Protelion Threat Detection and Response

Automatically detects threats
across your network and endpoints

Focused on priorities

> On average, companies spend more than 200 days to identify security breaches and 70 days to contain them

Ponemon Institute, 2020 Cost of a Data Breach Report

PROTELION

Protelion Threat Detection and Response (TD&R) detects threats in real-time and simplifies incident handling by researching millions of new threats. This advanced analytics system is capable of identifying ransomware, fileless attacks, threats to remote workers and other threats in the dynamically changing network environment and threat landscape.

HIGHLIGHTS

CONTINUOUS MONITORING

New evolving TD&R technologies ensure highly efficient threat detection and are focused on real incidents. The Protelion TD&R solution features integrated expert analysis engines and a threat knowledge base for continuous monitoring of threats in the network and at endpoints.

READINESS TO DETECT

The threat knowledge base contains up-to-date threat intelligence data and AI data for machine learning to detect intruder's tactics, techniques and procedures.

THREAT INTELLIGENCE

The threat knowledge base contains up-to-date threat intelligence data and AI data for machine learning to detect intruder's tactics, techniques and procedures. The Threat Intelligence platform processes the data received from the global network in real-time and updates the TD&R`s threat knowledge base using an analysis of malicious behaviour and malicious sources.

AUTOMATIC ANALYSIS

Searching for threats in multiple sources requires resources and time to sift through large amounts of data, assess the impact on assets and respond to threats. However, Protelion TD&R focuses on potential threats and reduces the time needed to find and eliminate threats, from several months to hours and minutes.

PROACTIVE RESPONSE

A threat notification proposes containment measures that speed up the response and prevents incidents from recurring. Protelion TD&R initiates an investigation in a matter of minutes. You can have a prospective view of all events and incidents on a single panel tailored for quick investigation and analysis of incidents.

TRUST AND COMPLIANCE

Protelion TD&R maintains the principals of a zero-trust architecture to ensure compliance and threat detection when processing intellectual property data, as well as business and personal data.

KEY BENEFITS

Protelion TD&R carries out comprehensive threat monitoring in the network and at the endpoints, allowing you to make better decisions and respond faster.

01 As soon as a threat to business continuity is detected response measures are ready

02 Stay ahead of new threats using an up-to-date threat knowledge base

03 Turnkey solution that works immediately with rapid deployment on premise or in the Cloud

04 Comprehensive Threat Management Center

05 Reports on threats and incidents, as well as compliance reports

06 Option to customize rules for threat hunting tailored to the network environment

HOW IT WORKS

FOCUSED ON PRIORITIES

Deploy Protelion TD&R´s components on premise and in the cloud, add network settings, and start detecting threats and responding to them right away.

Management Center monitors statuses, configures sensors and Threat intelligence analytics system, and updates the threat knowledge base.

The sensors send data to the Threat intelligence analytics system, which uses meta-rules (threat intelligence data) and machine learning to identify malicious behavior and threats in the network and at the endpoints.

Responding to threats becomes faster, simpler, and more efficient with threat notifications that propose containment and remediation measures.

Automatic threat detection and analysis keep small and large businesses safe regardless of their experience in responding to threats even when there is not enough staff. An IT team of one or two people can improve threat detection immediately after the solution is deployed.

INTELLIGENT SUPPORT

The Threat Intelligence platform analyzes more than a million threats per day, and expert engines automatically correlate new data and update the threat knowledge base.

DATA EXCHANGE

A set of API and interfaces simplifies communications with other security solutions.

EVALUATION OF THREATS

Every day, the Protelion TD&R support team evaluates the threat monitoring procedure and threat knowledge base.

DATA

Data on the detected threats associated with incidents is available for up to 3 years (1,095 days).

All the metadata generated and analyzed is available for up to 45 days and can contain over 22,000 patterns and over 4,000 signs of threats.

Unlimited access to all data for further analysis of incidents. Reports on threats and incidents, as well as compliance reports.

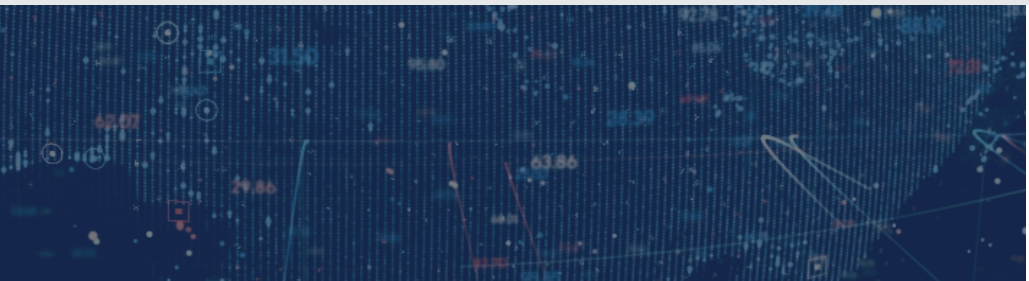
Data for in depth analysis. Contextual information to accelerate threat analysis and assessment.

