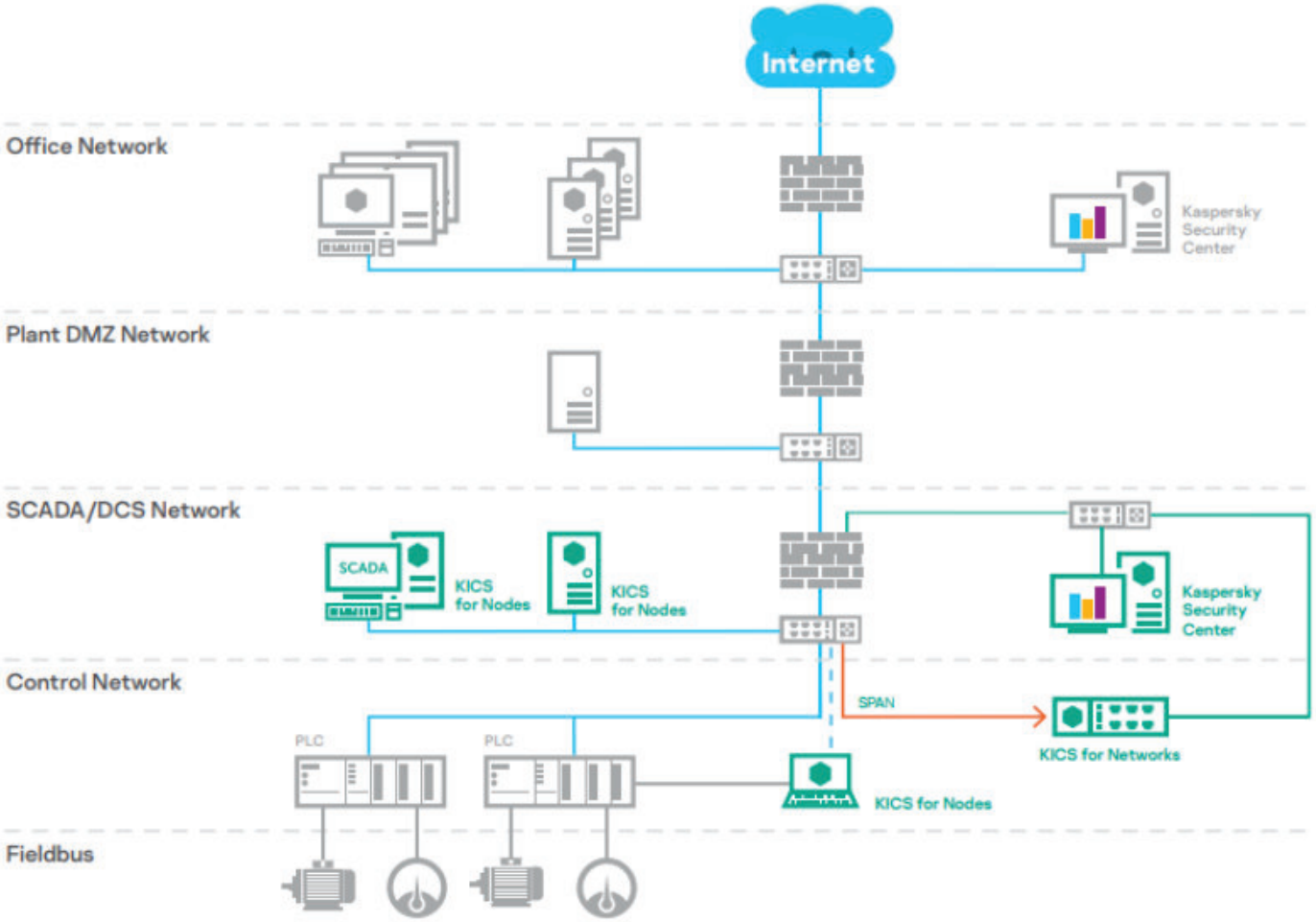
Kaspersky Industrial CyberSecurity

KICS product deployment



Passive network traffic monitoring and anomalies detection

Protection for SCADA, HMIs, historian, operator and engineering workstations, Windows & Linux

Works in air-gapped and distributed environments

Recap - Solution for industrial enterprises

Kaspersky Single Management Platform

Platform

Kaspersky Industrial CyberSecurity

for Nodes
Endpoint Protection, Detection and Response

for Networks
Network Traffic Analysis, Detection and Response

Services

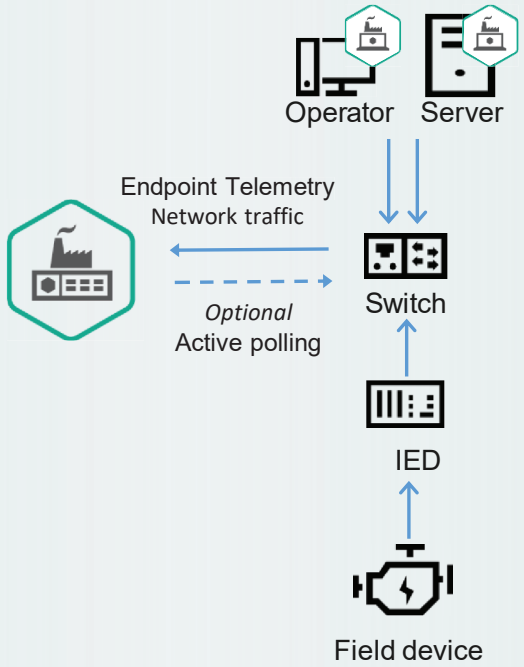
Training and Awareness

- Kaspersky Security Awarness
- Kaspersky Cybersecurity Training

Expert Services and Intelligence

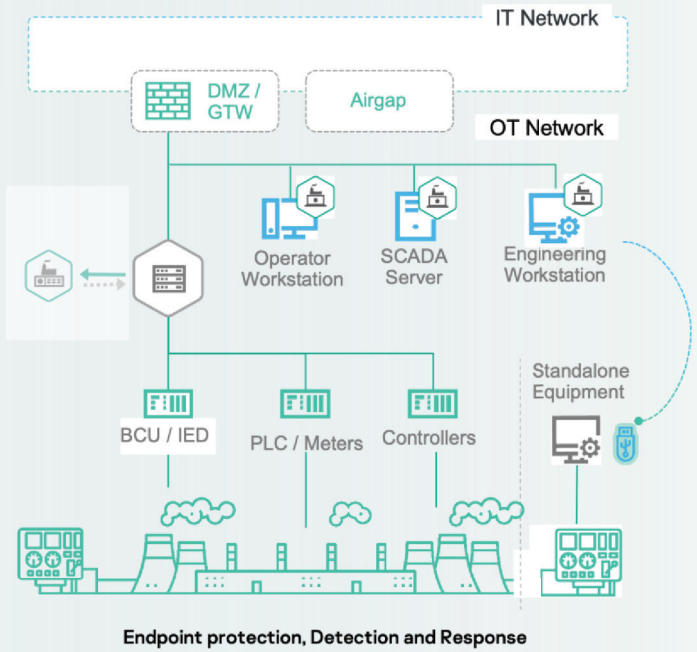
- Kaspersky Threat Intelligence
- Kaspersky Security Assessment
- Kaspersky Incident Response

Kaspersky Industrial CyberSecurity for Networks



Connected passively to ICS network

Kaspersky Industrial CyberSecurity for Nodes



KICS for Nodes. Options and application

Windows

Portable Scanner

Linux

Audit Agent

Gateway

Engineering workstation

Historian Server

System management workstation

SCADA server

Embedded systems

Operation workstation

Key benefits

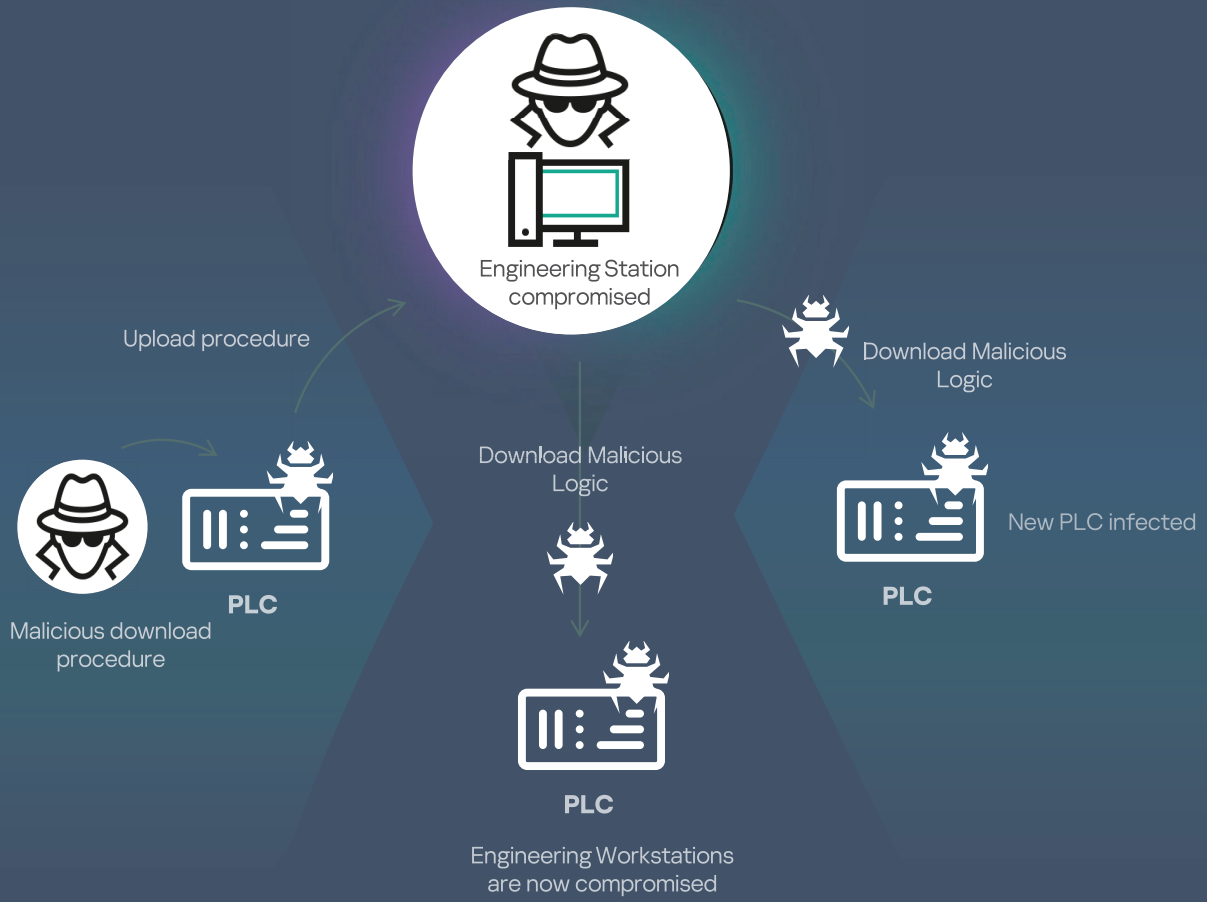
Kaspersky Industrial CyberSecurity for Nodes

- Compatibility* with Industrial Automation Vendors
- Legacy OS support starting from Windows XP SP2
- Non-blocking (statistic mode) availability
- No reboot on installation, update or upgrade
- Air-gapped database updates
- Components and settings specific for OT
- Modular architecture – component selection
- Tunable system resource consumption

* Learn more: **certification**

How important is to know about the ICS Attacks & OT Protocols?

