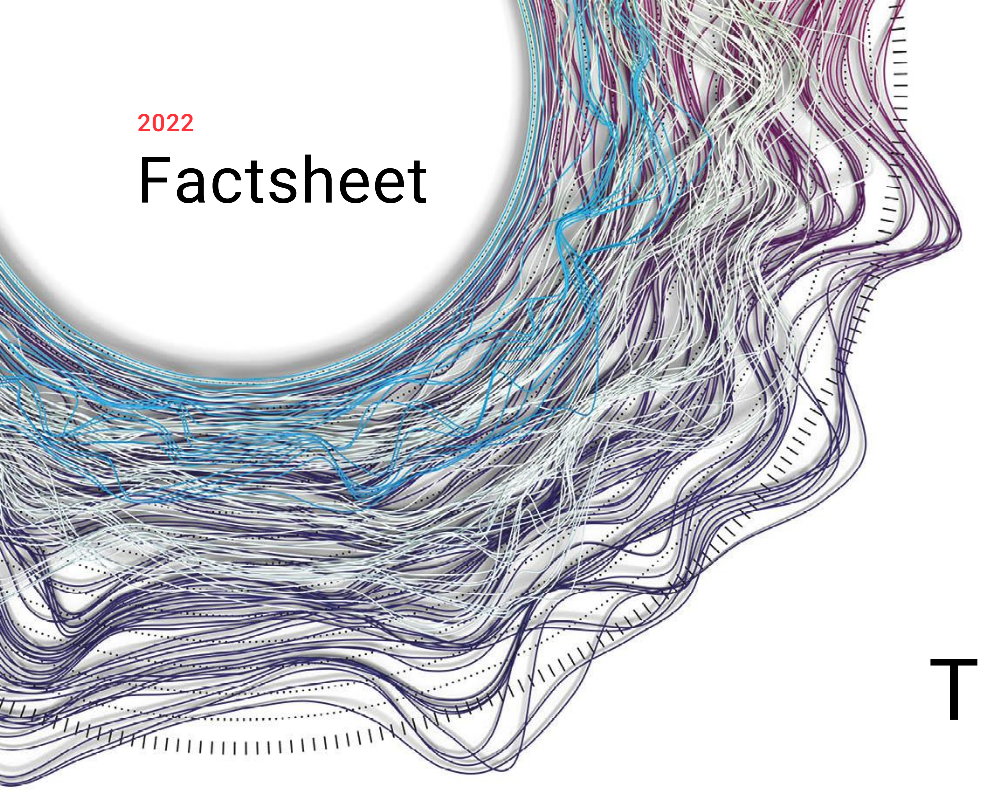


2022

Factsheet

exeon

Smart Cyber Security.

Exeon ThreatReport

01

We identify hidden cyber threats

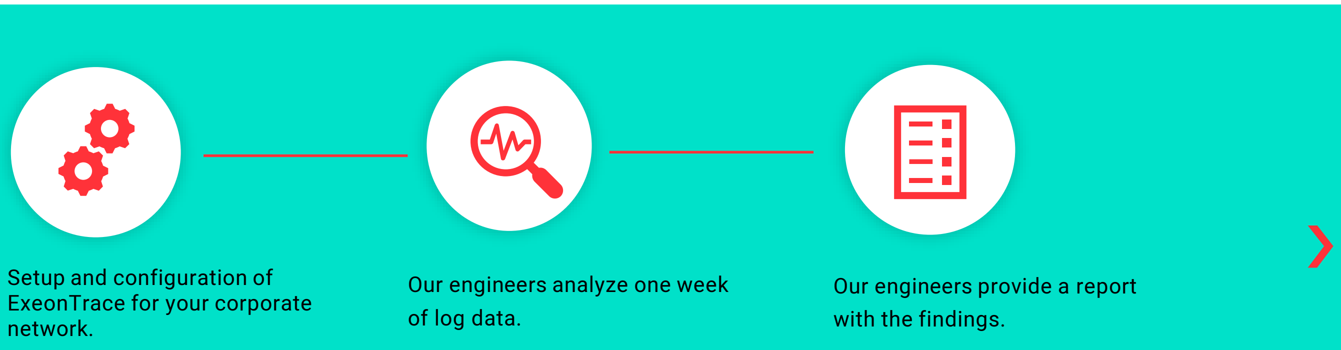
Cyber attackers and malicious insiders regularly avoid IT security measures and compromise highly sensitive data. Such attacks go undetected for months as they simply get lost in the millions of regular IT activities.

The average detection time for data compromises is currently more than 24 days. But it can also take much longer, as the hotel chain Marriott International discovered. The latter discovered a cyber attack only after four years and the disclosure of over 300 million customer data. Exeon specializes in uncovering hidden data leakage and advanced cyber-attacks. With ExeonTrace, our analysis and visualization software, we find the so-called needle in the haystack. ExeonTrace is based on award-winning algorithms, effectively identifies gaps in IT security perimeters and detects anomalies in millions of data points (log data). For our ExeonThreatReport security audit, we use ExeonTrace to derive concrete security insights from our customers' network log data.

02

Order security check

The ExeonThreatReport detects the potential needle in the haystack. During a security check, our experts verify the security status of your network by analyzing your log data using ExeonTrace algorithms.



Setup and configuration of ExeonTrace for your corporate network.

Our engineers analyze one week of log data.

Our engineers provide a report with the findings.

The internal effort on your side is 1-2 days.

03

Packages

The ExeonThreatReport offers two analysis packages. The packages can be selected independently or jointly. Package 1 analyzes proxy log data and package 2 analyzes flow and DNS log data.

Package 1
Proxy/Secure web gateway analysis

Analysis of the **web activities** of your internal devices.

APT attack detection

- Detecting hidden HTTP(S)-based command and control channels
- Detecting malware using Domain Generation Algorithms (DGAs)

Detection of hidden data leaks such as browser plugins or software collecting data

External shadow IT: Detection of unauthorized cloud services and uploads

Unauthorized and outdated devices: Clustering of machine-to-machine (M2M) devices for outlier detection

Identification of unauthenticated proxy access

Correlation with selected threat feeds (blacklists)

Requirements:
The log data is recorded by an SSL/TLS-intercepting secure web gateway.

Please contact us for more information or a live demo of ExeonTrace:
contact@exeon.com

Package 2
Flow and DNS analysis

Analysis of your **internal & external** network traffic.

APT attack detection

- Detecting lateral movement: Expansion of malicious software in your network
- Detecting horizontal and vertical scanning inside your corporate network
- Detecting malware using Domain Generation Algorithms (DGAs)
- Detecting covert DNS channel: Hidden data leakage via Domain Name System (DNS)

Network visibility

- Discovery of unusual services in your network
- Discovery of undesired/malicious access to internal services
- Identification of misconfigured devices
- Understand communication of critical networks

Correlation with selected threat feeds (blacklists) and CMDB information (internal shadow IT)

Requirements:
Firewalls/switches capable of exporting NetFlow v5/v9/IPFIX log data or Corelight sensors. DNS logs recorded by our network sensor or your DNS resolvers. Log data can be stored in Elasticsearch, Splunk or directly sent to ExeonTrace.