Security in IoT/OT Conference

Monitoring and analysis of network data in production network - added value

Joachim Gay
Senior Presales Engineer

kaspersky

IoT Security

About Kaspersky

Our mission is simple — building a safer world.

And in fulfilling that mission we aim to become the global leader in cybersecurity — by securing technology to make sure that the possibilities it brings become opportunities for each and every one of us.

Bring on endless possibilities.
Bring on a safer tomorrow.

Eugene Kaspersky, CEO

About me

Electronics engineer IT/CT

30+ years experience in IT industry

Joined Kaspersky in 2008

Joachim Gay

Senior Presales Engineer

Introduction

> As digital business blurs the digital and physical worlds, digital breaches result in physical damage.

Gartner

How does it happen?

“common ransoware” attack

Stage 1 – Intrusion

2021 Top 3 initial access vectors

- Vulnerability exploitation
- Compromised accounts
- Malicious email

Stage 2 – Attack

Data Exfiltration
Encryption
Blackmailing
↓
Quickly spreads from corporate network to shopfloor
↓
Production affected

Source: Kaspersky Incident Response Analytics Report

Why does it happen?

Unpatched public facing services
Human factor
Unpatched software usage

Missing network segregation/segmentation
No visibility on OT communications
Vulnerable OT components

How does it happen?

ICS specific attack - Triton

Stage 1 – Intrusion

External Remote Services
Valid Accounts
↓
Mimikatz, PsExec, and other tools
Remote Desktop Protocol
Remote Services

Stage 2 – SIS Attack

Engineering Workstation Compromise
↓
Firmware & program upload and
0-day vulnerability exploitation
in a safety controller
↓
Plant emergency shutdown

Why does it happen?

Large corporate infrastructures
Human factor
Supply chain attacks

OT is never isolated from IT
No visibility on OT communications
Vulnerable OT components

Industrial facility architecture – Purdue model (simplified)