Weaponized PLCs Can Hack Engineering Workstations in Attacks on Industrial Orgs



PLC Attack

- PLCs can be a tempting target for threat actors as they can be abused to cause damage and disruption, and to make changes to the processes they control.
- Evil PLC Attack - hacker first compromises the PLC, which can often be exposed to the internet and unprotected, and then tricks an engineer into connecting to the PLC from the engineering workstation

Ransomware and Data exfiltration – OT Environments

Ransomware Scenario

- Spyware is used for unauthorized remote access, exfiltration of confidential information or information used to deliver next-stage payloads, such as ransomware
- In many attacks, ransomware is the last stage of the kill chain

Malicious entity implants ransomware using phishing, file introduction or malicious website and gains access to enterprise IT System.

Ransomware exploits vulnerabilities on the receiving host and then, executes further malicious functionality.

Ransomware utilizes poor containment by traversing networks with weak ACLs, dual NIC and is able to access OT or beyond

Lack of controls with OT networks allows ransomware to spread across multiple business units, servers, hosts - further adding disruption

Lack of consistent, tested offline, secure backups, good practices of configurations or software means restorations is a highly involved and lengthy process

WannaCry Ransomware

nificant for the industrial sector – such contaminations can cause far-
tive target (especially WannaCry and exPetr type infections).

cific objectives – instead of encrypt data, malware can disrupt operations or

Most critical events

Events with the highest scores.

Event	Linked devices	Technology	Score
Attempted network interactions with IP address [redacted] in external network 2023-09-25 11:05:28	* (12) [redacted]	EXT	9.7
Attempted network interactions with IP address [redacted] external network 2023-09-25 11:28:16	* (12) [redacted]	EXT	9.7
Attempted network interactions with IP address [redacted] external network 2023-09-25 10:41:14	* (12)		
Attempted network interactions with IP address [redacted] external network 2023-09-25 11:04:06	* (12)		
Attempted network interactions with IP address [redacted] external network 2023-09-25 11:05:24	* (12)		
Attempted network interactions with IP address [redacted] external network 2023-09-25 11:05:54	* (12)		
Attempted network interactions with IP address [redacted] n external network 2023-09-25 11:04:39	* (12)		
Attempted network interactions with IP address [redacted] n external network 2023-09-25 11:05:44	* (12)		
Attempted network interactions with IP address [redacted] external network 2023-09-25 11:05:23	* (12)		
Attempted network interactions with IP address [redacted] in external network 2023-09-25 10:42:33	* (12)		

Most frequently triggered malicious activity detection rules

Malicious activity detection rules that were triggered most frequently on the devices.

Rule	Devices	Events
Exploit.CVE-2017-0144.UDP.C&C	CNC-D-III-New ([redacted]), [redacted]), WORKGROUP ([redacted])	26
Trojan-Ransom.Wanna.UDP.C&C	CNC-D-III-New[redacted], [redacted] WORKGROUP[redacted]	26
NetTool.TorTool.TCP.C&C	CNC-D-III-New [redacted] WORKGROUP [redacted]	12
NetTool.TorToolE.TCP.C&C	CNC-D-III-New [redacted] WORKGROUP[redacted]	5
Trojan.ShadowBro-kers.SMB.ServerRequest	CNC-D-III-New [redacted] WORKGROUP [redacted] PC [redacted]	2
Trojan-Spy.Stealer.TCP.C&C	AYS0003 [redacted] AYS0148 [redacted] * (12) [redacted]	2

KICS for Networks 4.0 - Industrial Protocols Supported

- OPC UA Binary
- PROFINET IO and RPC for PROFINET IO
- Schneider Electric UMAS
- Siemens Industrial Ethernet
- Siemens S7comm, S7comm-plus
- TASE.2
- YARD
- Yokogawa Vnet/IP
- Relematika BDUBus
- PNU20
- Modification of the Modbus TCP protocol for devices of Ekra 200 series
- AutomationDirect DirectLOGIC device interaction protocol
- Protocol for interaction of Foxboro FCP270, FCP280 devices
- IPU-FEU device interaction protocol
- MiCOM C264 device interaction protocol
- Valmet DNA device interaction protocol
- Protocol for initial setup of Prosoft-Systems devices
- DTS data transfer protocol
- Protocol of devices with Siemens DIGSI 4 system software
- Protocols for interaction of devices in Honeywell Experion PKS / PlantCruise control systems
- Protocols initial configuration/interaction of Moxa NPort series devices
- Protocols detection/interaction Honeywell ControlEDGE 900 series devices
- ABB SPA-Bus
- Allen-Bradley EtherNet/IP
- BECKHOFF® ADS/AMS
- BSAP
- CODESYS V2 and V3 Gateway over TCP and V3 Gateway over UDP
- COS
- DMS for ABB AC 700F devices
- DNP3
- Emerson ControlWave Designer
- Emerson DeltaV, including the protocol for updating embedded software (firmware)
- FTP
- General Electric EGD
- General Electric SRTP
- IEC 60870: IEC 60870-5-101, IEC 60870-5-104
- IEC 61850: GOOSE, MMS (including MMS Reports), Sampled Values
- INA2000
- KNXnet/IP
- Mitsubishi MELSEC System Q
- MMS (ISO 9506-2)
- Modbus TCP
- OMRON FINS
- OPC DA, protocol for interaction of devices over WMI technology

Kaspersky Industrial CyberSecurity for Nodes

All-in-one industrial-grade endpoint protection, EDR agent and endpoint sensor

KICS for Nodes. Components

Windows Nodes

- Anti-Malware
- Application Launch Control
- Device Control
- File Integrity Control
- **PLC Integrity Control**
- Anti-Cryptor
- Exploit Prevention
- Network Threat Prevention
- Windows Log inspector
- Wi-Fi control
- **Firewall Management**
- Registry Monitor
- Portable Scanner

Endpoint Agent

- Security Audit
- EDR Agent
- Endpoint Sensor (Integration with KICS for Networks)

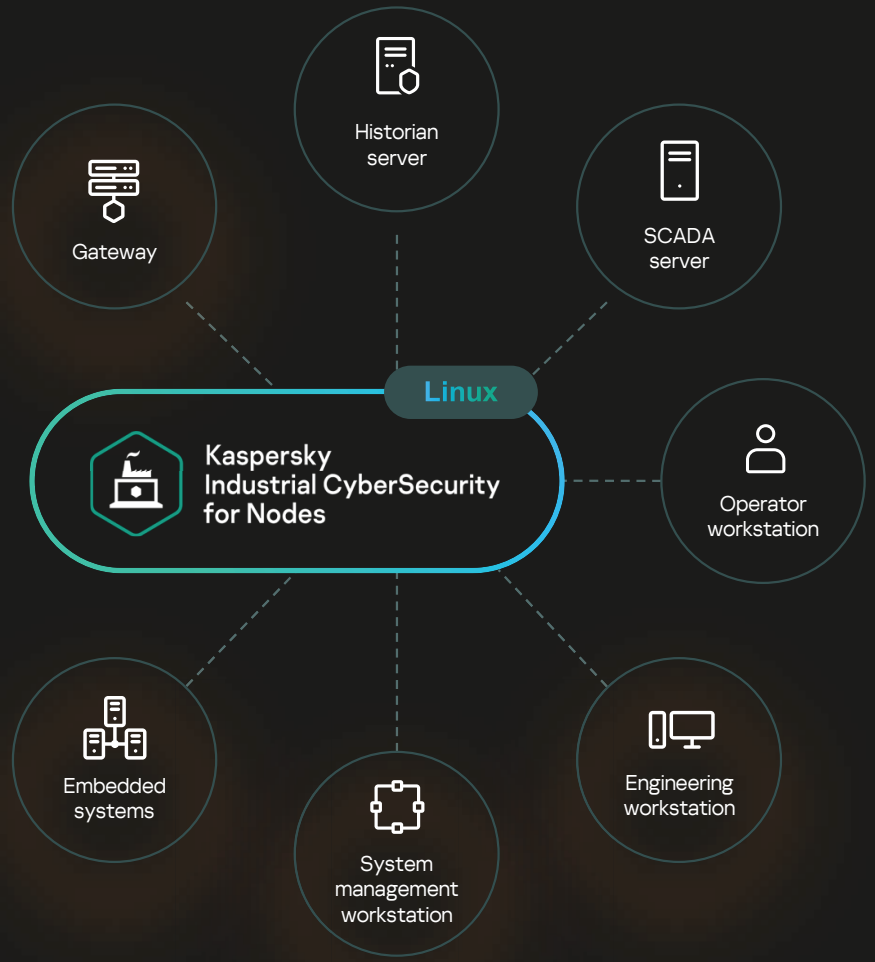
Industrial Endpoint Protection

KICS for Nodes. Components

Linux Nodes

- Anti-Malware
- Application Launch Control
- Device Control
- File Integrity Monitoring
- Anti-Cryptor
- Behavior Detection
- Network Threat Protection
- Firewall Management — Endpoint Agent
- Endpoint Sensor (Integration with KICS for Networks)

