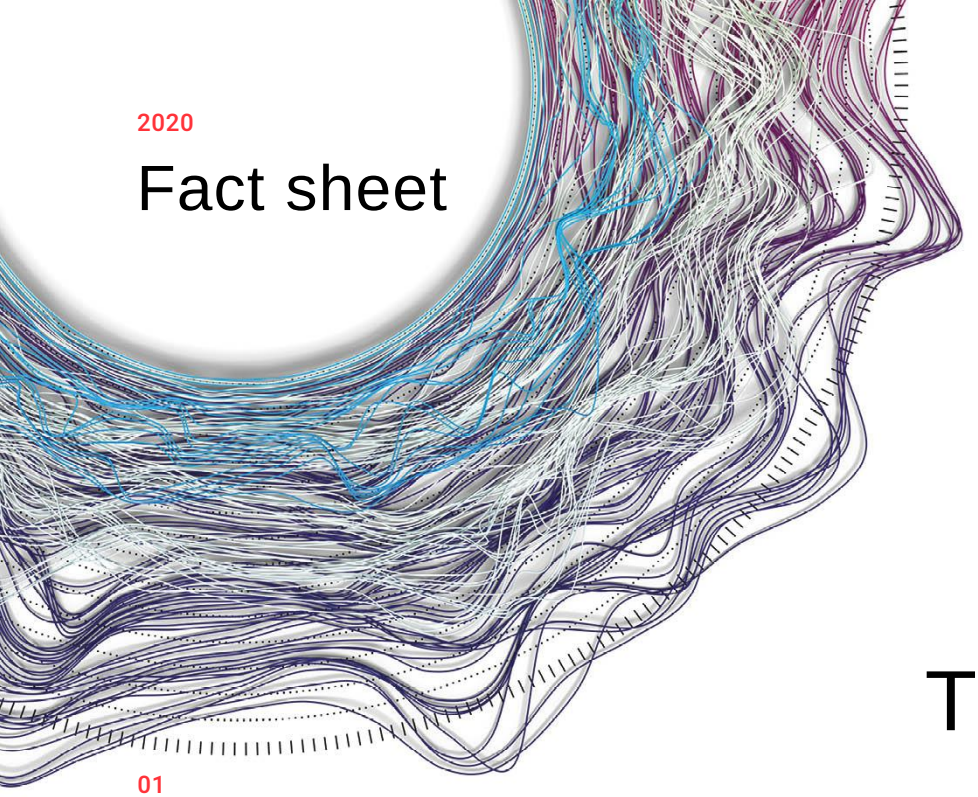
2020

Fact sheet

exeon

Detecting Hidden
Cyber Threats.



Exeon ThreatReport

01

Visibility into data leaving your organization

Cyber attackers and malicious insiders regularly circumvent IT protection measures and breach highly sensitive data. Such breaches often happen in plain sight, hidden in millions of regular activities caused by daily business operations and remain undetected over several months.

The current average detection time for a data breach is over 200 days. However, the detection time can also be much longer. For example, it took Marriott International more than four years to discover a data breach which exposed over 300 million customer records.
Exeon is specialized in detecting hidden data breaches 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 and effectively identifies gaps in IT security perimeters and detects anomalies in millions of data points (log data).
During our ExeonThreatReport security review, we use ExeonTrace to transform our costumer's network log data into actionable security insights.

02

Order a Security Review

Do you want to detect the potential needle in the haystack? During an ExeonThreatReport, our engineers review the security state of your network by analyzing your log data.

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.

Packages

The ExeonThreatReport offers two analysis packages. The packages can be selected independently or jointly. Package one analyzes proxy log data and package two 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- **Unauthorized and outdated devices:** Clustering of machine-to-machine (M2M) devices for outlier detection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)

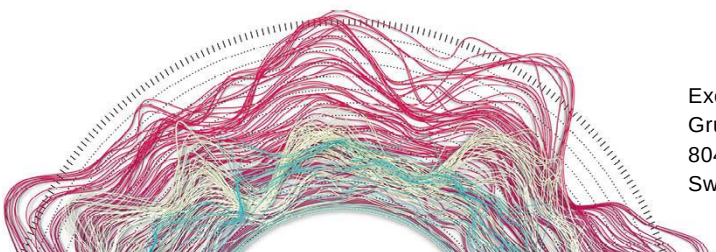
Requirements: The log data is recorded by an SSL/TLS-intercepting secure web gateway.

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.



Exeon Analytics AG
Grubenstrasse 12
8045 Zurich
Switzerland

info@exeon.ch