PERA –
hierarchical reference model

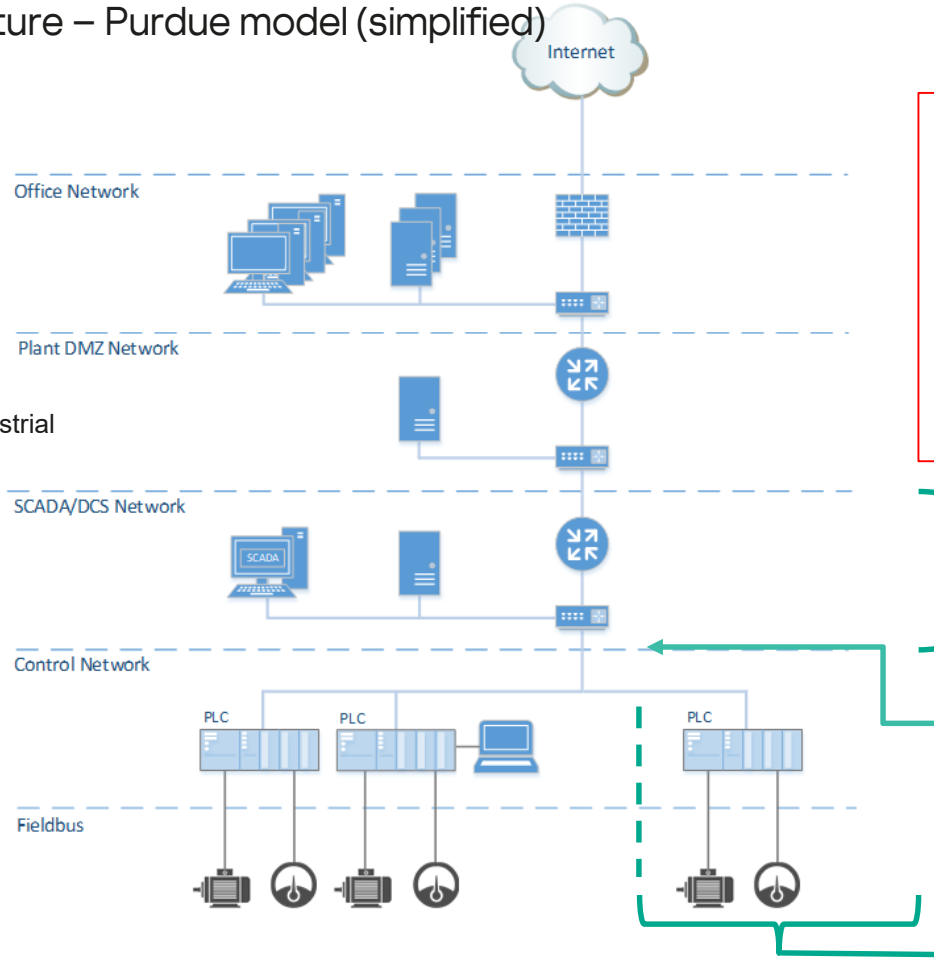
LEVEL 4 / 5
Enterprise

LEVEL 3 / 3.5
Site-level operation / industrial perimeter network

LEVEL 2
Supervisory

LEVEL 1
Process control

LEVEL 0
Physical



Standards like ISA/IEC 62443 have largely evolved beyond dependence on a traditional hierarchical view of functionality.
It address cybersecurity for operational technology in automation and control systems.

Zone
consists of assets that share the same cybersecurity requirements

Conduit
consists of assets dedicated exclusively to communications, share the same cybersecurity requirements

Sub-zone

Examples from the field

Machine-readable threat intelligence

Three examples of how machine-readable threat intelligence can help you:

- baseline systems and security posture
- prevent threats
- detect incidents
- remediate / investigate incidents

Example **#1** – security exposure

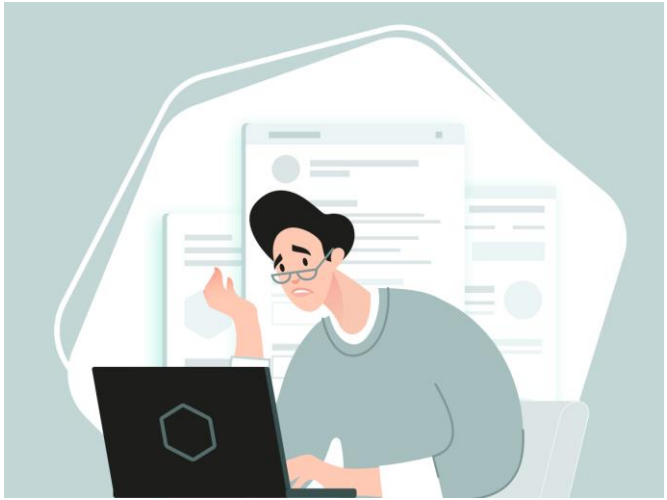
Your CISO requests to identify vulnerabilities in the Windows DCS/SCADA software used on your shop-floor-systems to perform risk assessment.

Easy to achieve?

Where do I find vulnerability information?

System already assessed?

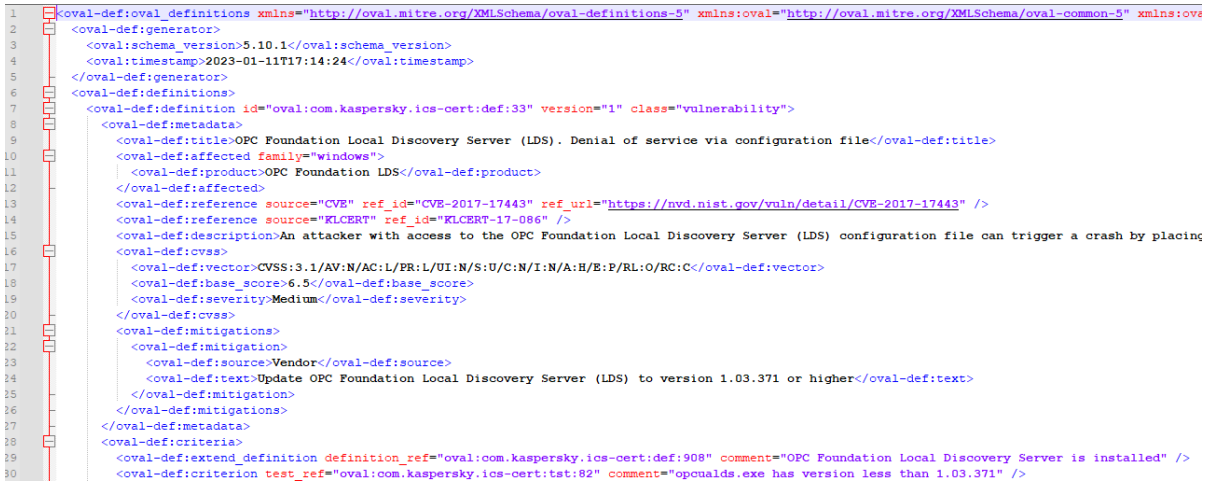
Software bill of materials available?