Industrial Endpoint Protection



KICS for Nodes. PLC and ICS coverage

PLC Integrity Control

PLC project change control to maintain OT process integrity

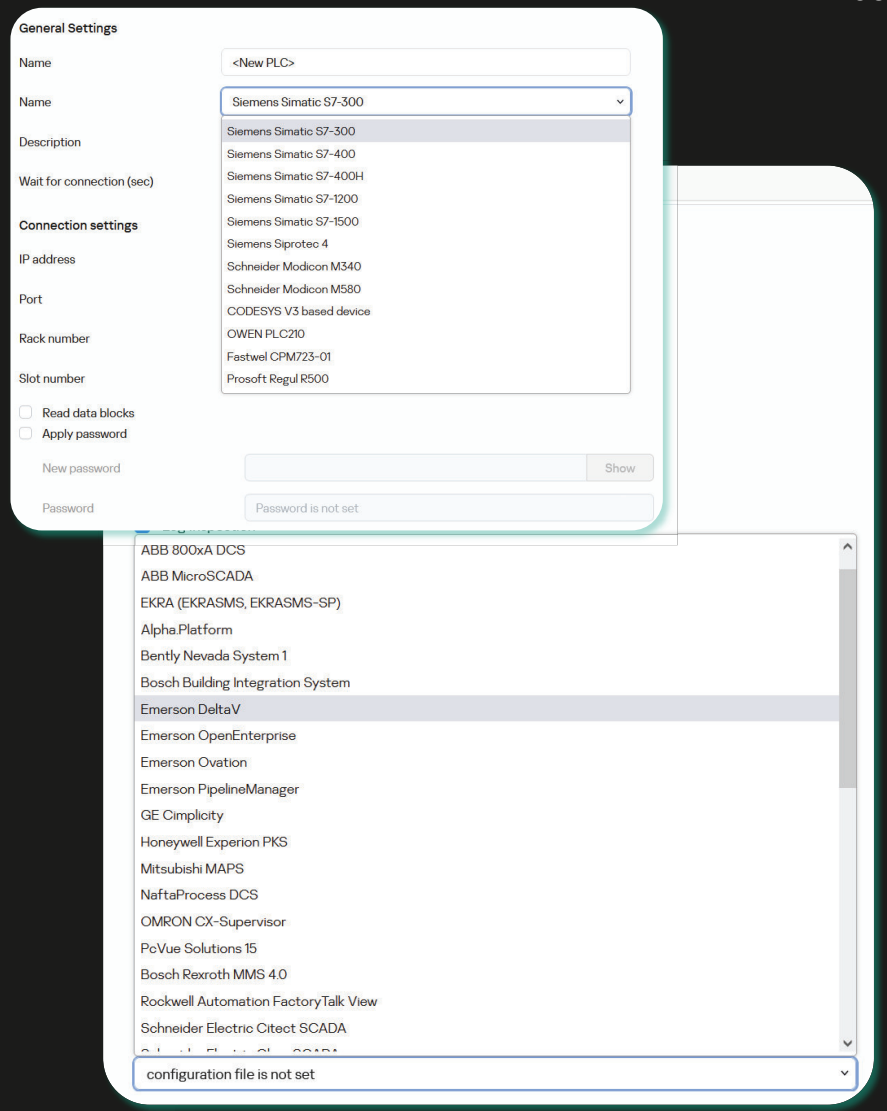
Verified Compatibility with ICS Vendors

- Cooperation with industrial automation vendors
- Joint compatibility and interoperability verification
- Joint reference architectures spanning different products

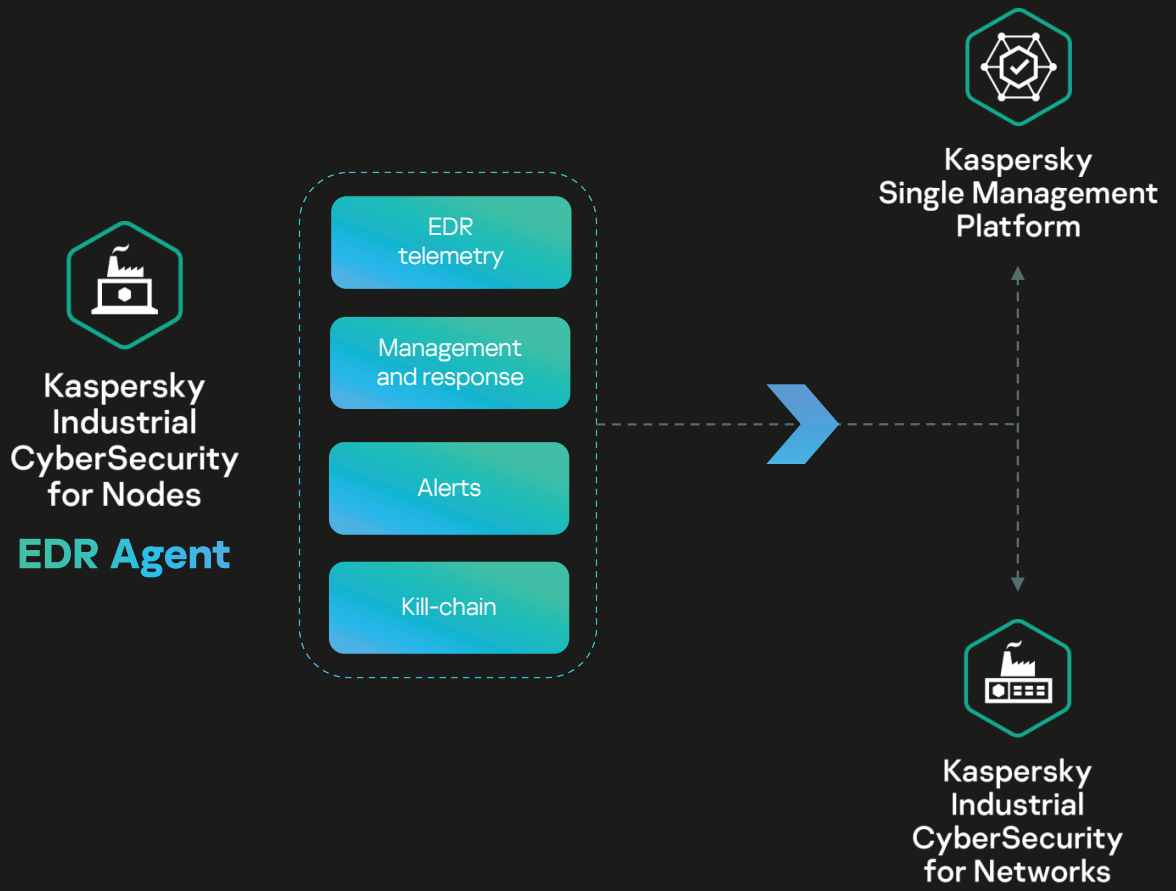
Recommended Settings

Recommended trusted processes and exclusions available out of the box and available for application on installation phase

- Expertise based on compatibility verification results
- Joint ICS vendor guides
- Technical support and issue resolution involving product experts with industry experience



KICS for Nodes. EDR Agent



Industrial-grade Endpoint Detection and Response (EDR)

Manageable from Kaspersky Security Center (ICS EDR) and KICS for Networks as part of OT XDR platform

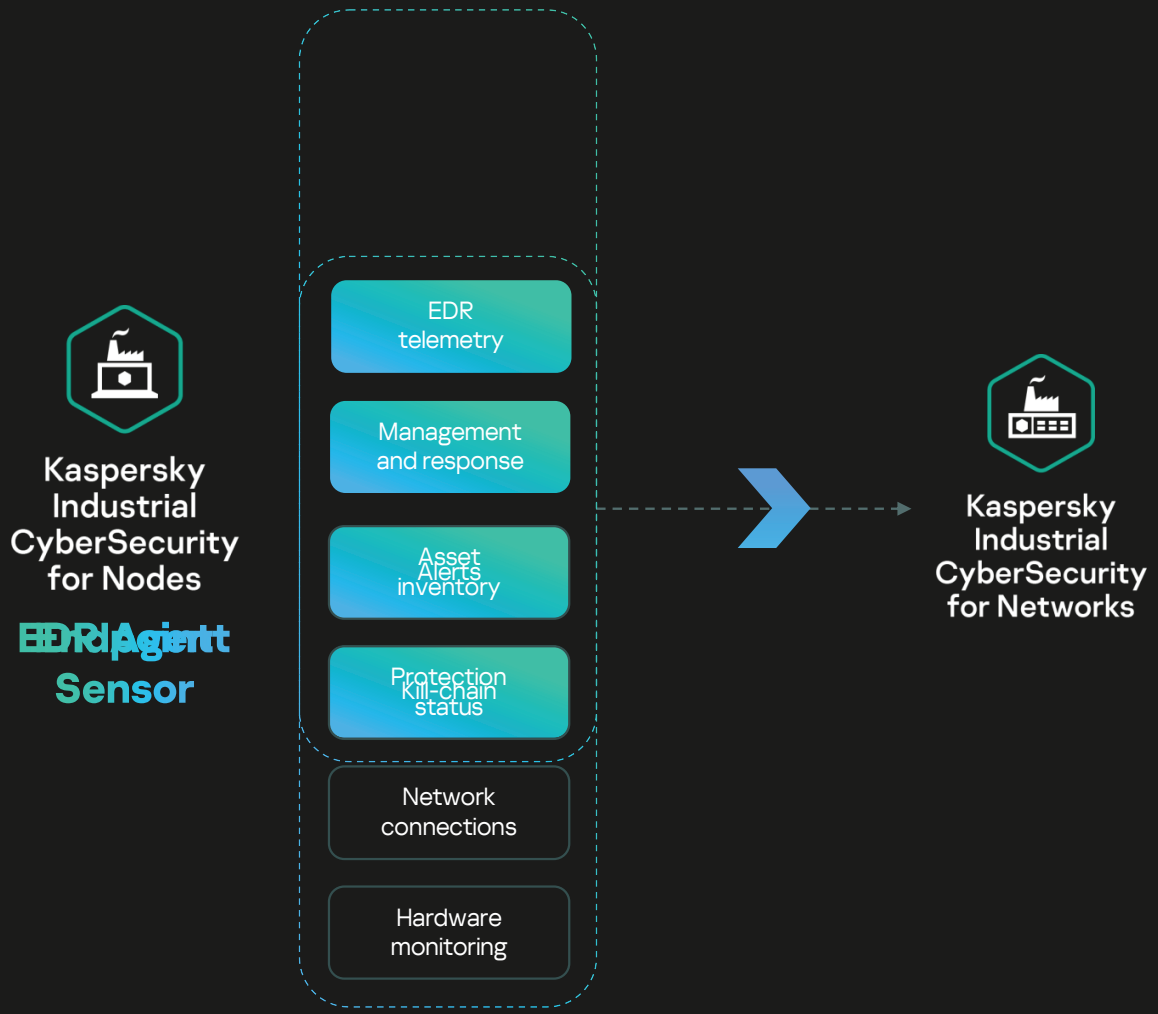
Detection and telemetry for root-cause analysis:

