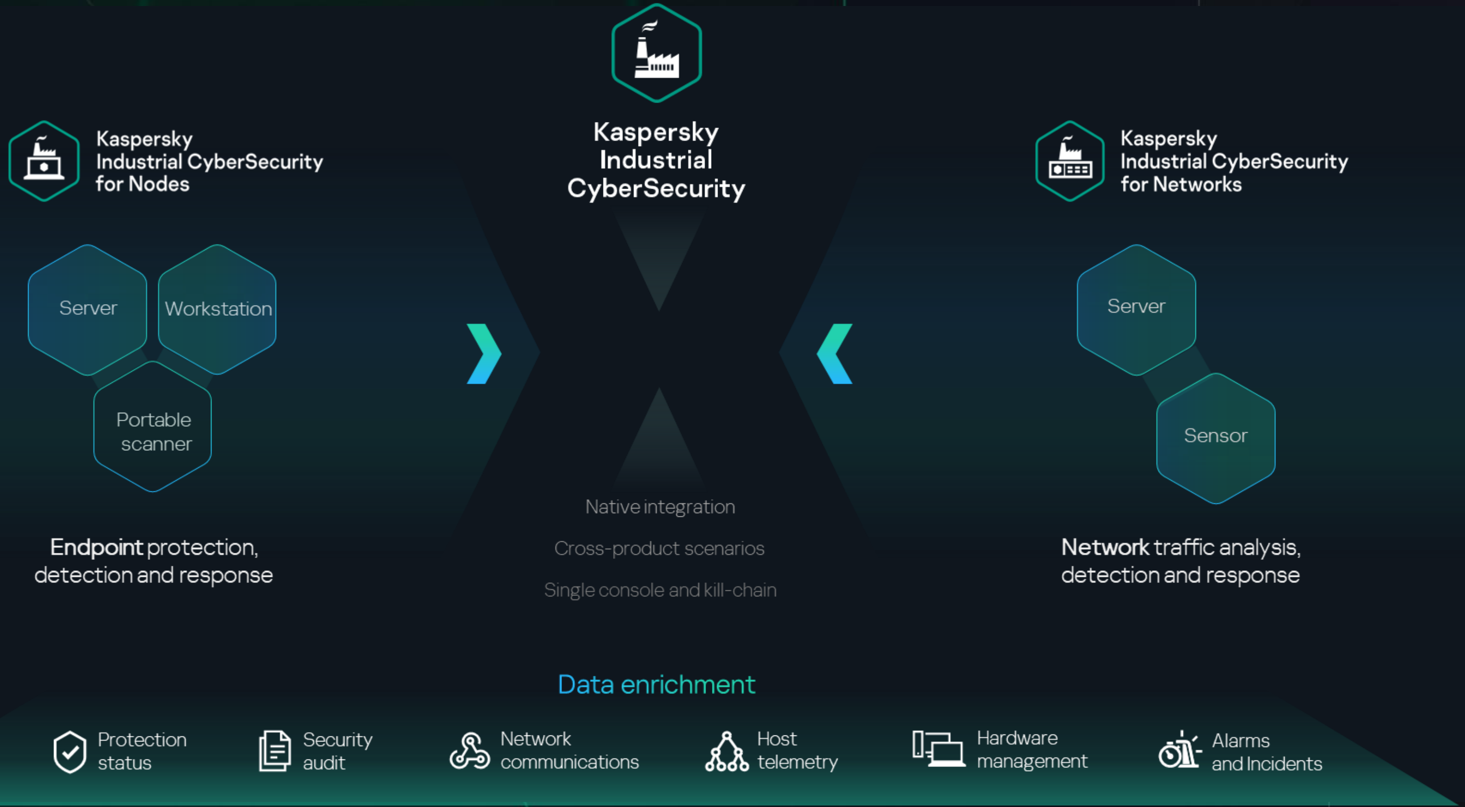
Kaspersky Industrial Cybersecurity Conference 2024

# KICS solution overview – a native XDR platform for critical infrastructure protection

Dmitry Astapov
Senior Product Manager, KICS
Kaspersky

kaspersky

# Kaspersky Industrial CyberSecurity Platform



Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity for Nodes

Server

Workstation

Portable scanner

**Endpoint** protection, detection and response

Native integration

Cross-product scenarios

Single console and kill-chain

Kaspersky Industrial CyberSecurity for Networks

Server

Sensor

**Network** traffic analysis, detection and response

Data enrichment

- Protection status
- Security audit
- Network communications
- Host telemetry
- Hardware management
- Alarms and Incidents

# KICS for Nodes. Endpoint protection options

- Windows
- Portable Scanner
- Linux
- Audit Agent

- Gateway
- Engineering workstation
- Historian server
- System management workstation
- SCADA server
- Embedded systems
- Operation workstation

**Kaspersky Industrial CyberSecurity for Nodes**

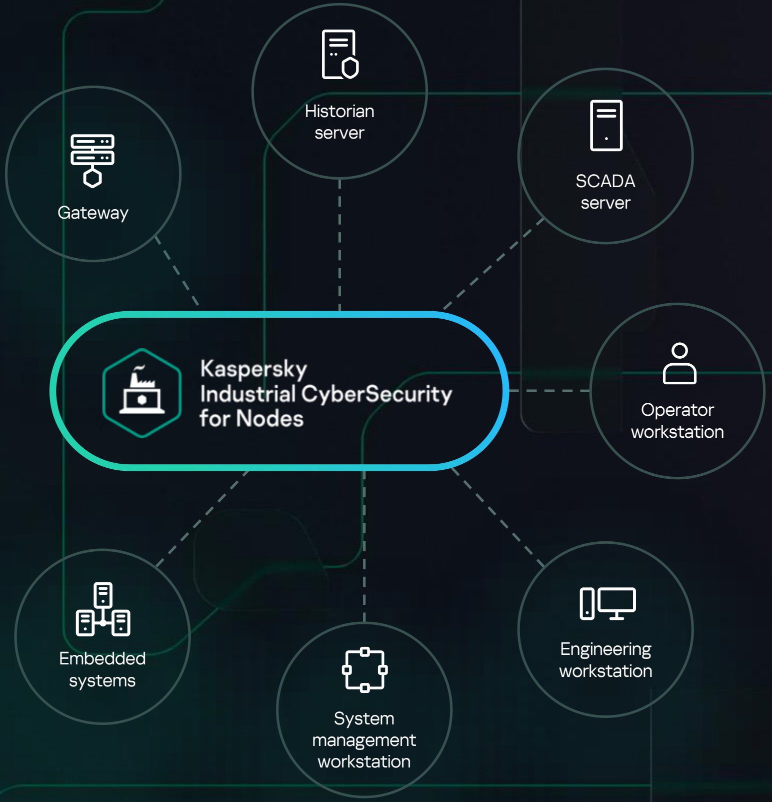
- Compatibility* with Industrial Automation Vendors
- Legacy OS support starting from Windows XP SP2
- Non-blocking (statistic mode) availability
- No reboot on installation, update or upgrade
- Air-gapped database updates
- Components and settings specific for OT
- Modular architecture – component selection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

* Learn more: **certification**

# KICS for Nodes. Endpoint protection components

- Anti-Malware
- Application Launch Control
- Device Control
- File Integrity Control
- PLC Integrity Control*
- Anti-Cryptor
- Exploit Prevention*
- Network Threat Prevention
- Firewall
- Windows Log inspector*
- Windows Registry Monitor*
- Portable Scanner
- Security Audit
- EDR Agent

## Industrial Endpoint Protection



* Windows version only

# KICS for Nodes. Industrial control systems support

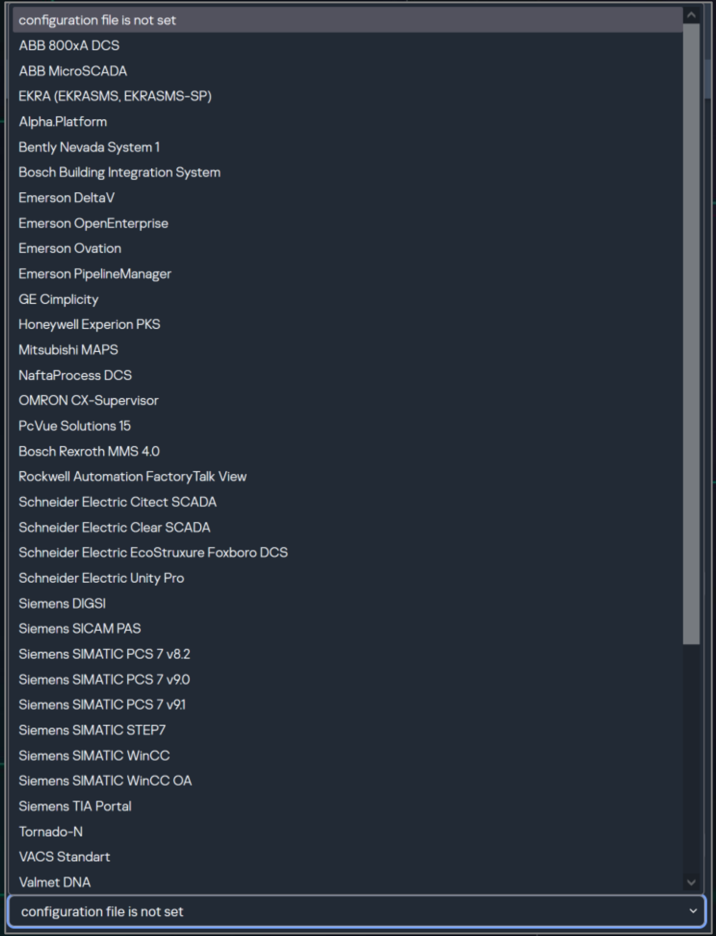
## Verified compatibility with ICS vendors

- Cooperation with industrial automation vendors
- Compatibility and interoperability verification
- Reference architectures

## 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
- ICS vendor guides
- Technical support and issue resolution



configuration file is not set
ABB 800xA DCS
ABB MicroSCADA
EKRA (EKRASMS, EKRASMS-SP)
Alpha.Platform
Bently Nevada System 1
Bosch Building Integration System
Emerson DeltaV
Emerson OpenEnterprise
Emerson Ovation
Emerson PipelineManager
GE Cimplicity
Honeywell Experion PKS
Mitsubishi MAPS
NaftaProcess DCS
OMRON CX-Supervisor
PcVue Solutions 15
Bosch Rexroth MMS 4.0
Rockwell Automation FactoryTalk View
Schneider Electric Citect SCADA
Schneider Electric Clear SCADA
Schneider Electric EcoStruxure Foxboro DCS
Schneider Electric Unity Pro
Siemens DIGSI
Siemens SICAM PAS
Siemens SIMATIC PCS 7 v8.2
Siemens SIMATIC PCS 7 v9.0
Siemens SIMATIC PCS 7 v9.1
Siemens SIMATIC STEP7
Siemens SIMATIC WinCC
Siemens SIMATIC WinCC OA
Siemens TIA Portal
Tornado-N
VACS Standart
Valmet DNA