Example **#1** - assess security exposure by OVAL data feed

OVAL stands for Open Vulnerability and Assessment Language, which is used to describe security vulnerabilities or desired system configurations and allows for standardized transfer of vulnerability information across various security tools and services.
It is one of the main components of the SCAP standard (Security Content Automation Protocol).

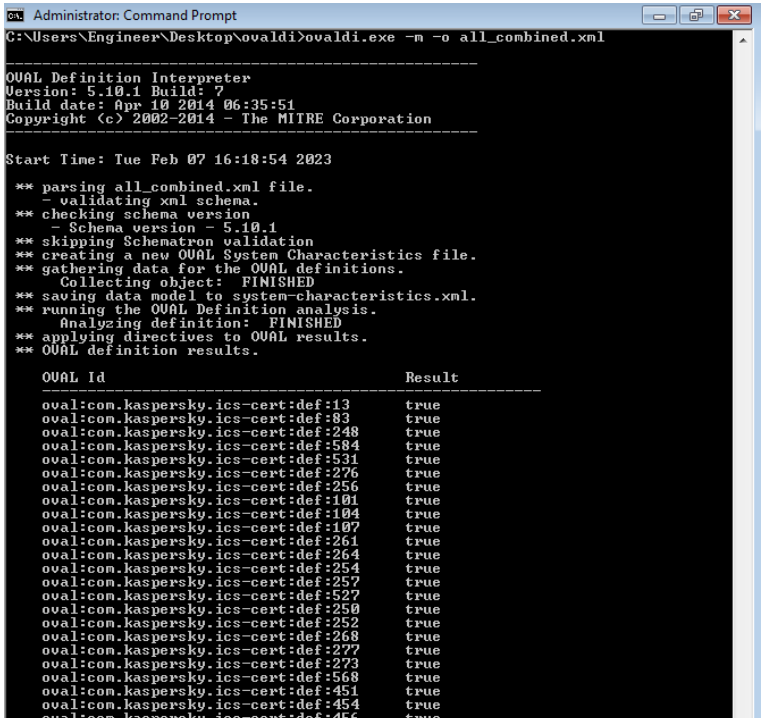
OVAL definition in XML:

