cognitix Threat Defender Protokolldatensensor

Internal Network Security

Facts and Features

Definition

cognitix Threat Defender Protokolldatensensor is a solution to capture meta data of all flows of the network traffic and sends it to a SIEM system for later analysis in the SOC. Depending on the protocol used in the communication, a comprehensive set of meta data will be extracted. It operates transparently inside the network perimeter and can be installed at the network edge or anywhere within the network.

Typical Use

- Enable visibility into the network communication
- Capture meta data of all network activities for forensic analyses in case of an attack
- Provide a comprehensive set of meta data depending on the protocol used for communication
- All traffic will be analyzed by a DPI (deep packet inspection) engine to extract the best possible data for later processing

Reasons to Choose cognitix Threat Defender Protokolldatensensor

- Provides your SIEM with comprehensive protocol specific details of all flows in your network
- Transparent integration inside the network without configuration adjustment
- Suitable hardware variants meet the performance requirements of your network
- GDPR friendly
- Clear and focused user interface
- IT security made in Germany

Customer Service

- Customer service directly from the manufacturer
- Security system management
- Hotline service

SecurITy made in Germany

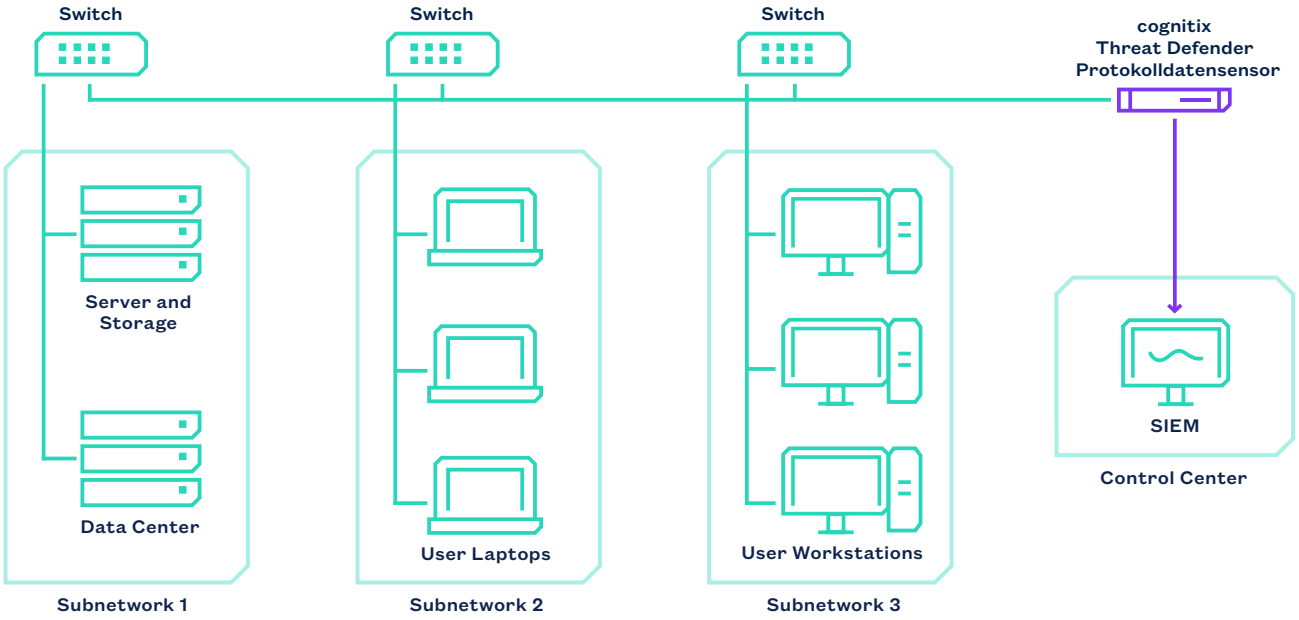
Network Integration	
Data extraction	
Mirror port	RX/TX must be received on one port
TAP	RX/TX must be received on one port
SPAN	RX/TX must be received on one port
Supported network capabilities	
Monitoring ports	Depending on the hardware variant, the system can monitor up 18 different sources, e.g. mirror ports
VLAN	VLAN information is part of the extracted meta data

SOC Export	
Capture	
Network flows	The system captures the meta data of all network flows
Deep packet inspection (DPI)	Depending on the communication protocol, the build in DPI engine extracts all meta data for the respective protocol
Export formats	
Elastic Search	Export using HTTP format for importing into Elastic Search
Syslog	Export using the syslog CIM format for importing into e.g. Splunk
IPFix	Export using the IPFix format for importing into respective systems

System Monitoring	
Monitoring options	
Hardware status	Status and health of all hardware components
System health	System health and load
Admin actions	An audit log of all configuration changes
Infrastructure monitoring interfaces	
genucenter integration	Core performance data is shared with the Central Management Station genucenter
SNMP v2/3	Network interface and system parameters are exposed for SNMP monitoring with tools like Checkmk, Zabbix or Paessler PRTG
SNMP traps	Administrators can define for which class of events SNMP traps will be send
Syslog	All syslog data can be exported to a remote syslog server

Administration	
General	
Web GUI	User-friendly, easy to learn web-based interface
Online documentation	Searchable HTML documentation provides quick help
Backups	Download and restore portable configurations
Admin accounts	
Local or LDAP accounts	Admin accounts can be configured locally or accounts from a connected LDAP server can be used
Role-based administration	Admin accounts can be assigned to various roles with different capabilities
Updates	
Automatic update	For systems which can access the genua update server, each new release will be offered as an update. Once confirmed by the admin, the update will be installed automatically.
Offline update	Update the system via web interface with newer releases, e.g. in air-gapped networks

Use Case



Visibility of Network Communication

cognitix Threat Defender Protokolldatensensor is connected to the mirror port of all major switches to see all traffic going from and to critical infrastructure and servers. All meta data communication is collected and consolidated into a central SIEM system for correlation and threat hunting.

Further Information:

www.genua.eu/threat-defender

genua GmbH
Domagkstrasse 7 | 85551 Kirchheim | Germany
+49 89 991950-0 | info@genua.eu | www.genua.eu

1025-02-E