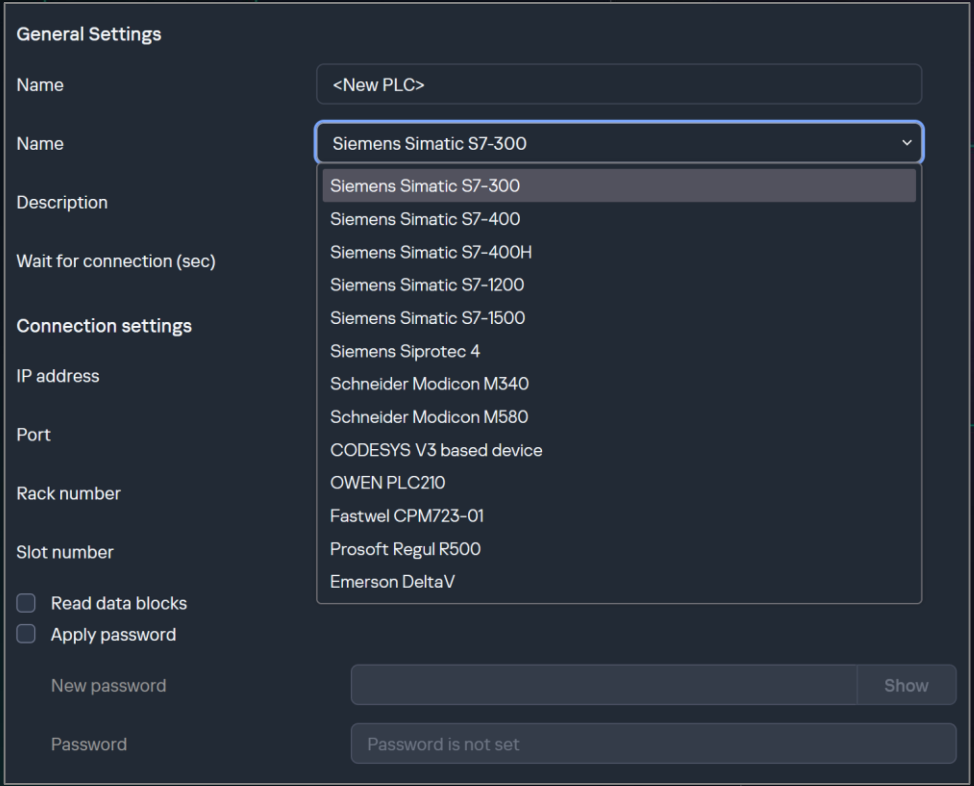
configuration file is not set

# KICS for Nodes. PLC integrity control

Monitoring of actual PLC project, using direct communication with PLC over its native protocol

Step 1. PLC Project Investigation: Upload a project from PLC to use as a benchmark

Step 2. PLC Project Integrity Check: Create a periodical task to check the integrity of downloaded project



**General Settings**

Name: <New PLC>

Name: Siemens Simatic S7-300

- Siemens Simatic S7-300
- Siemens Simatic S7-400
- Siemens Simatic S7-400H
- Siemens Simatic S7-1200
- Siemens Simatic S7-1500
- Siemens Siprotec 4
- Schneider Modicon M340
- Schneider Modicon M580
- CODESYS V3 based device
- OWEN PLC210
- Fastwel CPM723-01
- Prosoft Regul R500
- Emerson DeltaV

Description

Wait for connection (sec)

**Connection settings**

IP address

Port

Rack number

Slot number

☐ Read data blocks

☐ Apply password

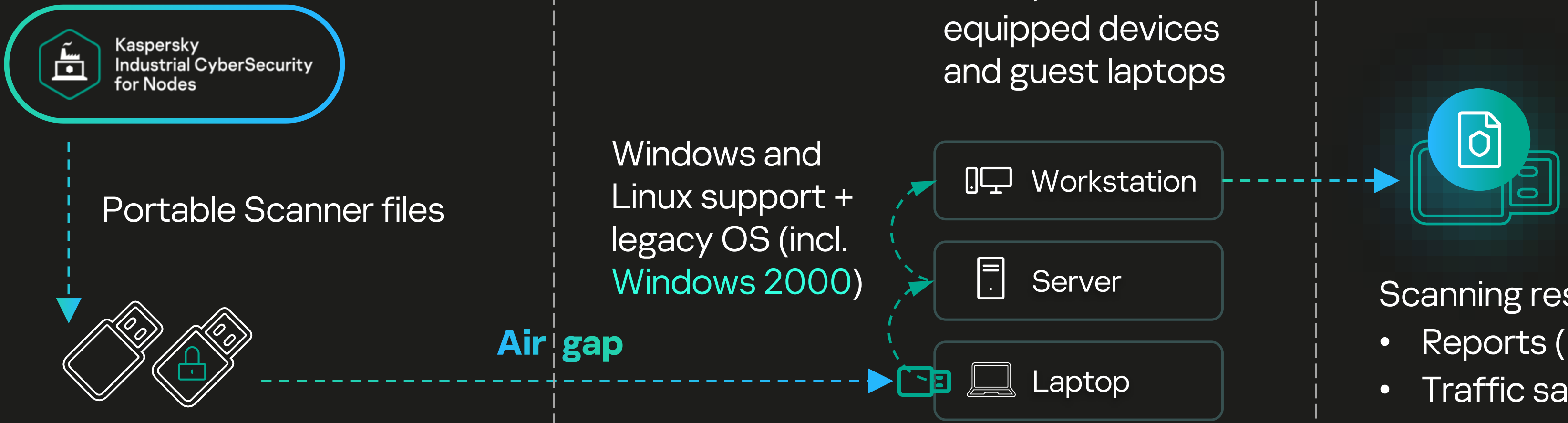
New password

Password: Password is not set

# KICS Portable Scanner update: use cases

IT | OT

Get the host with **KICS for Nodes** installed



Portable Scanner files

Windows and Linux support + legacy OS (incl. Windows 2000)

Define standalone hosts, not EPP-equipped devices and guest laptops

Scanning results:

- Reports (HTML, txt)
- Traffic samples

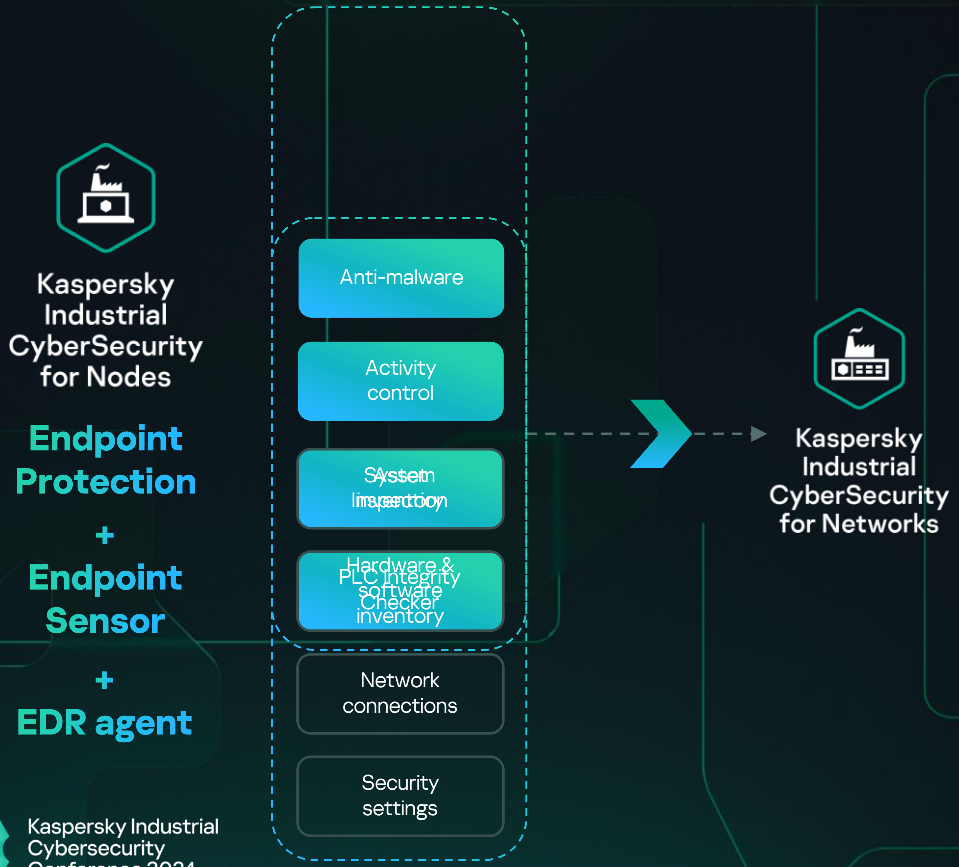
Deploy **Portable Scanner** in required configuration onto:

- Any USB-drive or
- Secure USB-drive with hidden password-protected storage for inventory and report files

Inspect hosts one by one, the results are saved on the drive:

- Host inventory
- Anti-Virus scan
- Vulnerability scan
- Traffic sample capture

# KICS for Nodes. All-in-one endpoint sensor



Kaspersky Industrial CyberSecurity for Nodes

**Endpoint Protection**

**+**

**Endpoint Sensor**

**+**

**EDR agent**

## Endpoint sensor for enhanced asset inventory

- Host attributes (host name, vendor, model, OS and more)
- Network communications
- Hardware and software monitoring
- Security audit for discovering vulnerabilities and misconfigurations

## EDR agent

- Network alert enrichment by accurate host information (processes, users)
- Kill-chain view for root-cause analysis
- Response options

# KICS for Networks as core of KICS Platform

Kaspersky
Industrial CyberSecurity
for Networks

## KICS for Networks

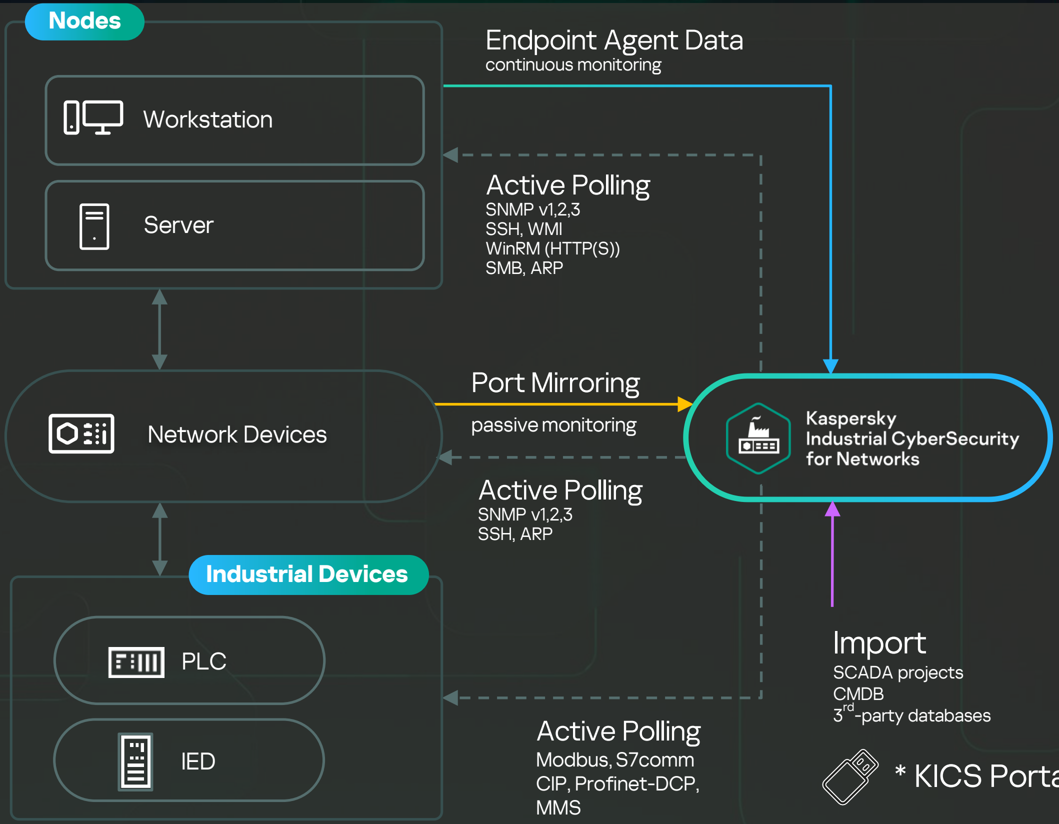
Network monitoring and threat detection for industrial enterprises