- Files, processes, registry and network communications telemetry
- Alert kill-chain visualization
- Indicators of Compromise

Response options:

- Prevent execution
- Quarantine file
- Isolate host

KICS for Nodes. All-in-one Endpoint Sensor



All-in-one Endpoint Sensor (Asset Inventory + EDR)

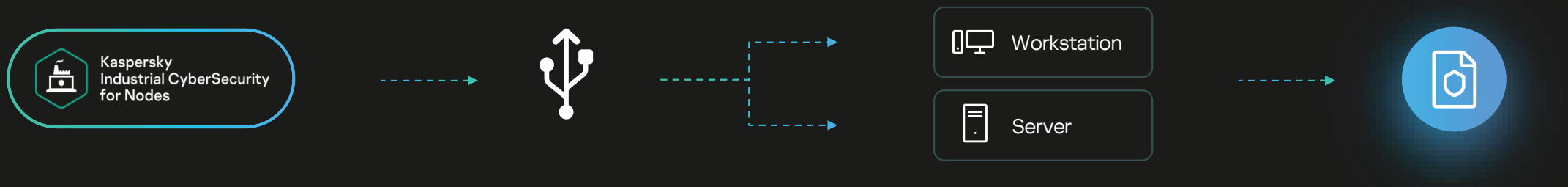
Integration of KICS for Networks and KICS for Nodes enables asset inventory functionality:

- Host attributes (host name, vendor, model, OS and more)
- EPP status
- Network communications
- Hardware monitoring
- Network alert enrichment by accurate host information (processes, users)
- Security audit for discovering vulnerabilities and risks

KICS for Nodes. Portable Scanner

- Standalone ICS systems without network connection
- Systems where Anti-malware software installation is not permitted or not possible
- Guest laptop security verification

- ✓ USB-drive with KICS for Nodes Portable Scanner
- ✓ Portable scanner compatible for use with legacy OS
- ✓ Installation-free approach and no impact on process operation
- ✓ Blocking or “notify only” modes
- ✓ Reports are stored on Portable Scanner USB-drive



KICS for Nodes with KICS Portable license

- Standard USB-flash drive to prepare scanner
- Copy protected
- Command-line based interface
- No installation

Scan standalone or restricted Windows-based ICS components with no impact

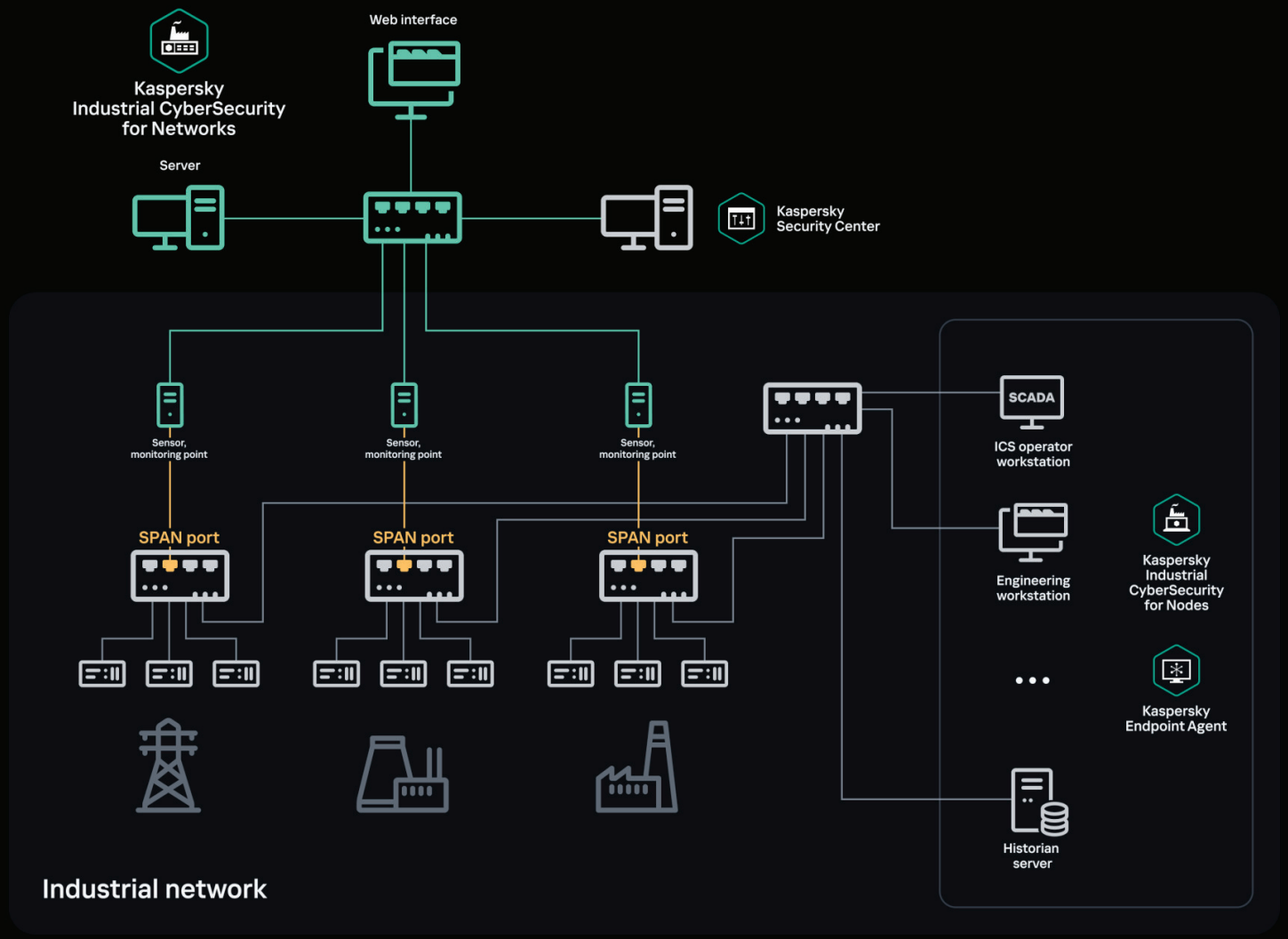
Reports are stored on Portable Scanner USB-drive

Systems can be scanned one by one with same Portable Scanner

Kaspersky Industrial CyberSecurity for Networks

Industrial network discovery and visualization, risk management and threat detection

KICS for Networks. Architecture



Complete visibility for distributed environments

KICS for Networks Server – central node for local data processing

- Capture and store raw traffic
- Receive telemetry from endpoints
- Process all information from numerous sites, register assets and alerts in product database
- Point of integration and data sharing

KICS for Networks Sensor - external node for traffic capturing and pre-processing

- Capture and store local raw traffic
- Receive telemetry from local endpoints
- Pre-process and send pre-processed data to the Server

KICS for Networks. Technologies

Kaspersky Industrial CyberSecurity for Networks

XDR

- Correlated events from network and endpoints
- Network event enrichment by endpoint telemetry, user and process data
- Advanced threat detection + kill-chain view
- Response action availability

Asset Inventory

Automatic asset inventory and data collection using passive and active methods of data gathering

Network Inventory & Visualization

- Network communications map
- Network topology diagram

Vulnerability & Risk Assessment

- OT-specific vulnerability and risk management
- Automatic scoring & prioritization
- Risk remediation recommendations
- Links to ICS vendor resources

Network Anomaly Detection

Network integrity control with baseline deviation monitoring and detection of malicious and suspicious network activity

