cognitix Threat Defender

Anomaly detection, IDS/IPS, and segmentation

genua.

Internal Network Security

Non-invasive analysis of assets and network traffic, ultra-fast anomaly detection, and dynamic response

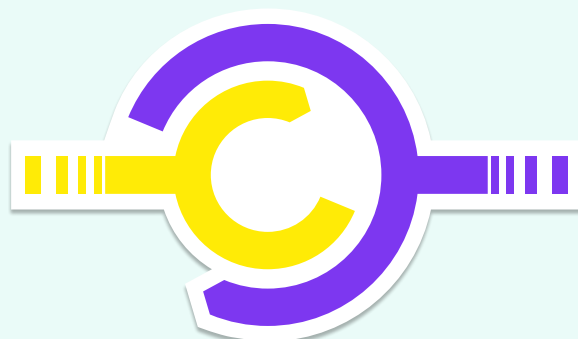### Optimum Availability and Security for Your Assets

With cognitix Threat Defender, you improve the security and availability of assets in IT and OT networks within an intrusion detection ecosystem.

- Intrusion Detection System (IDS):
  cognitix Threat Defender correlates the network traffic with up to tens of thousands of patterns and with intelligent analysis protocols to reliably identify threats

- Intrusion Prevention System (IPS):
  cognitix Threat Defender protects your assets in the network at all times without manual intervention and prevents damage

- Segmentation on layer 2 and 7:
  cognitix Threat Defender enables the micro-segmentation of the network structure up to the application level

All Advantages at a Glance

Real-time traffic detection of more than 3,700 applications/apps and protocols

Deep packet inspection (DPI) to monitor the data traffic up to the application level

Incident response with dynamic policies due to a smart event engine

Interface for federal and private-sector threat databases

Micro-segmentation at the network and application level

On-premises operation possible for exclusive (i.e. sovereign) data storage by the operator

Interested? Contact us:
+49 89 991950-902 or sales@genua.de

> There's a great deal of intelligence in the system. Without any additional manual effort, we have permanent 24/7 monitoring of the network traffic. Our network operation has yet again become significantly more secure against increasingly complex attacks.

Carsten Viell, IT Director Bad Reichenhall Public Utilities

SecurITy
made in Germany

SecurITy
made in EU

Secure Network Through Transparency and Anomaly Detection

cognitix Threat Defender provides visibility of all network traffic and supports network security by detecting anomalies, identifying attacks, and providing comprehensive protection against threats.
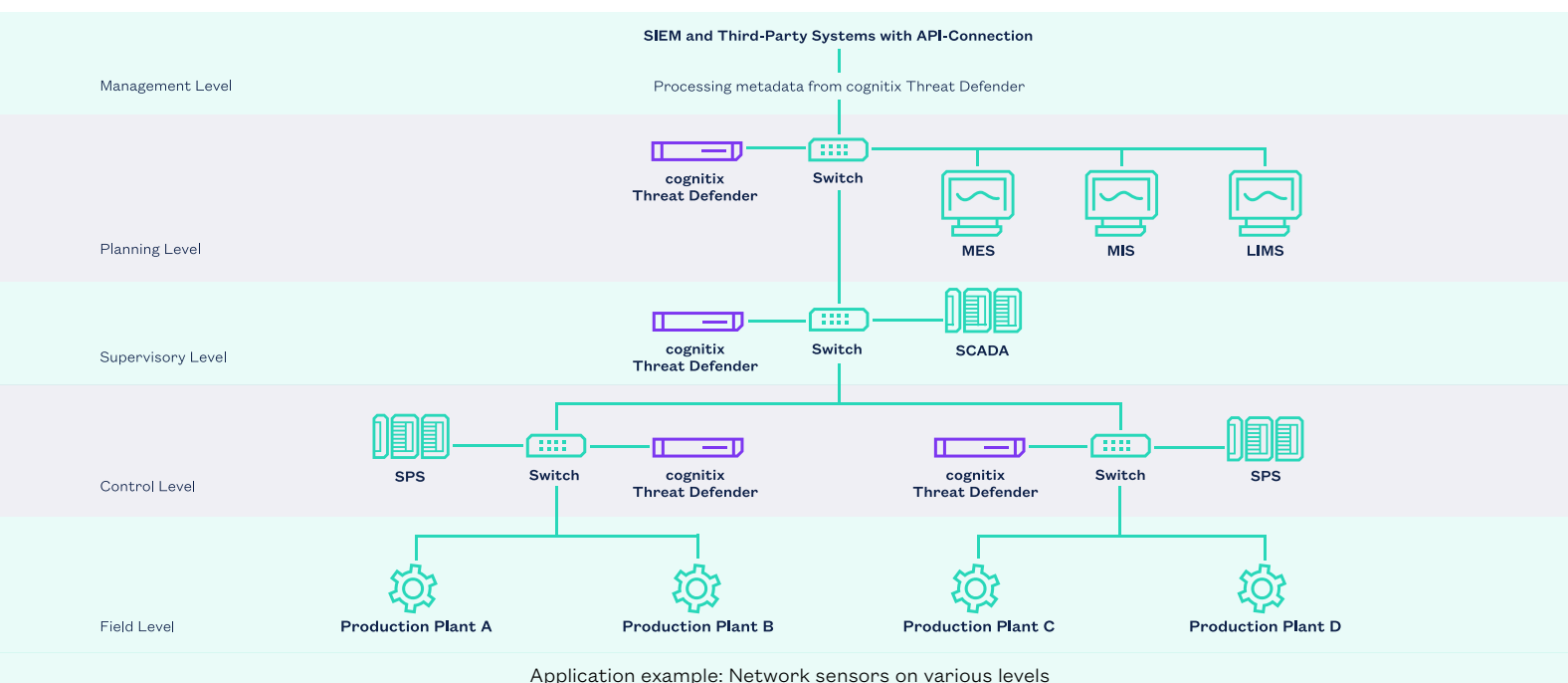
As an IDS with deep packet inspection, it recognizes attempted attacks and supports micro-segmentation to mitigate external and internal attacks.

In terms of response and recovery, cognitix Threat Defender responds to anomalies as an Intrusion Prevention System (IPS) and also provides valuable network information for forensic analyses.

Flexible Monitoring and Effective Defense

Comprehensive monitoring and reporting options can be used locally and across multiple sites. Network information can be evaluated either aggregated in the system or using connected alerting, SIEM, and monitoring applications.

Through its highly dynamic response to attacks cognitix Threat Defender enables effective network security. The information sources of the attack patterns (IoC) can be expanded, making it possible to adapt to specific requirements and the development of cyber threats.

SIEM and Third-Party Systems with API-Connection

Management Level — Processing metadata from cognitix Threat Defender

cognitix Threat Defender — Switch

Planning Level — MES — MIS — LIMS

Supervisory Level — cognitix Threat Defender — Switch — SCADA

Control Level — SPS — Switch — cognitix Threat Defender — cognitix Threat Defender — Switch — SPS

Field Level — Production Plant A — Production Plant B — Production Plant C — Production Plant D

Application example: Network sensors on various levels

Reasons Why

- Experts for the IT security of companies and public organizations

- Offer of a comprehensive, modular IT security portfolio

- Quality without compromise for all products, services, and processes

genua – Excellence in Digital Security

genua develops innovative, reliable as well as market-shaping products and solutions. Whether in the public sector, for the operators of critical infrastructures, in industry or in the protection of classified information: we provide answers to the IT security challenges of today and of tomorrow.

Further information:
www.genua.eu/threat-defender