Network traffic analysis, detection and response solution

Core of KICS Platform, a single place for data accumulation, management and incident investigation

Multifunctional platform for asset discovery, risk management, security audit, extended detection and response (XDR)

# KICS for Networks. Asset discovery



## Discovery methods

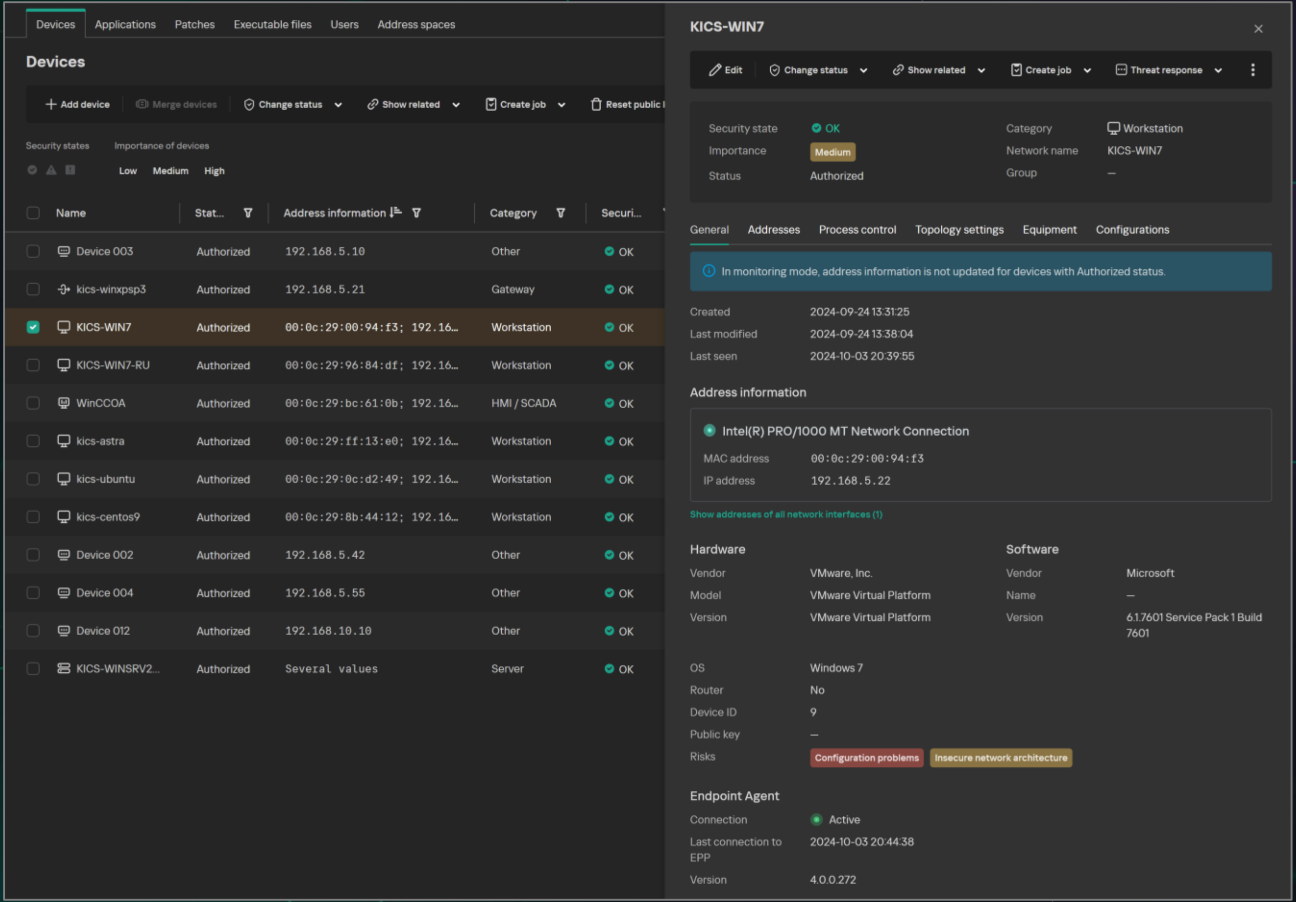
1. Passive Monitoring (SPAN session)
2. Endpoint agent data (SPAN-less)
3. Active polling
4. Import (manual or automated)

* KICS Portable Scanner reports

# Asset discovery results

## Devices: the start of the journey

- Device-centric approach, data, events, network behavior statistics linked to devices
- Device categories, importance, risks are calculated automatically
- Device monitoring, all changes are registered



### Devices

| | Name | Stat... | Address information | Category | Securi... |
|---|---|---|---|---|---|
| □ | Device 003 | Authorized | 192.168.5.10 | Other | OK |
| □ | kics-winxpsp3 | Authorized | 192.168.5.21 | Gateway | OK |
| ☑ | KICS-WIN7 | Authorized | 00:0c:29:00:94:f3; 192.16... | Workstation | OK |
| □ | KICS-WIN7-RU | Authorized | 00:0c:29:96:84:df; 192.16... | Workstation | OK |
| □ | WinCCOA | Authorized | 00:0c:29:bc:61:0b; 192.16... | HMI / SCADA | OK |
| □ | kics-astra | Authorized | 00:0c:29:ff:13:e0; 192.16... | Workstation | OK |
| □ | kics-ubuntu | Authorized | 00:0c:29:0c:d2:49; 192.16... | Workstation | OK |
| □ | kics-centos9 | Authorized | 00:0c:29:8b:44:12; 192.16... | Workstation | OK |
| □ | Device 002 | Authorized | 192.168.5.42 | Other | OK |
| □ | Device 004 | Authorized | 192.168.5.55 | Other | OK |
| □ | Device 012 | Authorized | 192.168.10.10 | Other | OK |
| □ | KICS-WINSRV2... | Authorized | Several values | Server | OK |

### KICS-WIN7

Security state: OK
Importance: Medium
Status: Authorized
Category: Workstation
Network name: KICS-WIN7
Group: —

In monitoring mode, address information is not updated for devices with Authorized status.

Created: 2024-09-24 13:31:25
Last modified: 2024-09-24 13:38:04
Last seen: 2024-10-03 20:39:55

**Address information**

Intel(R) PRO/1000 MT Network Connection
MAC address: 00:0c:29:00:94:f3
IP address: 192.168.5.22

Show addresses of all network interfaces (1)

**Hardware**

Vendor: VMware, Inc.
Model: VMware Virtual Platform
Version: VMware Virtual Platform

**Software**

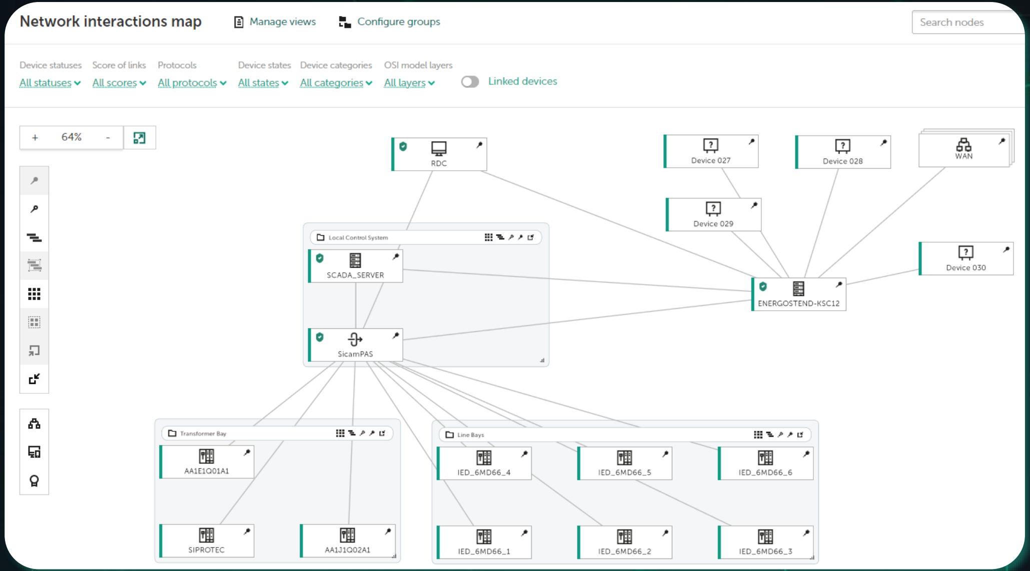
Vendor: Microsoft
Name: —
Version: 6.1.7601 Service Pack 1 Build 7601

OS: Windows 7
Router: No
Device ID: 9
Public key: —
Risks: Configuration problems; Insecure network architecture

**Endpoint Agent**

Connection: Active
Last connection to EPP: 2024-10-03 20:44:38
Version: 4.0.0.272

# KICS for Networks. Network Inventory & visualization

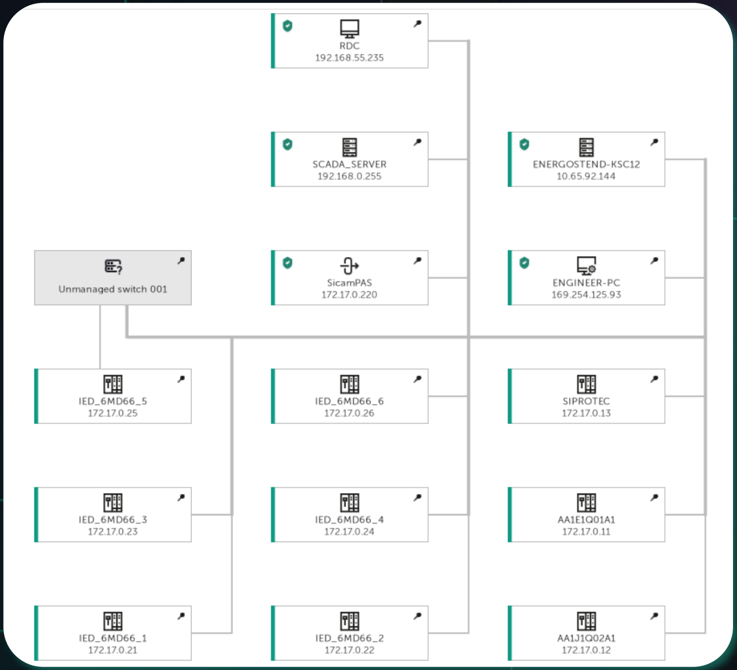


Network interactions map | Manage views | Configure groups | Search nodes

Device statuses: All statuses | Score of links: All scores | Protocols: All protocols | Device states: All states | Device categories: All categories | OSI model layers: All layers | Linked devices