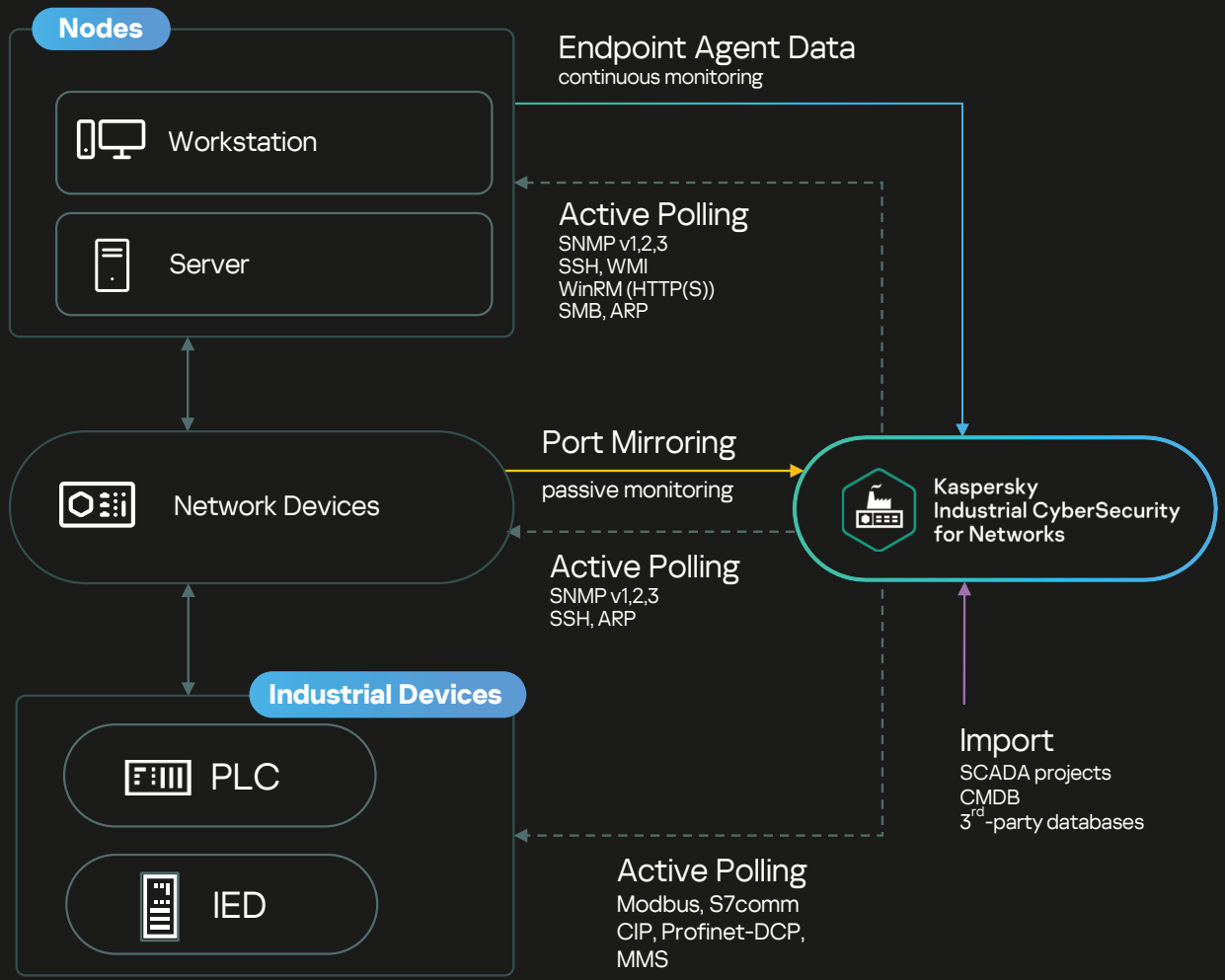
OT Process Control & Deep Packet Inspection

- Industrial payload data extraction
- Real-time process control
- Industrial command control
- Advanced OT process monitoring by Kaspersky MLAD

Integration and Data Exchange

- Centralized information
- Integration with Kaspersky and third-party or Customer systems (IEC 104, OPC, CEF, Syslog, API-based connectors)

KICS for Networks. Asset Inventory



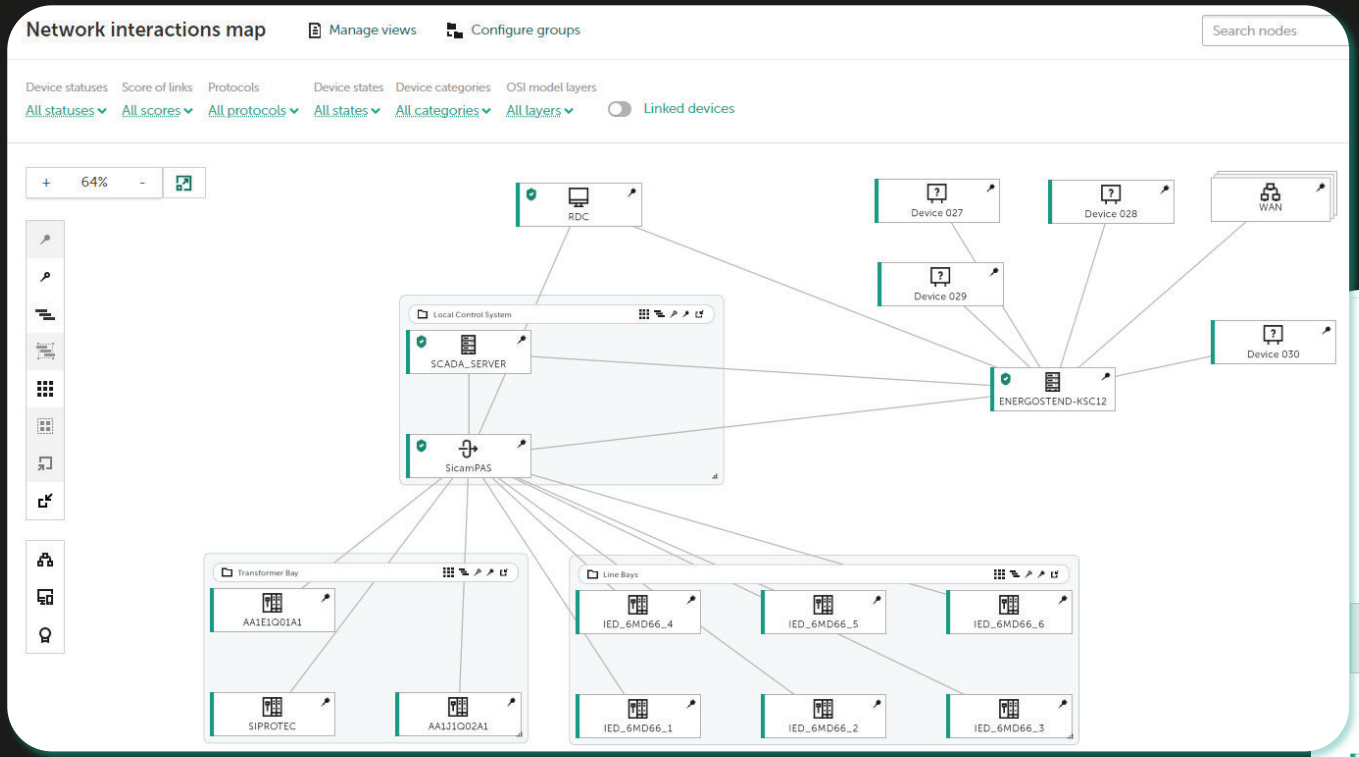
Asset Inventory

1. Passive Monitoring (SPAN session)
2. Endpoint Agent Telemetry Data (SPAN-less)
3. Active Polling
4. Configuration Import (manual or automated)

Key benefits

- **Different Methods** for asset inventory
- **Efficient approach**, not depending on site production phase
- **No SPAN session dependency** to conduct asset inventory
- **Active Polling risks are minimized** – fully aligned with device category, only supported protocols and methods are used
- **Risk analysis and security audit** – made by automatic device inventory and categorization

KICS for Networks. Network Inventory & Visualization



Network topology diagram

- Physical network connection diagram
- Permits to determine Ethernet switch port a device is connected to
- Built automatically based on active network equipment polling
- Device security status is reflected on topology

Network interactions map

- Logical network communication diagram
- Communications protocols and amount of traffic
- Grouping, Search and Filtering
- Bound to timeframe chosen by user

KICS for Networks. OT Vulnerability, Risk & Security Configuration Assessment

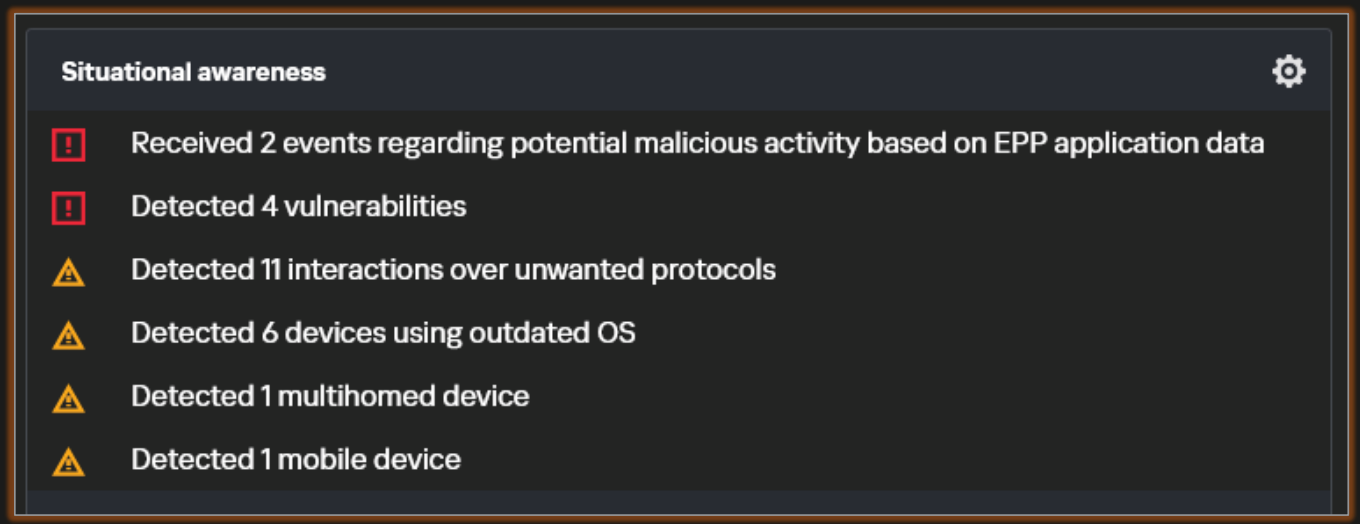
Incident | What happened? › Risk | What could happen?

