlung verborgener HTTP(S)-basierte Kommunikationskanäle von Cyber-Angreifern
- Ermittlung von Schadsoftware, die Domain-Generation-Algorithmen (DGAs) verwendet

Erkennung **verborgener Datenlecks** wie etwa Browser-Plugins oder Software, die Daten sammelt

Externe Schatten-IT:
Entdeckung unautorisierter Cloud-Dienste und Uploads

Unautorisierte und veraltete Geräte:
Clustering von Geräten mit Machine-to-Machine-Aktivitäten (M2M) zur Erkennung von Ausreissern

Identifizierung **nicht authentifizierter** Proxy-Zugriffe

Korrelation mit ausgewählten **Bedrohungs-Feeds** (Blacklists)

Anforderungen: Proxy-Logs aufgezeichnet von einem Secure Web Gateway mit SSL/TLS-Interception.

Paket 2
Flow and DNS Analyse

Analyse des **internen & externen** Netzwerkverkehrs

Ermittlung von APT Attacken:

- Erkennen von lateraler Bewegungen: Ausbreiten von Schadsoftware in Ihrem Unternehmens-netzwerk
- Horizontales und vertikales Scannen innerhalb des Unternehmensnetzwerkes wird entdeckt
- Erkennen von Schadsoftware, die Domain-Generation-Algorithmen (DGAs) verwendet
- Erkennen verdeckter DNS-Kanäle: Verborgener Datenverlust über das Domain Name System (DNS)

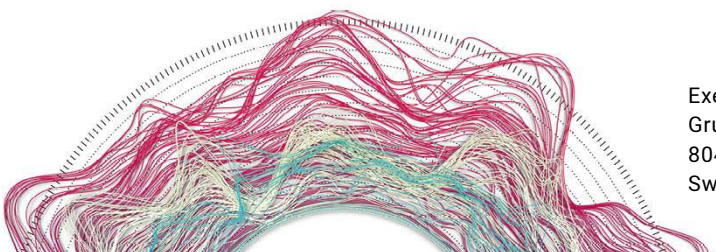
Netzwerk Visibilität:

- Erkennen ungewöhnlicher Dienste im Netzwerk
- Erkennen von ungewollten/bösartigen Zugriffen auf interne Dienste
- Identifizierung von fehlkonfigurierten Geräten
- Verständnis, wie kritische Netzwerke kommunizieren

Korrelation mit ausgewählten **Bedrohungs-Feeds** (Blacklists) und **CMDB-Informationen** (interne Schatten-IT)

Anforderungen: Firewalls/Switches, die in der Lage sind, NetFlow v5/v9/IPFIX-Protokolldaten zu exportieren oder Corelight-Sensoren. DNS-Daten, die von unserem Netzwerksensor oder Ihren DNS-Resolvern aufgezeichnet werden. Logdaten können in Elasticsearch oder Splunk gespeichert oder direkt an ExeonTrace gesendet werden.

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



Exeon Analytics AG
Grubenstrasse 12
8045 Zürich
Switzerland

contact@exeon.com