## Network interactions map

- Logical network communication diagram
- Protocols and amount of traffic
- Grouping, search and filtering



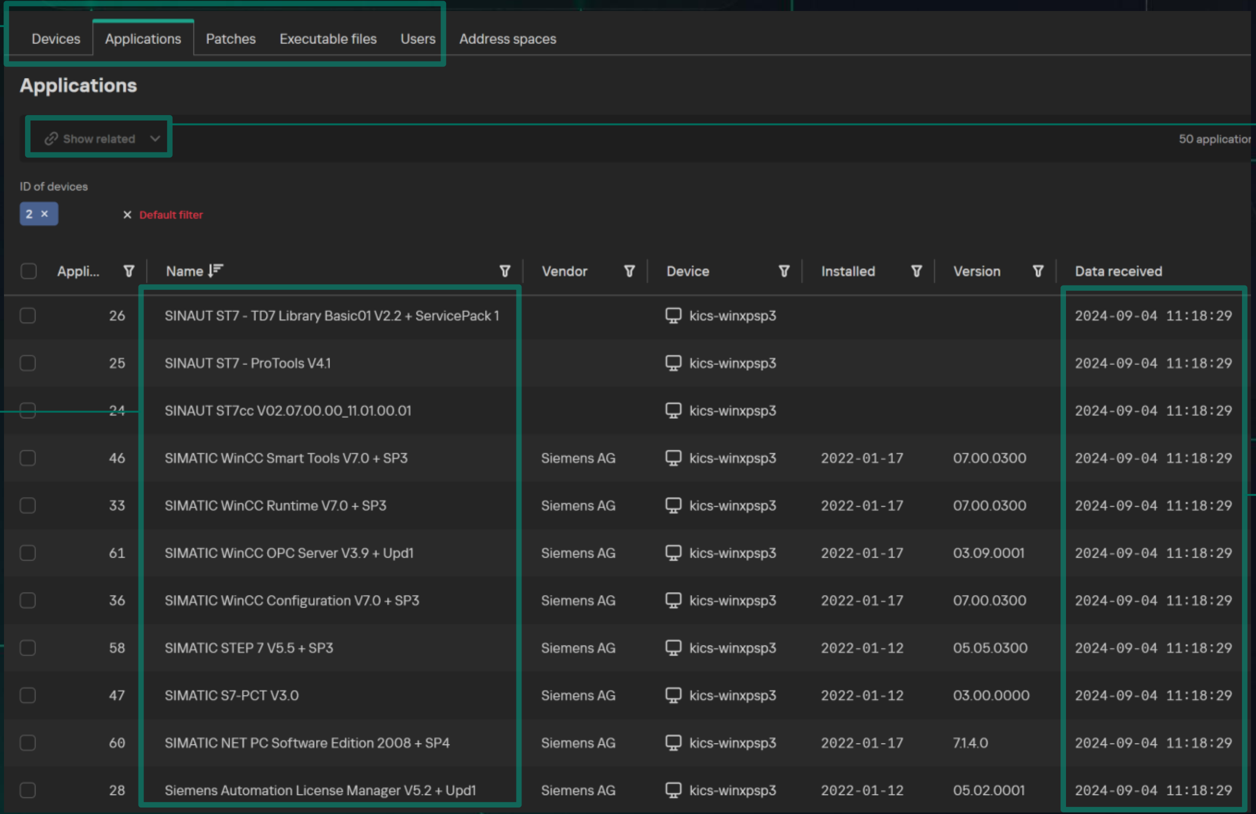
## Network topology diagram

- Physical network connection diagram
- Shows switch port a device is connected to
- Built automatically with network equipment polling

# Software, patches and user accounts inventory

Inventory lists of software, patches, users and executables

Data collected automatically after integration is configured



## Applications

ID of devices

2 ×

× Default filter

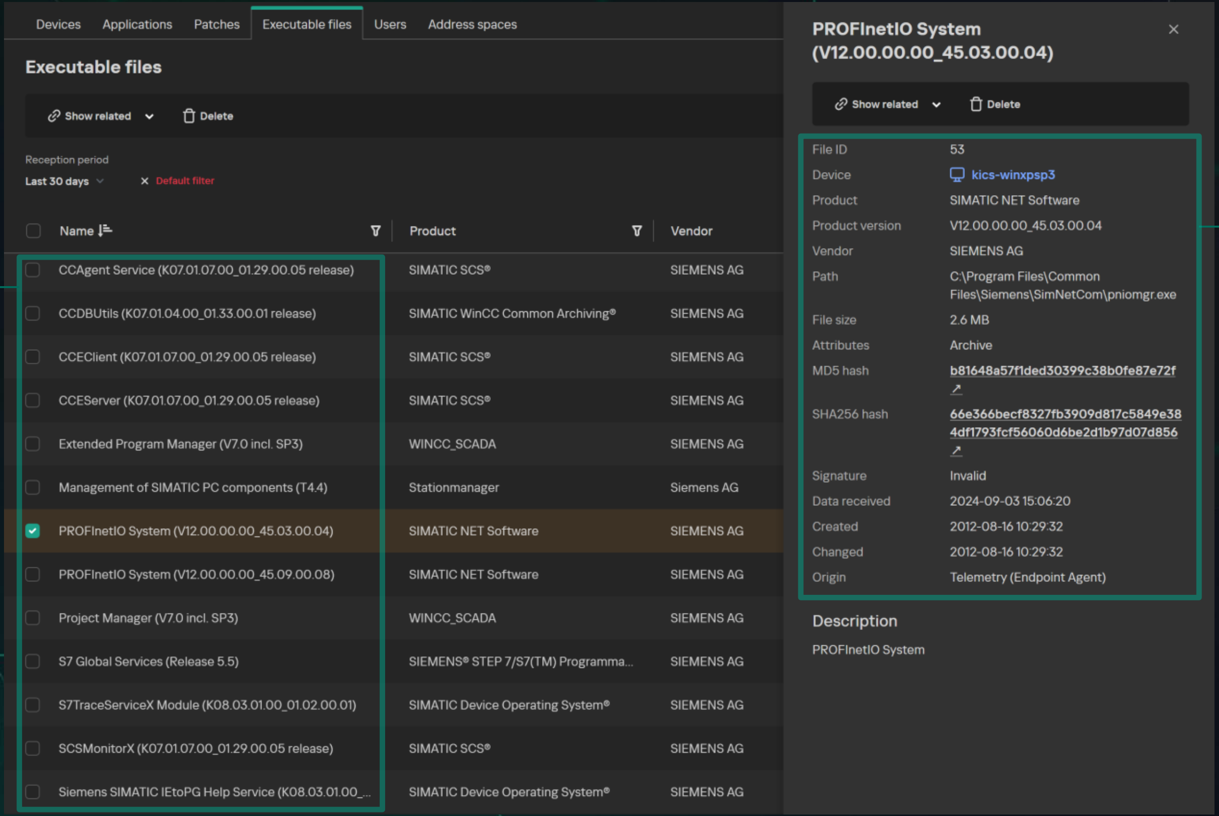
| □ | Appli... | Name | Vendor | Device | Installed | Version | Data received |
|---|---|---|---|---|---|---|---|
| □ | 26 | SINAUT ST7 - TD7 Library Basic01 V2.2 + ServicePack 1 | | kics-winxpsp3 | | | 2024-09-04 11:18:29 |
| □ | 25 | SINAUT ST7 - ProTools V4.1 | | kics-winxpsp3 | | | 2024-09-04 11:18:29 |
| □ | 24 | SINAUT ST7cc V02.07.00.00_11.01.00.01 | | kics-winxpsp3 | | | 2024-09-04 11:18:29 |
| □ | 46 | SIMATIC WinCC Smart Tools V7.0 + SP3 | Siemens AG | kics-winxpsp3 | 2022-01-17 | 07.00.0300 | 2024-09-04 11:18:29 |
| □ | 33 | SIMATIC WinCC Runtime V7.0 + SP3 | Siemens AG | kics-winxpsp3 | 2022-01-17 | 07.00.0300 | 2024-09-04 11:18:29 |
| □ | 61 | SIMATIC WinCC OPC Server V3.9 + Upd1 | Siemens AG | kics-winxpsp3 | 2022-01-17 | 03.09.0001 | 2024-09-04 11:18:29 |
| □ | 36 | SIMATIC WinCC Configuration V7.0 + SP3 | Siemens AG | kics-winxpsp3 | 2022-01-17 | 07.00.0300 | 2024-09-04 11:18:29 |
| □ | 58 | SIMATIC STEP 7 V5.5 + SP3 | Siemens AG | kics-winxpsp3 | 2022-01-12 | 05.05.0300 | 2024-09-04 11:18:29 |
| □ | 47 | SIMATIC S7-PCT V3.0 | Siemens AG | kics-winxpsp3 | 2022-01-12 | 03.00.0000 | 2024-09-04 11:18:29 |
| □ | 60 | SIMATIC NET PC Software Edition 2008 + SP4 | Siemens AG | kics-winxpsp3 | 2022-01-17 | 7.1.4.0 | 2024-09-04 11:18:29 |
| □ | 28 | Siemens Automation License Manager V5.2 + Upd1 | Siemens AG | kics-winxpsp3 | 2022-01-12 | 05.02.0001 | 2024-09-04 11:18:29 |

Quick focus change to devices and events

Basic change management, alerts on new and missing previously known item

# Application/script launches and non-resident software

A catalog with detected recent launches, including scripts, not installed and temporary applications