Granular risk scoring for better prioritization

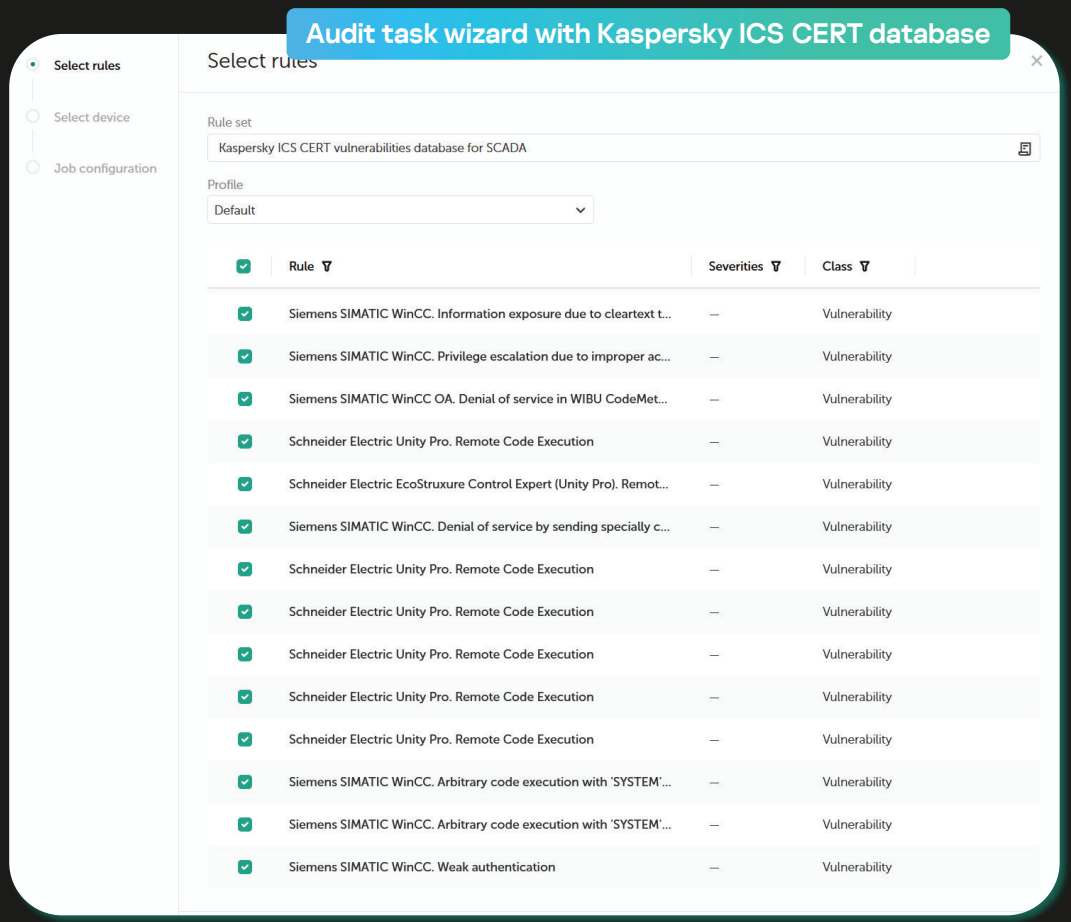
Dynamic scoring based on importance of the asset, its network connections and vulnerabilities

Customizable base risk scores

- Vulnerable network architecture
- Weak host security settings
- Obsolete, vulnerable, inappropriate, unencrypted protocols, anomalies in network protocols
- Outdated OS, unauthorized devices
- Vulnerabilities for industrial devices



KICS for Networks. Security Audit rules

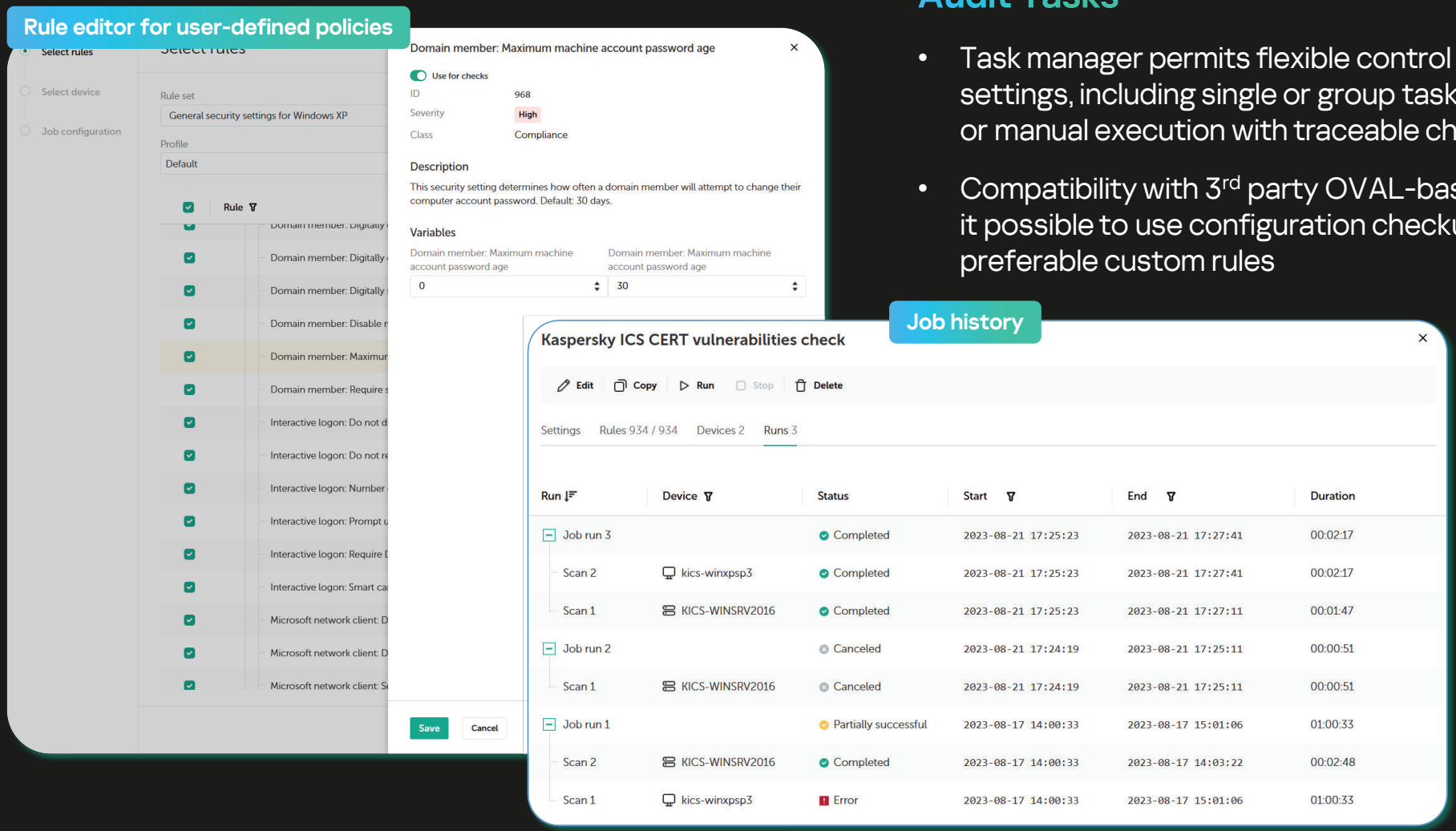


Set of security audit configuration rules is provided with product out of the box

- Kaspersky ICS CERT vulnerabilities database for SCADA
- General security settings for Windows XP/7/8.1/10/11
- General security settings for Window Server 2012/2012 R2/2016/2019/2022
- General security settings for Debian
- General security settings for Red Hat Enterprise Linux, CentOS, Oracle Linux
- General security settings for Ubuntu
- General security settings for SUSE Linux Enterprise, openSUSE
- Security Level -1 for Cisco routers and switches
- Security Level -2 for Cisco routers and switches
- General security settings for FortiGate

New configuration rules are provided with product updates, specific rule sets may be developed and provided upon request

KICS for Networks. Security Audit tasks



Audit Tasks

- Task manager permits flexible control of task settings, including single or group tasks for scheduled or manual execution with traceable change history
- Compatibility with 3rd party OVAL-based rules makes it possible to use configuration checkups against preferable custom rules

KICS for Networks. Network Traffic Analysis, Core Functions

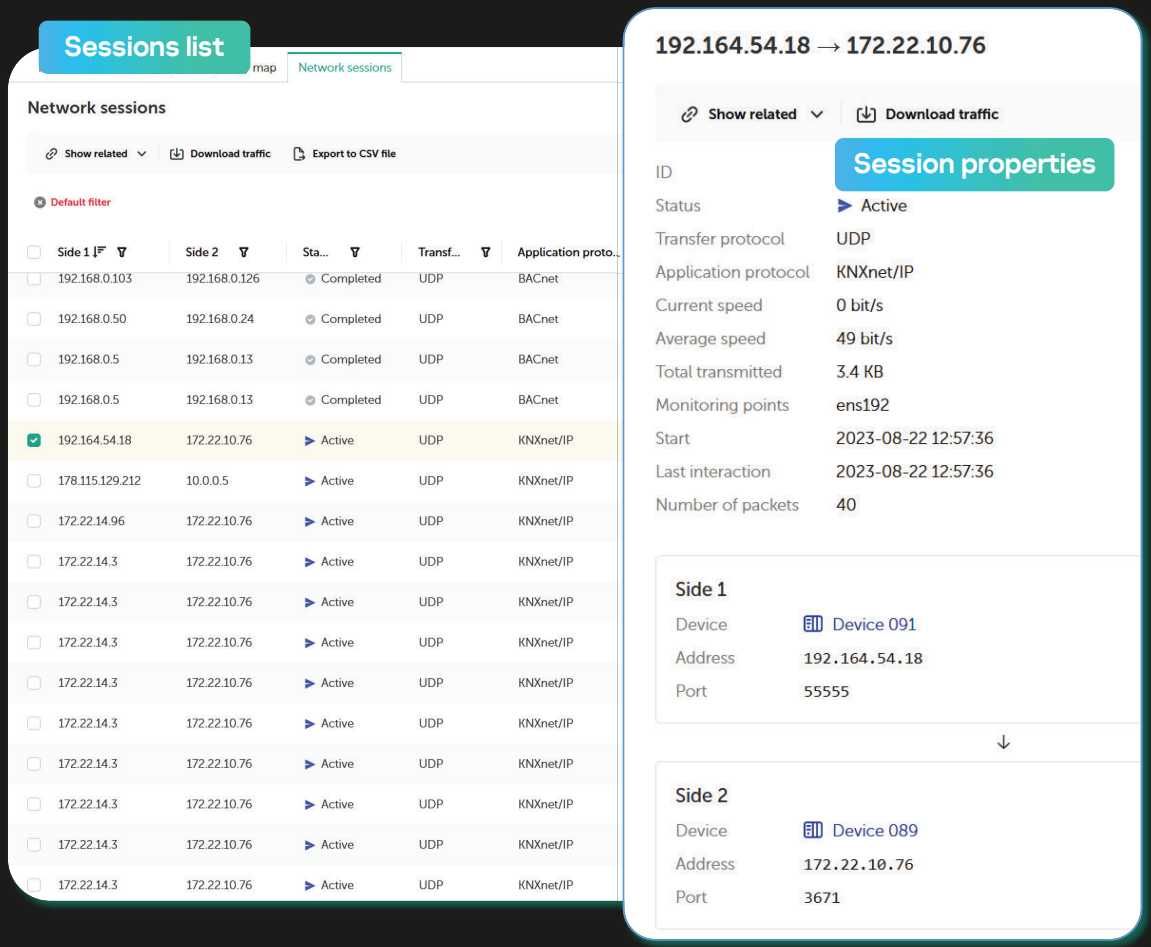
Network Traffic Analysis (NTA)