EXPERT ANALYSIS

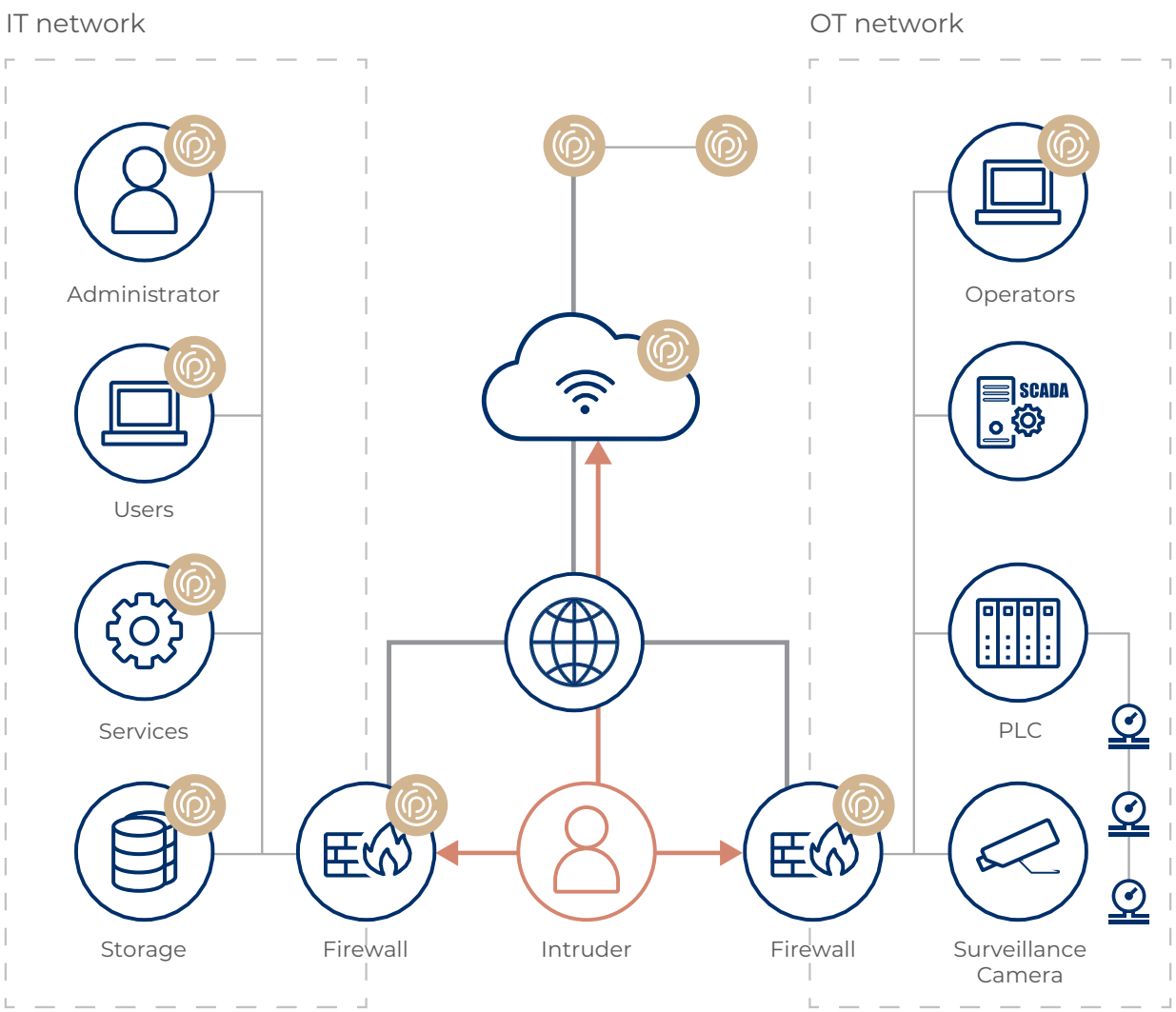
When a new threat is detected, send a sample to the TD&R support team and receive an additional threat assessment.

OPPORTUNITIES

- Take a remote training course in Protelion TD&R management and threat analysis in a real network environment on the Protelion Cyber Range Platform.
- Protelion TD&R solution ensures high ROI and lower TCO for self-service and service delivery.
- Support and partnership program.



PROTELION TD&R COMPONENTS



PROTELION

Protelion
Oberwallstr. 24
D-10117 Berlin

info@protelion.com

+49 30 206 43 66-0