**Executable files**

Reception period

Last 30 days

× Default filter

| ☐ | Name | Product | Vendor |
|---|---|---|---|
| ☐ | CCAgent Service (K07.01.07.00_01.29.00.05 release) | SIMATIC SCS® | SIEMENS AG |
| ☐ | CCDBUtils (K07.01.04.00_01.33.00.01 release) | SIMATIC WinCC Common Archiving® | SIEMENS AG |
| ☐ | CCEClient (K07.01.07.00_01.29.00.05 release) | SIMATIC SCS® | SIEMENS AG |
| ☐ | CCEServer (K07.01.07.00_01.29.00.05 release) | SIMATIC SCS® | SIEMENS AG |
| ☐ | Extended Program Manager (V7.0 incl. SP3) | WINCC_SCADA | SIEMENS AG |
| ☐ | Management of SIMATIC PC components (T4.4) | Stationmanager | Siemens AG |
| ☑ | PROFInetIO System (V12.00.00.00_45.03.00.04) | SIMATIC NET Software | SIEMENS AG |
| ☐ | PROFInetIO System (V12.00.00.00_45.09.00.08) | SIMATIC NET Software | SIEMENS AG |
| ☐ | Project Manager (V7.0 incl. SP3) | WINCC_SCADA | SIEMENS AG |
| ☐ | S7 Global Services (Release 5.5) | SIEMENS® STEP 7/S7(TM) Programma... | SIEMENS AG |
| ☐ | S7TraceServiceX Module (K08.03.01.00_01.02.00.01) | SIMATIC Device Operating System® | SIEMENS AG |
| ☐ | SCSMonitorX (K07.01.07.00_01.29.00.05 release) | SIMATIC SCS® | SIEMENS AG |
| ☐ | Siemens SIMATIC IEtoPG Help Service (K08.03.01.00_... | SIMATIC Device Operating System® | SIEMENS AG |

**PROFInetIO System (V12.00.00.00_45.03.00.04)**

| | |
|---|---|
| File ID | 53 |
| Device | kics-winxpsp3 |
| Product | SIMATIC NET Software |
| Product version | V12.00.00.00_45.03.00.04 |
| Vendor | SIEMENS AG |
| Path | C:\Program Files\Common Files\Siemens\SimNetCom\pniomgr.exe |
| File size | 2.6 MB |
| Attributes | Archive |
| MD5 hash | b81648a57f1ded30399c38b0fe87e72f ↗ |
| SHA256 hash | 66e366becf8327fb3909d817c5849e384df1793fcf56060d6be2d1b97d07d856 ↗ |
| Signature | Invalid |
| Data received | 2024-09-03 15:06:20 |
| Created | 2012-08-16 10:29:32 |
| Changed | 2012-08-16 10:29:32 |
| Origin | Telemetry (Endpoint Agent) |

**Description**

PROFInetIO System

Key details to locate file on host, check file reputation using Kaspersky TIP or perform a response action

# Security Audit

It ensures the secure configuration of assets and monitors any changes for potential security risks and compliance issues

KICS Platform has an internal subsystem to extract more security state data and identify risks and misconfigurations

**Active polling**

Basic inventory and risk detection technology

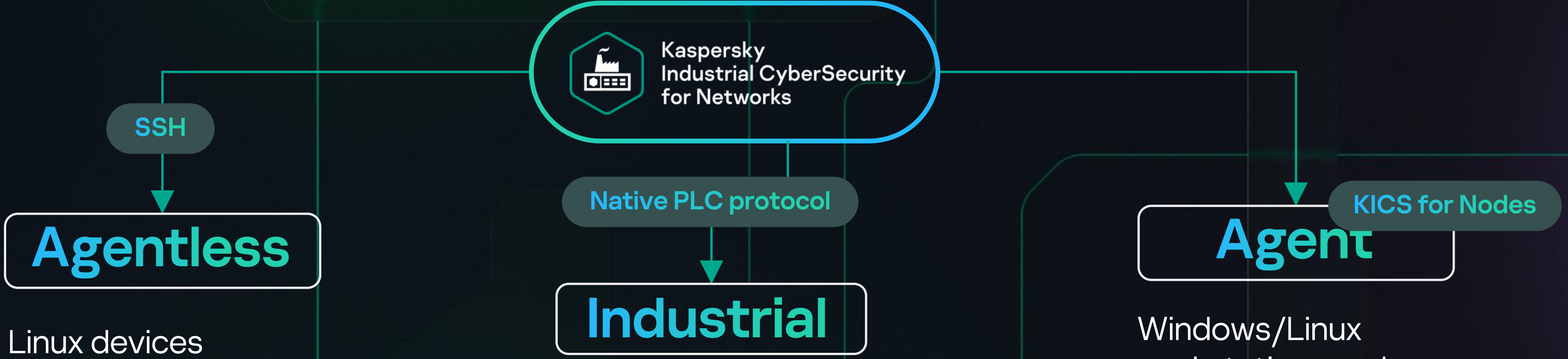
**Vulnerability and compliance monitoring**

Vulnerability search and compliance checks against pre-defined policy

**Configuration control**

Change management and security settings monitoring

# Security Audit: what we poll



Kaspersky Industrial CyberSecurity for Networks

SSH

## Agentless

Native PLC protocol

## Industrial

KICS for Nodes

## Agent

Linux devices
Cisco IOS devices
Siemens Scalance
Moxa PT-series

Security settings, users, ARP tables, executable processes, running config, start-up config, routing tables, and more

Siemens SIMATIC S7-300/400
Schneider Electric M340/580
Allen-Bradley ControlLogix*
Emerson DeltaV*

- Operation mode
- Detailed I/O subsystem info
- Extended downloaded project info (control blocks and hashes)
- CPU event log

Windows/Linux workstations and servers:

- Security settings and policies
- Applications and patches
- Users and groups
- Services
- Drivers
- Scheduled tasks
- Shared folders
- Startup objects

* — by the end of 2024

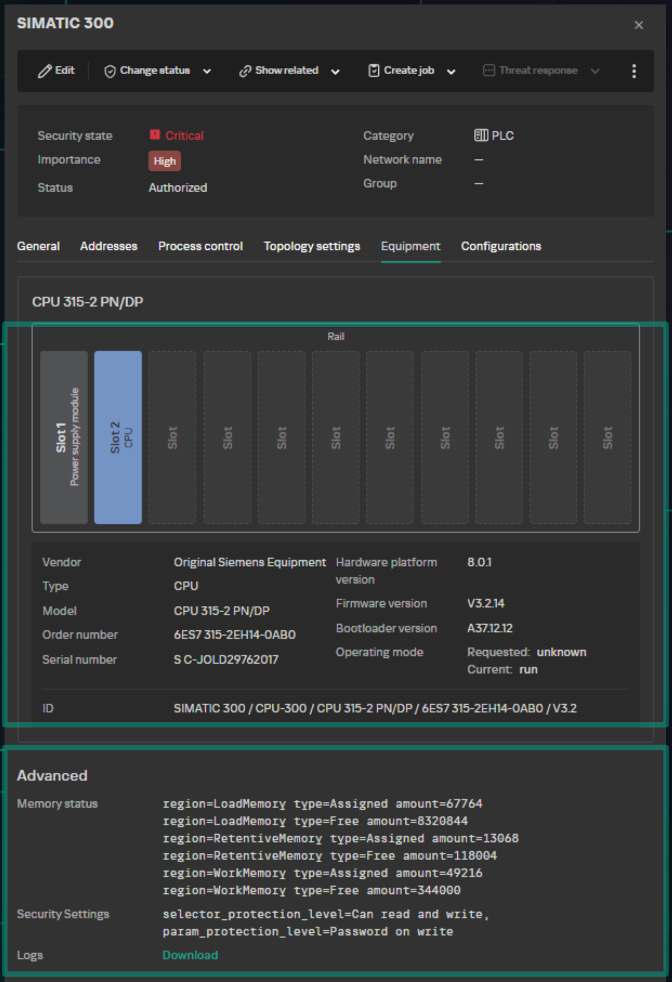
# Security Audit. PLC active polling

## Rack & slots

I/O subsystem information with extra details for each card

## Security settings

Available security parameters, memory status and CPU logs



SIMATIC 300

| | | | |
|---|---|---|---|
| Security state | Critical | Category | PLC |
| Importance | High | Network name | — |
| Status | Authorized | Group | — |

CPU 315-2 PN/DP

| | | | |
|---|---|---|---|
| Vendor | Original Siemens Equipment | Hardware platform version | 8.0.1 |
| Type | CPU | Firmware version | V3.2.14 |
| Model | CPU 315-2 PN/DP | Bootloader version | A37.12.12 |
| Order number | 6ES7 315-2EH14-0AB0 | Operating mode | Requested: unknown<br>Current: run |
| Serial number | S C-JOLD29762017 | | |
| ID | SIMATIC 300 / CPU-300 / CPU 315-2 PN/DP / 6ES7 315-2EH14-0AB0 / V3.2 | | |

Advanced

Memory status

```
region=LoadMemory type=Assigned amount=67764
region=LoadMemory type=Free amount=8320844
region=RetentiveMemory type=Assigned amount=13068
region=RetentiveMemory type=Free amount=118004
region=WorkMemory type=Assigned amount=49216
region=WorkMemory type=Free amount=344000
```

Security Settings

```
selector_protection_level=Can read and write,
param_protection_level=Password on write
```

Logs Download

# Security Audit. Vulnerability and compliance

## List of vulnerabilities

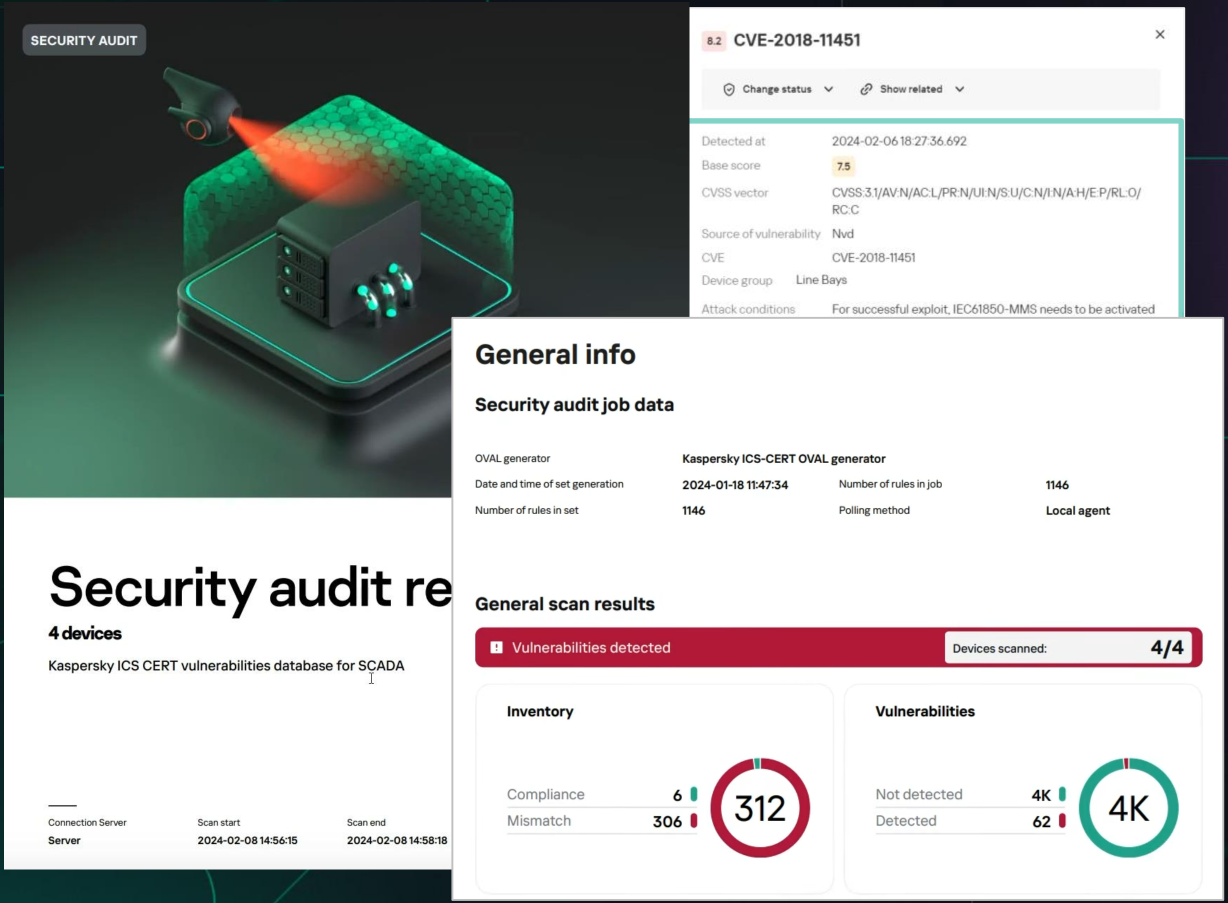
Firmware and software vulnerabilities

## Description

Conditions, mitigations, reference links

## Compliance reports

Conditions, mitigations, reference links



# Security audit re

**4 devices**

Kaspersky ICS CERT vulnerabilities database for SCADA

| Connection Server | Scan start | Scan end |
|---|---|---|
| Server | 2024-02-08 14:56:15 | 2024-02-08 14:58:18 |