1. NTA systems analyze traffic both at the perimeter and in the infrastructure, unlike IDS / IPS
2. NTA systems use a combined set of technologies and methods to detect attacks – detection of deviations from the network baseline, behavioral analysis, detection rules, indicators of compromise, protocol inspection
3. NTAs are actively used to investigate incidents, store information about network interactions in a processed form, as well as an archive of raw traffic for a long time
4. In incident investigation, NTA is used as source of historical information on network activity, providing instruments for network information processing

Industrial NTA

- Improved attack and anomaly detection capabilities by use of statistic analyzer (bruteforce/spoofing/temporal anomalies)
- Network session detection capabilities (session status, destinations, protocols, traffic data)
- May work with separate storages for traffic archives
- Advanced settings for traffic archives
- Uploading PCAPs for incident investigation (traffic per node, per protocol, per time range, per session)

Network Traffic Analysis: Network sessions



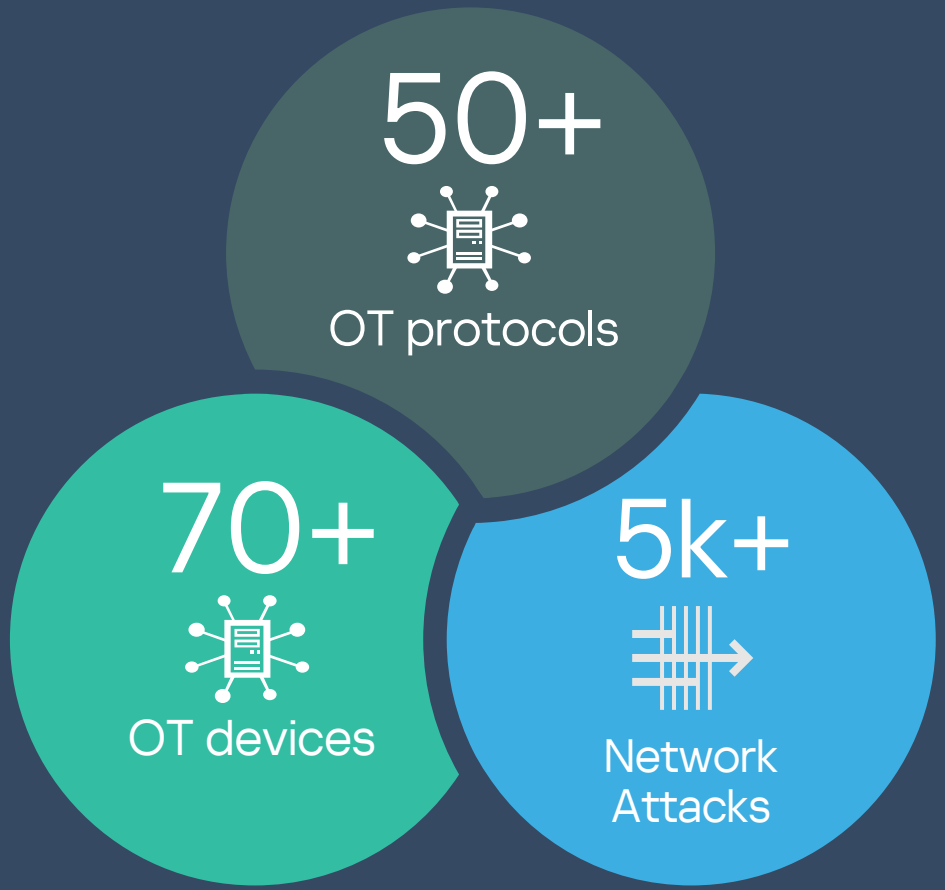
Network sessions

- Session status (Active/Completed)
- Communication direction
- Transport and application protocols
- Sessions statistics (speed, bytes)

Use cases

- Observing count of active session for specific protocol
- Analyzing sessions timestamps for temporary connections
- Traffic download for selected sessions

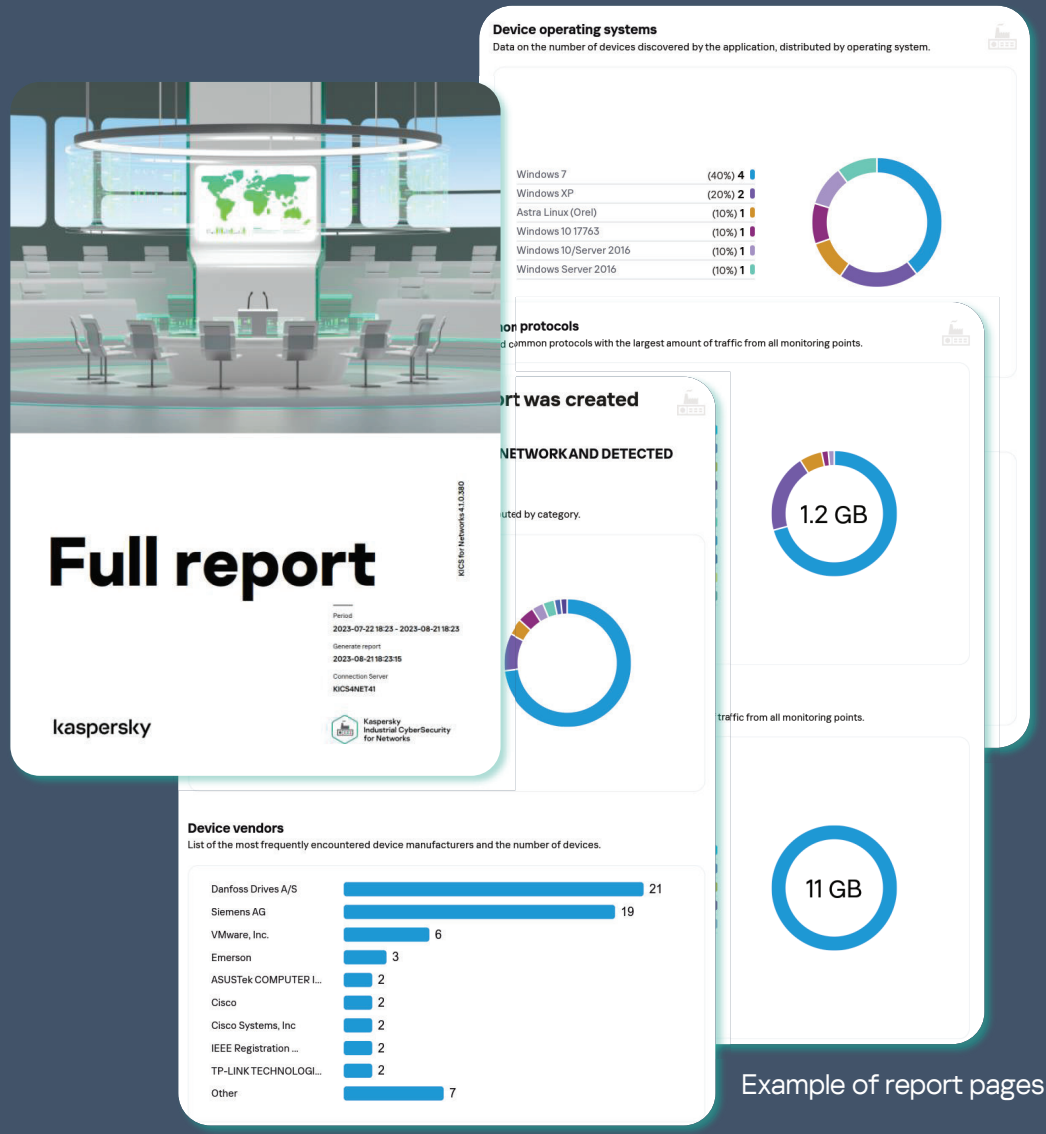
KICS for Networks. Support for Industrial Devices and Protocols



- Deep Packet Inspection (DPI) for OT and IT protocols
- Updates for DPI without necessity of product reinstallation or upgrade
- Support for new device models and protocols is provided via regular product updates
- Automatic process parameter detection and ready to use automatically generated process parameter rules
- SCADA project import for industrial devices and process parameters
- Passive PLC project integrity control

KICS for Networks. Reports

- OT network inventory
- Network baseline
- Risk summary
- Adjustable time period
- Scheduling and e-mail delivery