8.2 **CVE-2018-11451**

| | |
|---|---|
| Detected at | 2024-02-06 18:27:36.692 |
| Base score | 7.5 |
| CVSS vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| Source of vulnerability | Nvd |
| CVE | CVE-2018-11451 |
| Device group | Line Bays |
| Attack conditions | For successful exploit, IEC61850-MMS needs to be activated |

## General info

### Security audit job data

| | | | |
|---|---|---|---|
| OVAL generator | Kaspersky ICS-CERT OVAL generator | | |
| Date and time of set generation | 2024-01-18 11:47:34 | Number of rules in job | 1146 |
| Number of rules in set | 1146 | Polling method | Local agent |

### General scan results

Vulnerabilities detected — Devices scanned: 4/4

**Inventory**

| | |
|---|---|
| Compliance | 6 |
| Mismatch | 306 |

312

**Vulnerabilities**

| | |
|---|---|
| Not detected | 4K |
| Detected | 62 |

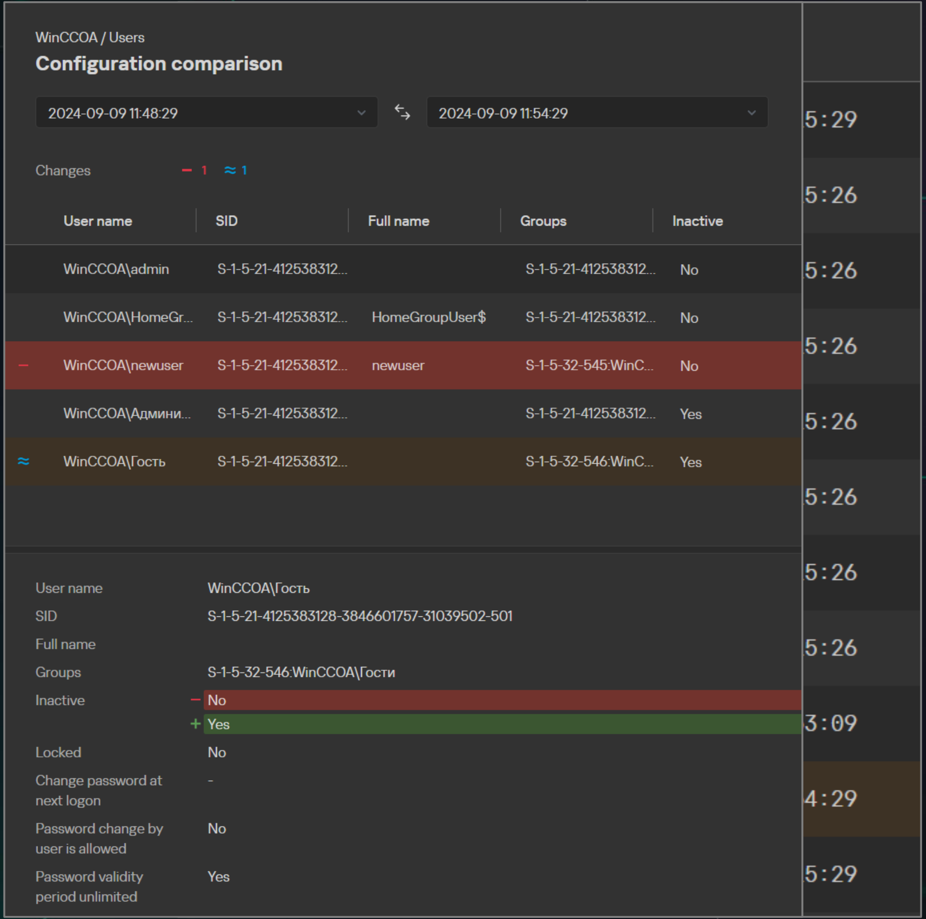
4K

Kaspersky Industrial
Cybersecurity
Conference 2024

# Configuration Control: what we see

Each configuration template has its own view – text listing, list or table, depending on content

The diff is shown as changes in lines, highlighting the new and missing lines



WinCCOA / Users

## Configuration comparison

2024-09-09 11:48:29 ⇆ 2024-09-09 11:54:29

Changes − 1 ≈ 1

| | User name | SID | Full name | Groups | Inactive |
|---|---|---|---|---|---|
| | WinCCOA\admin | S-1-5-21-412538312... | | S-1-5-21-412538312... | No |
| | WinCCOA\HomeGr... | S-1-5-21-412538312... | HomeGroupUser$ | S-1-5-21-412538312... | No |
| − | WinCCOA\newuser | S-1-5-21-412538312... | newuser | S-1-5-32-545:WinC... | No |
| | WinCCOA\Админи... | S-1-5-21-412538312... | | S-1-5-21-412538312... | Yes |
| ≈ | WinCCOA\Гость | S-1-5-21-412538312... | | S-1-5-32-546:WinC... | Yes |

User name WinCCOA\Гость

SID S-1-5-21-4125383128-3846601757-31039502-501

Full name

Groups S-1-5-32-546:WinCCOA\Гости

Inactive − No
+ Yes

Locked No

Change password at next logon -

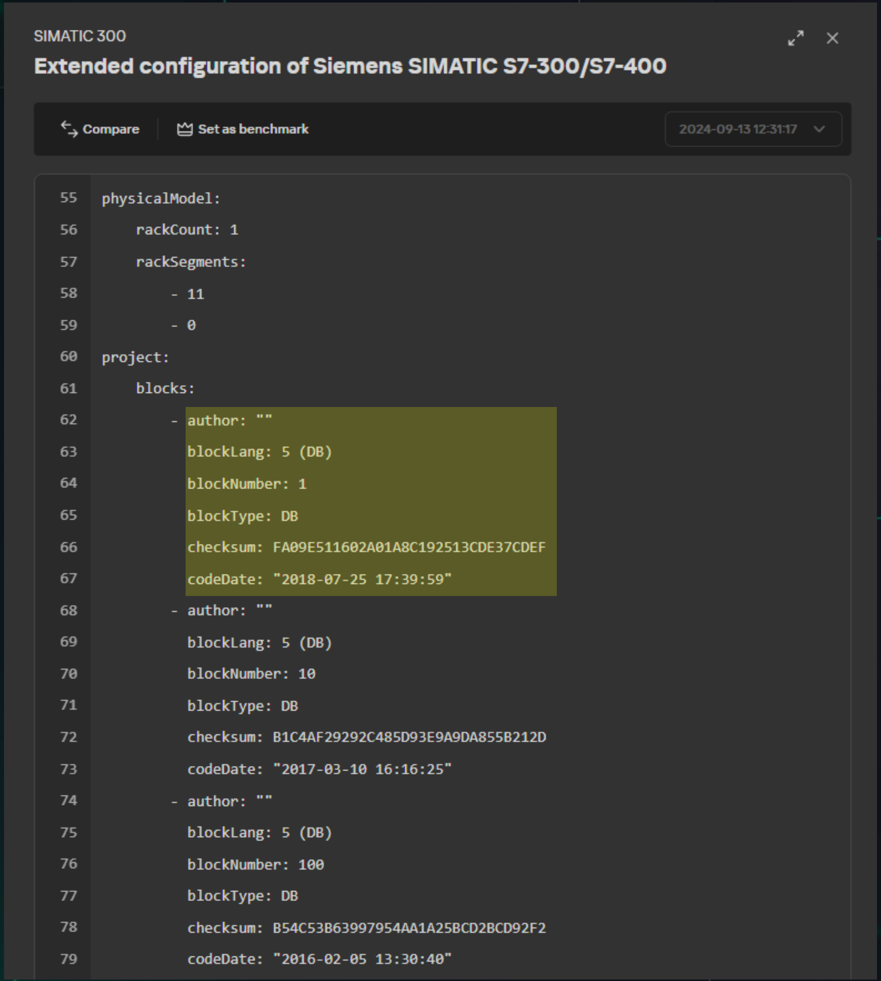
Password change by user is allowed No

Password validity period unlimited Yes

Kaspersky Industrial Cybersecurity Conference 2024

# Configuration Control: PLC configuration

**PLC configuration** is a combination of hardware and software attributes, security settings and current project



**Extended configuration of Siemens SIMATIC S7-300/S7-400**

```
physicalModel:
    rackCount: 1
    rackSegments:
        - 11
        - 0
project:
    blocks:
        - author: ""
          blockLang: 5 (DB)
          blockNumber: 1
          blockType: DB
          checksum: FA09E511602A01A8C192513CDE37CDEF
          codeDate: "2018-07-25 17:39:59"
        - author: ""
          blockLang: 5 (DB)
          blockNumber: 10
          blockType: DB
          checksum: B1C4AF29292C485D93E9A9DA855B212D
          codeDate: "2017-03-10 16:16:25"
        - author: ""
          blockLang: 5 (DB)
          blockNumber: 100
          blockType: DB
          checksum: B54C53B63997954AA1A25BCD2BCD92F2
          codeDate: "2016-02-05 13:30:40"
```

# Detection and response

### Detection technologies

IDS, deep packet inspection, brute force and scan detectors, SIGMA, and more

### Event correlation

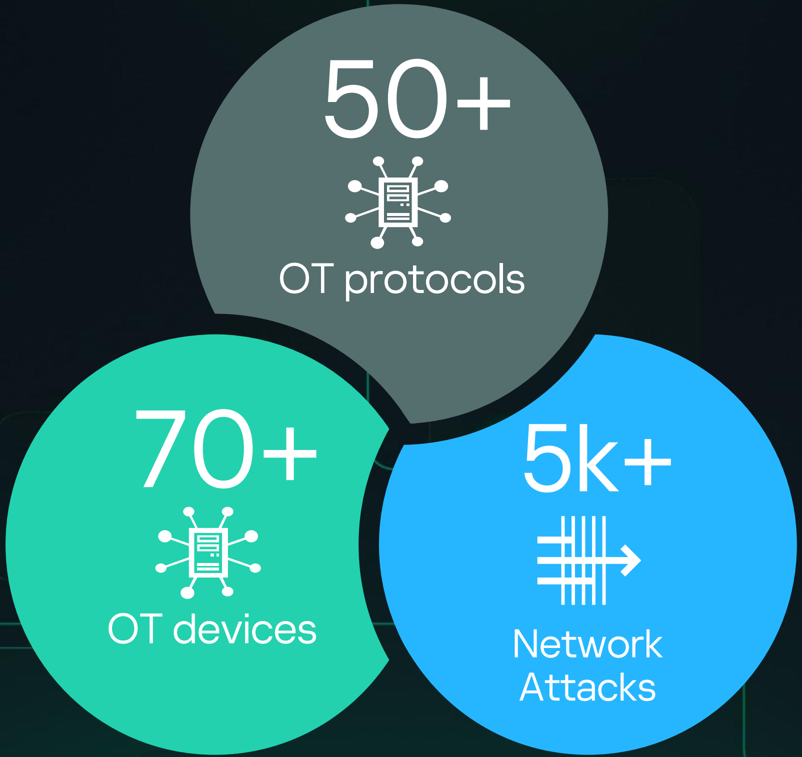
Network and host security event enrichment and correlation to identify incidents

### Investigation graph and responses

Graph with kill-chain view for root-cause analysis, response options

# Support for Industrial devices and protocols

Kaspersky ICS CERT



50+ OT protocols

70+ OT devices

5k+ Network Attacks

## Regular updates

- Asset discovery rules
- Intrusion detection rules
- Vulnerability databases
- Compliance audit rules
- Event correlation rules

## Deep packet inspection for OT and IT protocols

- Command control
- PLC project modification monitoring
- Automatic tags detection and process control rules

# Threat and anomaly detection

## Event correlation

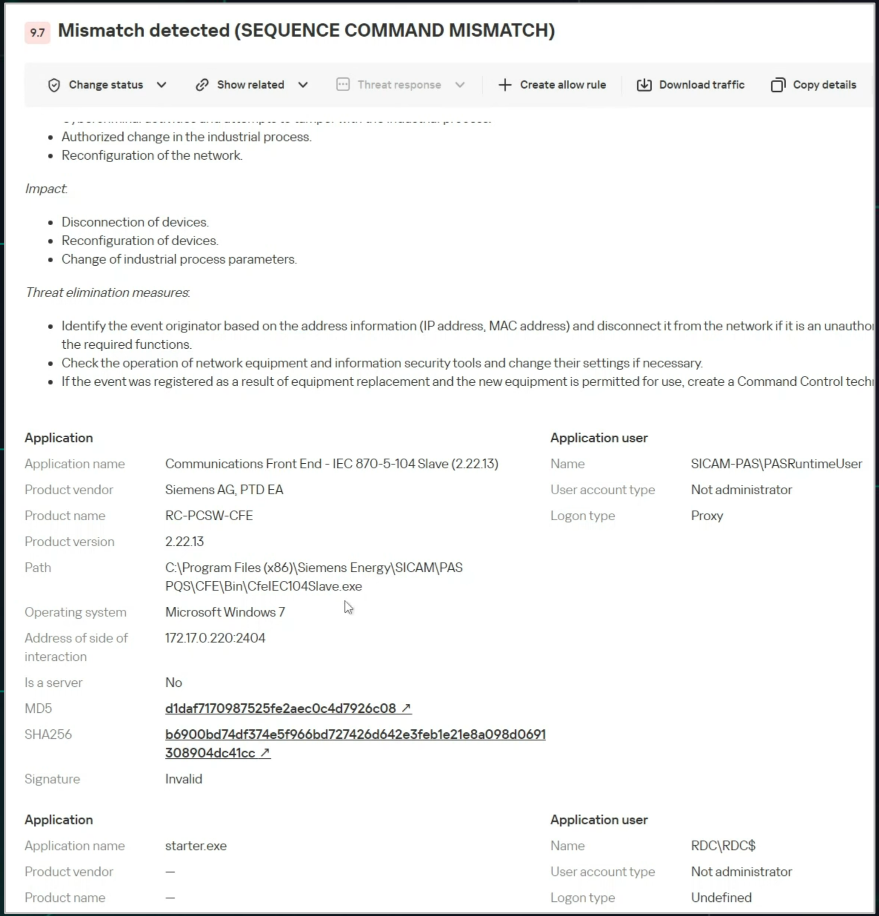
Host and network sourced events

## Industrial DPI events

Device manipulation commands and abnormal process values

## Description

Data enrichment, possible causes, mitigation advice and MITRE mapping



9.7 **Mismatch detected (SEQUENCE COMMAND MISMATCH)**

- Cybercriminal activities and attempts to tamper with the industrial process.
- Authorized change in the industrial process.
- Reconfiguration of the network.

*Impact:*

- Disconnection of devices.
- Reconfiguration of devices.
- Change of industrial process parameters.

*Threat elimination measures:*

- Identify the event originator based on the address information (IP address, MAC address) and disconnect it from the network if it is an unautho the required functions.
- Check the operation of network equipment and information security tools and change their settings if necessary.
- If the event was registered as a result of equipment replacement and the new equipment is permitted for use, create a Command Control tech

| Application | |
|---|---|
| Application name | Communications Front End - IEC 870-5-104 Slave (2.22.13) |
| Product vendor | Siemens AG, PTD EA |
| Product name | RC-PCSW-CFE |
| Product version | 2.22.13 |
| Path | C:\Program Files (x86)\Siemens Energy\SICAM\PAS PQS\CFE\Bin\CfeIEC104Slave.exe |
| Operating system | Microsoft Windows 7 |
| Address of side of interaction | 172.17.0.220:2404 |
| Is a server | No |
| MD5 | d1daf7170987525fe2aec0c4d7926c08 ↗ |
| SHA256 | b6900bd74df374e5f966bd727426d642e3feb1e21e8a098d0691308904dc41cc ↗ |
| Signature | Invalid |

| Application user | |
|---|---|
| Name | SICAM-PAS\PASRuntimeUser |
| User account type | Not administrator |
| Logon type | Proxy |

| Application | |
|---|---|
| Application name | starter.exe |
| Product vendor | — |
| Product name | — |

| Application user | |
|---|---|
| Name | RDC\RDC$ |
| User account type | Not administrator |
| Logon type | Undefined |

Kaspersky Industrial Cybersecurity Conference 2024

# Kill-chain and responses

## Response options

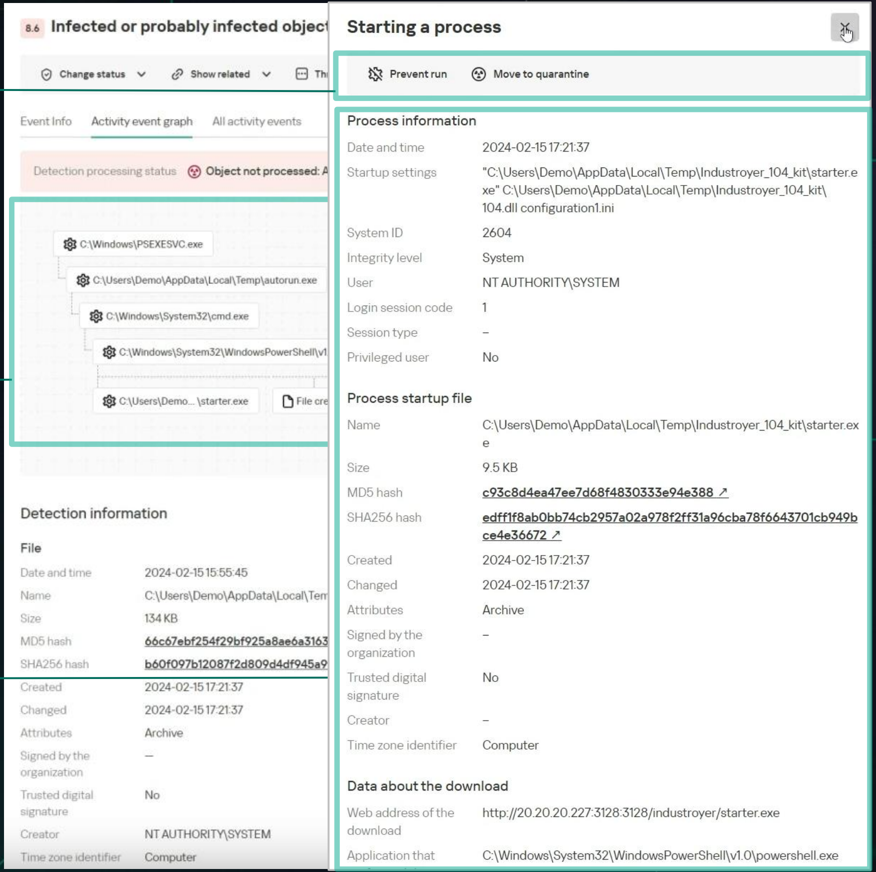
React precisely to file or process

## Kill-chain view

Attack path from very beginning to first detection alert

## Detection info

Extended telemetry details



8.6
Change status
Show related
Th
Event Info
Activity event graph
All activity events
C:\Windows\PSEXESVC.exe
C:\Users\Demo\AppData\Local\Temp\autorun.exe
C:\Windows\System32\cmd.exe
C:\Windows\System32\WindowsPowerShell\v1
C:\Users\Demo... \starter.exe
File cre
Prevent run
Move to quarantine

### Infected or probably infected object

Detection processing status: Object not processed: A

#### Detection information

**File**

| | |
|---|---|
| Date and time | 2024-02-15 15:55:45 |
| Name | C:\Users\Demo\AppData\Local\Tem |
| Size | 134 KB |
| MD5 hash | 66c67ebf254f29bf925a8ae6a3163 |
| SHA256 hash | b60f097b12087f2d809d4df945a9 |
| Created | 2024-02-15 17:21:37 |
| Changed | 2024-02-15 17:21:37 |
| Attributes | Archive |
| Signed by the organization | – |
| Trusted digital signature | No |
| Creator | NT AUTHORITY\SYSTEM |
| Time zone identifier | Computer |

### Starting a process

#### Process information

| | |
|---|---|
| Date and time | 2024-02-15 17:21:37 |
| Startup settings | "C:\Users\Demo\AppData\Local\Temp\Industroyer_104_kit\starter.exe" C:\Users\Demo\AppData\Local\Temp\Industroyer_104_kit\104.dll configuration1.ini |
| System ID | 2604 |
| Integrity level | System |
| User | NT AUTHORITY\SYSTEM |
| Login session code | 1 |
| Session type | – |
| Privileged user | No |

#### Process startup file

| | |
|---|---|
| Name | C:\Users\Demo\AppData\Local\Temp\Industroyer_104_kit\starter.exe |
| Size | 9.5 KB |
| MD5 hash | c93c8d4ea47ee7d68f4830333e94e388 ↗ |
| SHA256 hash | edff1f8ab0bb74cb2957a02a978f2ff31a96cba78f6643701cb949bce4e36672 ↗ |
| Created | 2024-02-15 17:21:37 |
| Changed | 2024-02-15 17:21:37 |
| Attributes | Archive |
| Signed by the organization | – |
| Trusted digital signature | No |
| Creator | – |
| Time zone identifier | Computer |

#### Data about the download

| | |
|---|---|
| Web address of the download | http://20.20.20.227:3128:3128/industroyer/starter.exe |
| Application that | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe |

Kaspersky Industrial
Cybersecurity
Conference 2024

# SIGMA rules support

Sigma

SIEM Detection Format

**SIGMA** is an open and platform-independent standard for describing rules for detecting malicious or suspicious behavior in various logs.