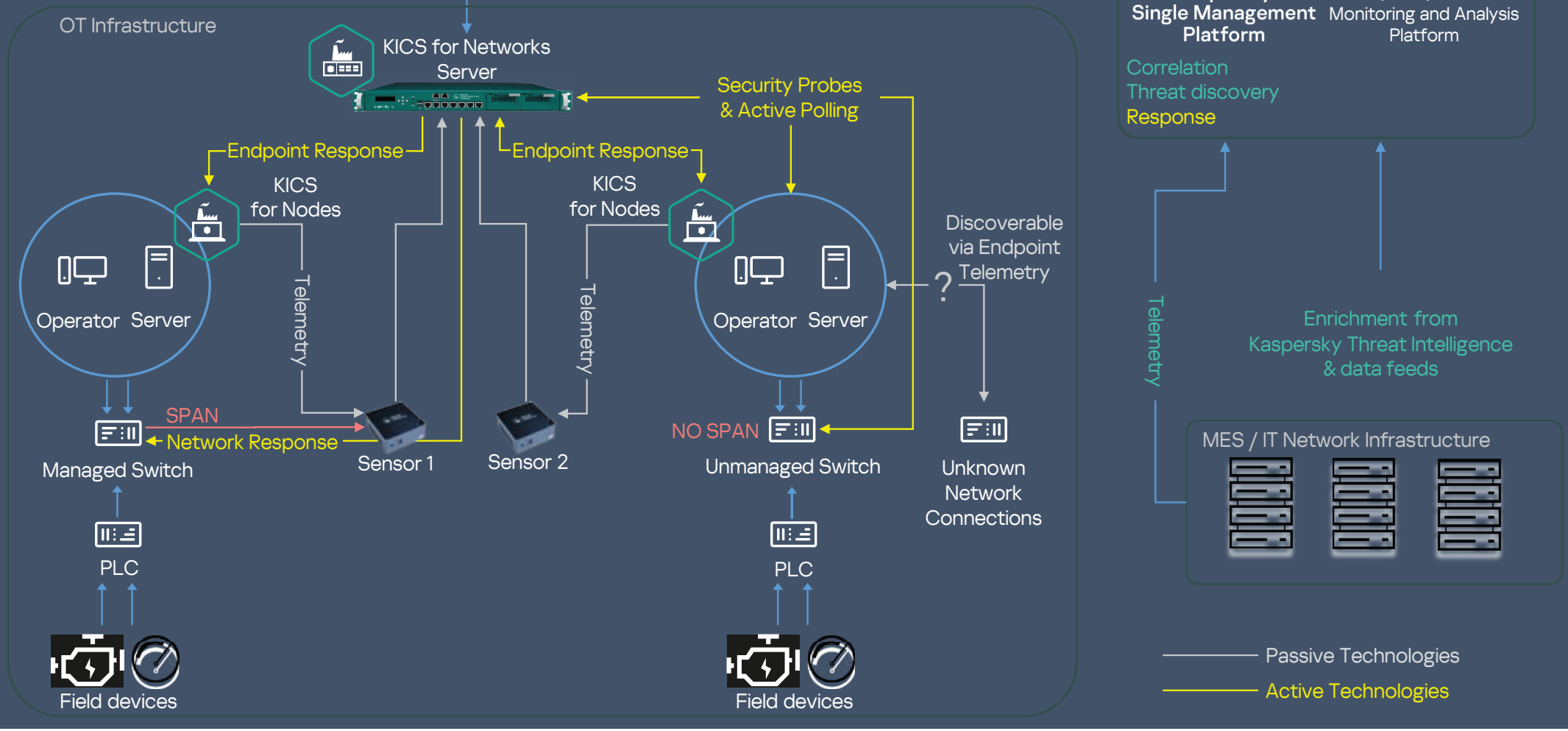


Example of report pages

Kaspersky Industrial CyberSecurity for Networks

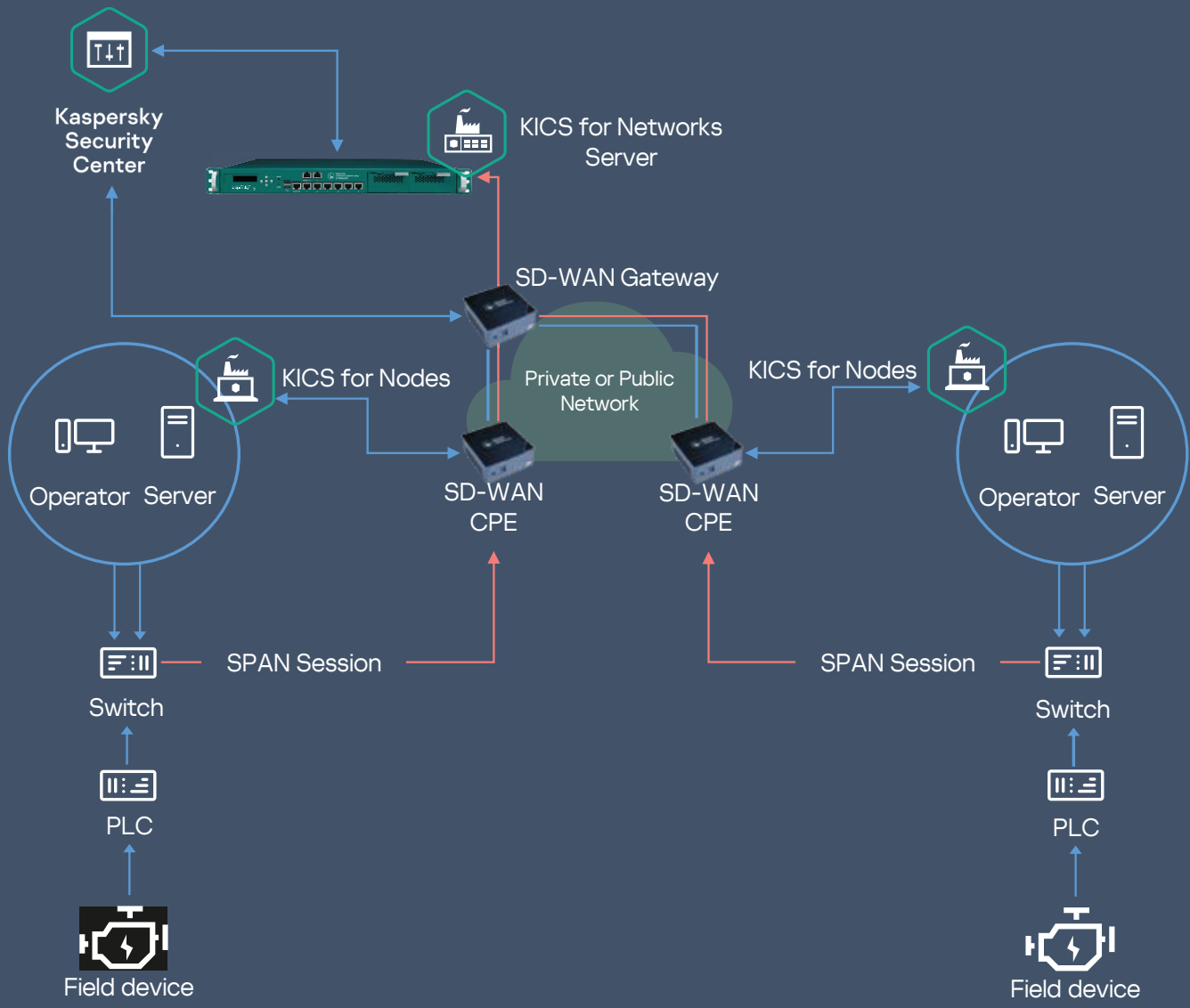
Industrial Network Architectures

Sample Integration & Capability Overview

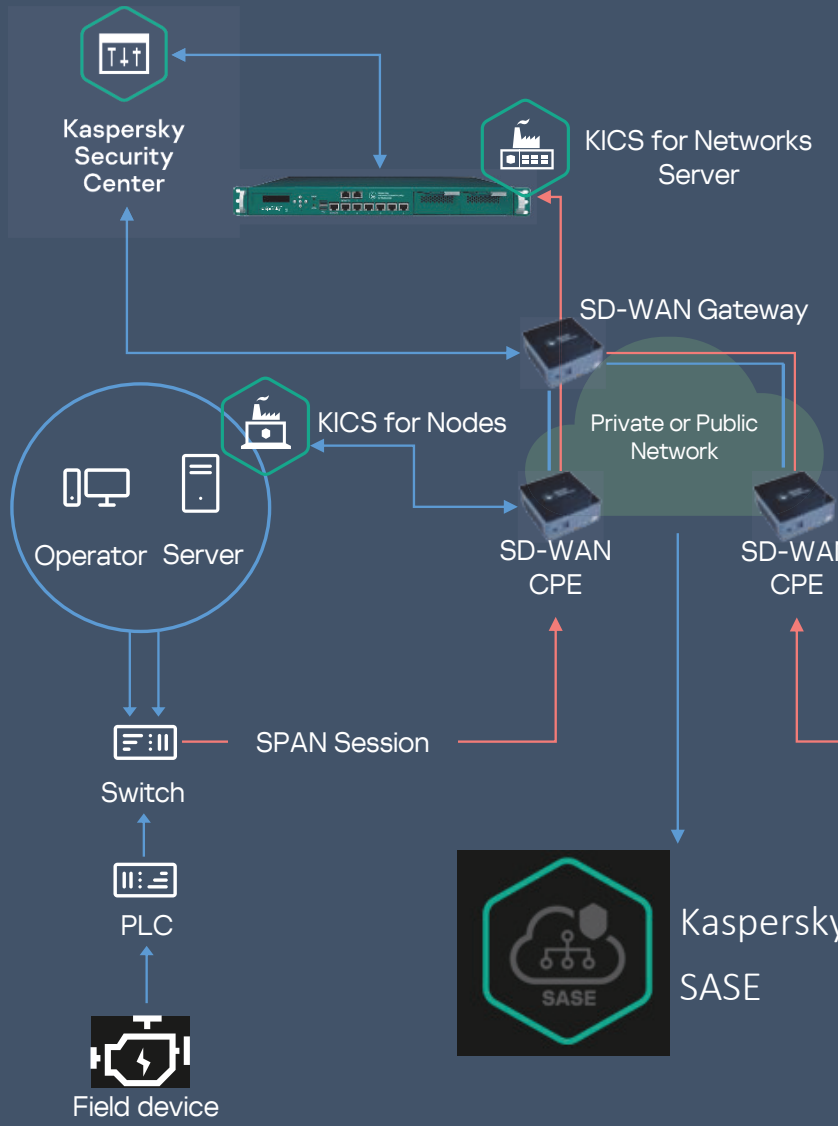


KICS and Kaspersky SD-WAN in distributed infrastructures

- Flexible transport layer for security management in distributed OT infrastructures
- Portable SD-WAN CPE for installation on customer premises
- KICS functions without onsite product installation (remote mirrored traffic provision for KICS for Networks, Active Polling, KICS Integration, KICS for Nodes management and telemetry sharing)
- Data channel segregation / support of independent channels and scenarios
- Multiple network provider access connections for SD-WAN reliability



KICS and Kaspersky SD-WAN in distributed infrastructures



SASE – Secure Access Service Edge

- Cloud Access Security Brokers (CASB)
- Zero Trust Network Access (ZTNA)
- Firewall as a Service (FWaaS)
- Secure Web Gateways (SWG)