“Sigma is for log files what Snort is for network traffic and YARA is for files.”

We position this technology as an **open, extensible markup language** to search anomalies on endpoints

Detection of suspicious activities, avoiding implementation of resource-intensive technologies of behavioral analysis

**Rule collections:**

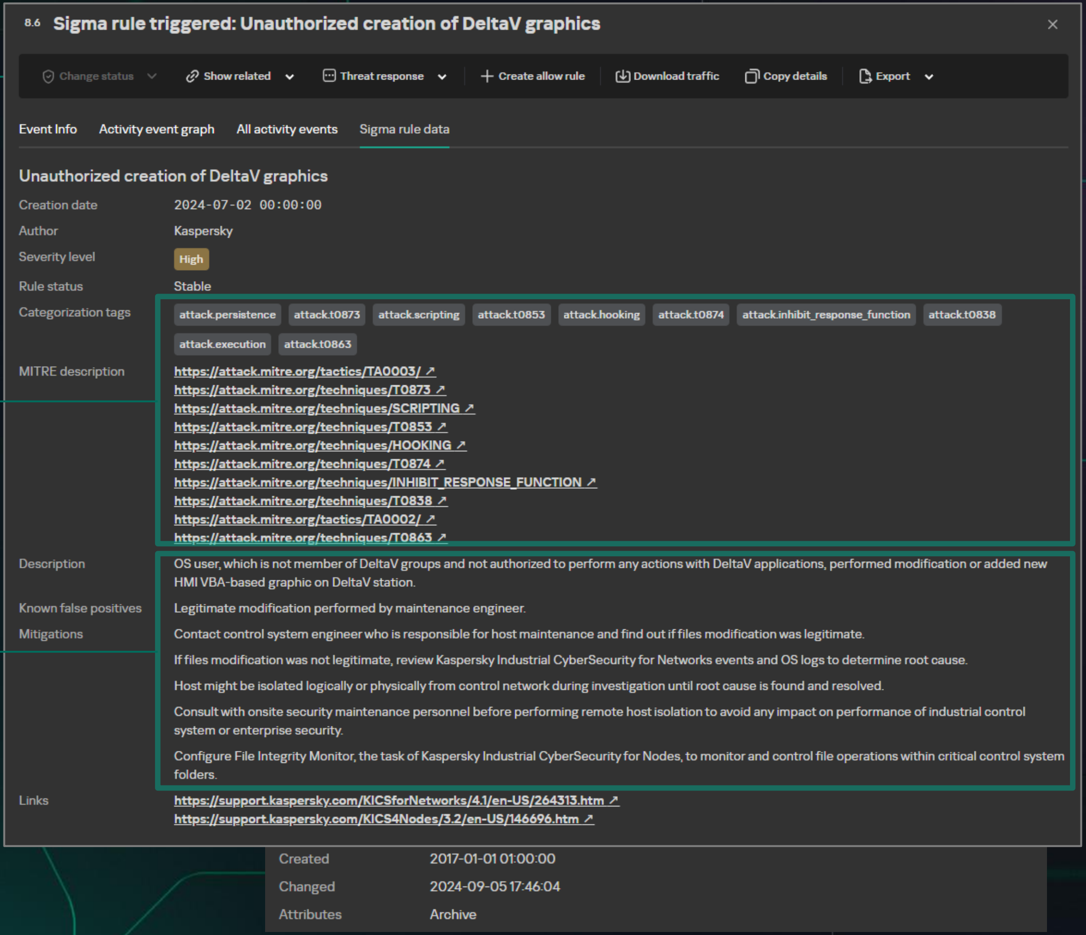
- Detection of remote administration tools (RAT)
- ICS software behavior analysis
- Custom rules

# Detection of suspicious activity in Emerson DeltaV logs

Kill-chain view for root-cause analysis (file drops, registry changes, network connections and more)

MITRE matrix mapping and reference links

Explained in details mitigation measures including KICS for Nodes settings



**Sigma rule triggered: Unauthorized creation of DeltaV graphics**

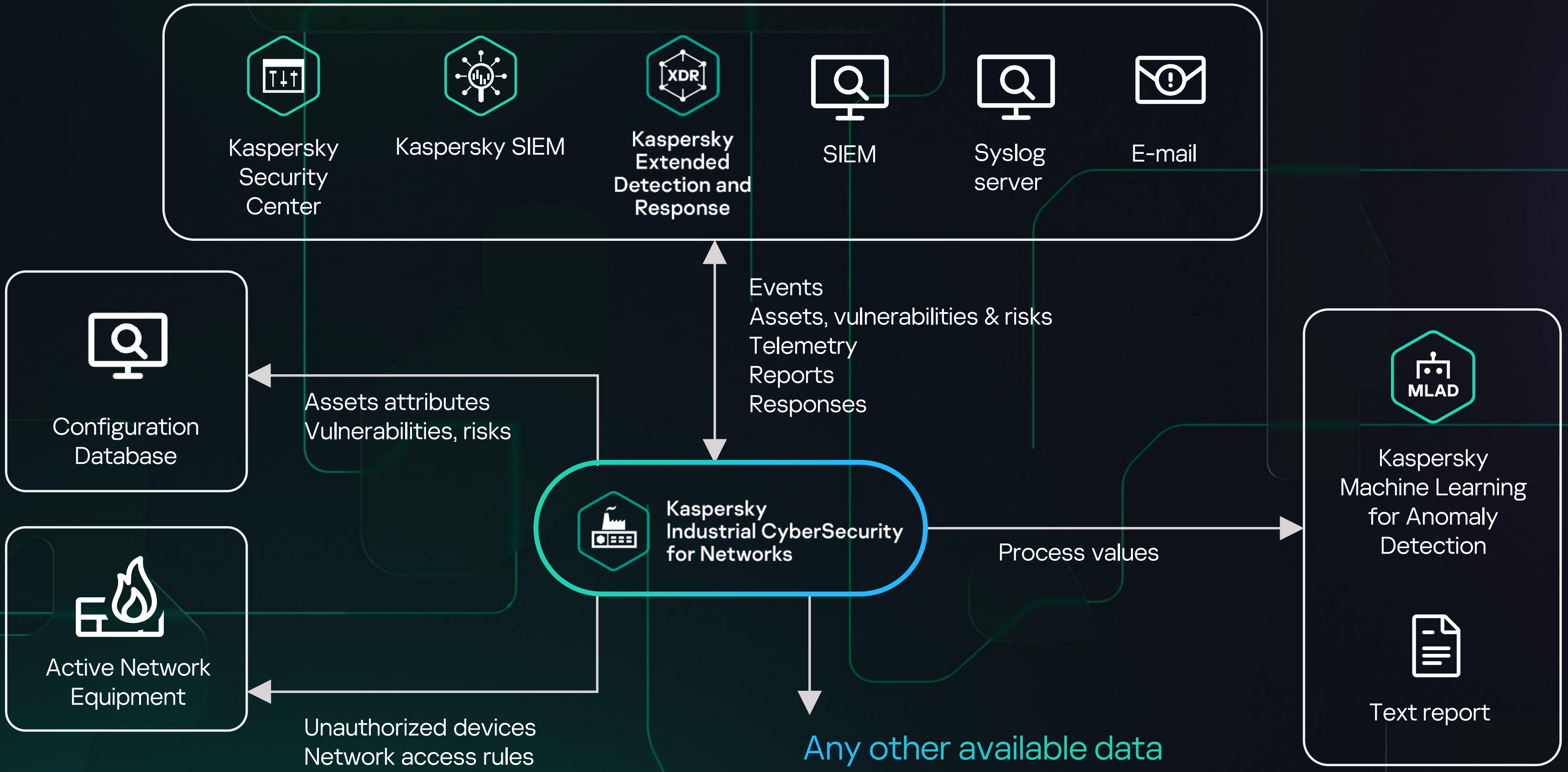
**Unauthorized creation of DeltaV graphics**

| | |
|---|---|
| Creation date | 2024-07-02 00:00:00 |
| Author | Kaspersky |
| Severity level | High |
| Rule status | Stable |
| Categorization tags | attack.persistence<br>attack.t0873<br>attack.scripting<br>attack.t0853<br>attack.hooking<br>attack.t0874<br>attack.inhibit_response_function<br>attack.t0838<br>attack.execution<br>attack.t0863 |
| MITRE description | https://attack.mitre.org/tactics/TA0003/ ↗<br>https://attack.mitre.org/techniques/T0873 ↗<br>https://attack.mitre.org/techniques/SCRIPTING ↗<br>https://attack.mitre.org/techniques/T0853 ↗<br>https://attack.mitre.org/techniques/HOOKING ↗<br>https://attack.mitre.org/techniques/T0874 ↗<br>https://attack.mitre.org/techniques/INHIBIT_RESPONSE_FUNCTION ↗<br>https://attack.mitre.org/techniques/T0838 ↗<br>https://attack.mitre.org/tactics/TA0002/ ↗<br>https://attack.mitre.org/techniques/T0863 ↗ |
| Description | OS user, which is not member of DeltaV groups and not authorized to perform any actions with DeltaV applications, performed modification or added new HMI VBA-based graphic on DeltaV station. |
| Known false positives | Legitimate modification performed by maintenance engineer. |
| Mitigations | Contact control system engineer who is responsible for host maintenance and find out if files modification was legitimate.<br>If files modification was not legitimate, review Kaspersky Industrial CyberSecurity for Networks events and OS logs to determine root cause.<br>Host might be isolated logically or physically from control network during investigation until root cause is found and resolved.<br>Consult with onsite security maintenance personnel before performing remote host isolation to avoid any impact on performance of industrial control system or enterprise security.<br>Configure File Integrity Monitor, the task of Kaspersky Industrial CyberSecurity for Nodes, to monitor and control file operations within critical control system folders. |
| Links | https://support.kaspersky.com/KICSforNetworks/4.1/en-US/264313.htm ↗<br>https://support.kaspersky.com/KICS4Nodes/3.2/en-US/146696.htm ↗ |

| | |
|---|---|
| Created | 2017-01-01 01:00:00 |
| Changed | 2024-09-05 17:46:04 |
| Attributes | Archive |

Kaspersky Industrial
Cybersecurity
Conference 2024

# Build your own ecosystem



Any other available data can be transferred using KICS for Networks API

Dmitry Astapov

Senior Product Manager, KICS

kaspersky