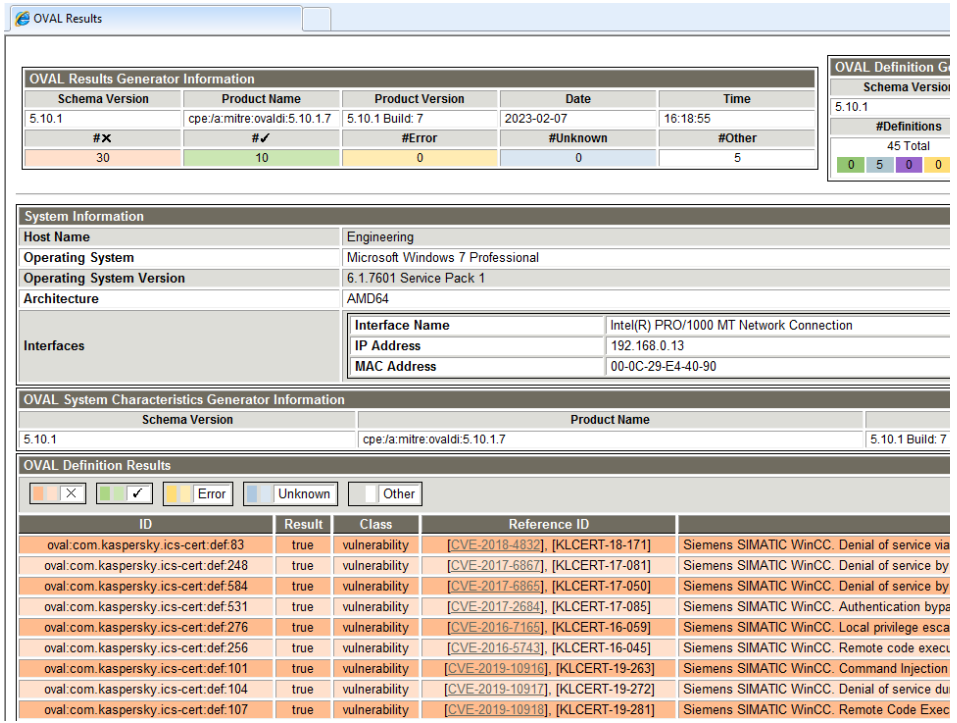


```
<oval-def:oval_definitions xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5" xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5" xmlns:ova
  <oval-def:generator>
    <oval:schema_version>5.10.1</oval:schema_version>
    <oval:timestamp>2023-01-11T17:14:24</oval:timestamp>
  </oval-def:generator>
  <oval-def:definitions>
    <oval-def:definition id="oval:com.kaspersky.ics-cert:def:33" version="1" class="vulnerability">
      <oval-def:metadata>
        <oval-def:title>OPC Foundation Local Discovery Server (LDS). Denial of service via configuration file</oval-def:title>
        <oval-def:affected family="windows">
          <oval-def:product>OPC Foundation LDS</oval-def:product>
        </oval-def:affected>
        <oval-def:reference source="CVE" ref_id="CVE-2017-17443" ref_url="https://nvd.nist.gov/vuln/detail/CVE-2017-17443" />
        <oval-def:reference source="KLCERT" ref_id="KLCERT-17-086" />
        <oval-def:description>An attacker with access to the OPC Foundation Local Discovery Server (LDS) configuration file can trigger a crash by placing
        <oval-def:cvss>
          <oval-def:vector>CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C</oval-def:vector>
          <oval-def:base_score>6.5</oval-def:base_score>
          <oval-def:severity>Medium</oval-def:severity>
        </oval-def:cvss>
        <oval-def:mitigations>
          <oval-def:mitigation>
            <oval-def:source>Vendor</oval-def:source>
            <oval-def:text>Update OPC Foundation Local Discovery Server (LDS) to version 1.03.371 or higher</oval-def:text>
          </oval-def:mitigation>
        </oval-def:mitigations>
      </oval-def:metadata>
      <oval-def:criteria>
        <oval-def:extend_definition definition_ref="oval:com.kaspersky.ics-cert:def:908" comment="OPC Foundation Local Discovery Server is installed" />
        <oval-def:criterion test_ref="oval:com.kaspersky.ics-cert:tst:82" comment="opcualds.exe has version less than 1.03.371" />
```

Example **#1** – OVAL data feed can be used in open-source or commercial tools

ovaldi.exe –m –o oval_feed.xml → results.[xml | html]





Example **#1** - HTML output file of OVALdi local command line scanner

1 engineering workstation scanned

4 ICS software products detected

30 vulnerabilities found:

CVSS 3.0 rating:

Critical:	3
High:	15
Medium:	11
Low:	0

CVSS 2.0 rating:

Critical:	0
High:	1
Medium	0
Low:	0

✕ ✓ Error Unknown Other

ID	Result	Class	Reference ID	Title
oval:com.kaspersky.ics-cert:def:83	true	vulnerability	[CVE-2018-4832], [KLCERT-18-171]	Siemens SIMATIC WinCC. Denial of service via specially crafted RPC messages
oval:com.kaspersky.ics-cert:def:248	true	vulnerability	[CVE-2017-6867], [KLCERT-17-081]	Siemens SIMATIC WinCC. Denial of service by sending specially crafted DCOM packets
oval:com.kaspersky.ics-cert:def:584	true	vulnerability	[CVE-2017-6865], [KLCERT-17-050]	Siemens SIMATIC WinCC. Denial of service by sending specially crafted PROFINET DCP broadcast packets
oval:com.kaspersky.ics-cert:def:531	true	vulnerability	[CVE-2017-2684], [KLCERT-17-085]	Siemens SIMATIC WinCC. Authentication bypass
oval:com.kaspersky.ics-cert:def:276	true	vulnerability	[CVE-2016-7165], [KLCERT-16-059]	Siemens SIMATIC WinCC. Local privilege escalation due to unquoted service paths
oval:com.kaspersky.ics-cert:def:256	true	vulnerability	[CVE-2016-5743], [KLCERT-16-045]	Siemens SIMATIC WinCC. Remote code execution
oval:com.kaspersky.ics-cert:def:101	true	vulnerability	[CVE-2019-10916], [KLCERT-19-263]	Siemens SIMATIC WinCC. Command Injection with Local Database Server Rights
oval:com.kaspersky.ics-cert:def:104	true	vulnerability	[CVE-2019-10917], [KLCERT-19-272]	Siemens SIMATIC WinCC. Denial of service during project file loading process
oval:com.kaspersky.ics-cert:def:107	true	vulnerability	[CVE-2019-10918], [KLCERT-19-281]	Siemens SIMATIC WinCC. Remote Code Execution with "SYSTEM" Privileges
oval:com.kaspersky.ics-cert:def:261	true	vulnerability	[CVE-2019-10935], [KLCERT-19-200]	Siemens SIMATIC WinCC. Remote code execution via unrestricted file upload
oval:com.kaspersky.ics-cert:def:264	true	vulnerability	[CVE-2019-19282], [KLCERT-19-212]	Siemens SIMATIC WinCC (including TIA Portal). Denial of service via a specially crafted UDP packet when encrypted communication is enabled
oval:com.kaspersky.ics-cert:def:254	true	vulnerability	[CVE-2020-7580], [KLCERT-20-142]	Siemens SIMATIC WinCC. Arbitrary code execution with 'SYSTEM' privileges
oval:com.kaspersky.ics-cert:def:257	true	vulnerability	[CVE-2020-10048], [KLCERT-20-141]	Siemens SIMATIC WinCC. Authentication Bypass to the password-protected files
oval:com.kaspersky.ics-cert:def:527	true	vulnerability	[CVE-2021-40142], [KLCERT-21-440]	Siemens SIMATIC WinCC. Denial of service
oval:com.kaspersky.ics-cert:def:250	true	vulnerability	[CVE-2021-40358], [KLCERT-21-329]	Siemens SIMATIC WinCC. Arbitrary file operations via Path Traversal
oval:com.kaspersky.ics-cert:def:252	true	vulnerability	[CVE-2021-40359], [KLCERT-21-331]	Siemens SIMATIC WinCC. Arbitrary file reading via Path Traversal
oval:com.kaspersky.ics-cert:def:268	true	vulnerability	[CVE-2021-40360], [KLCERT-21-390]	Siemens SIMATIC WinCC. Exposure of password hash to an unauthorized actor
oval:com.kaspersky.ics-cert:def:277	true	vulnerability	[CVE-2021-40363], [KLCERT-21-391]	Siemens SIMATIC WinCC. Insertion of sensitive information into externally accessible file or directory
oval:com.kaspersky.ics-cert:def:273	true	vulnerability	[CVE-2021-40364], [KLCERT-21-330]	Siemens SIMATIC WinCC. Information disclosure via log files
oval:com.kaspersky.ics-cert:def:451	true	vulnerability	[CVE-2015-1594], [KLCERT-15-026]	Siemens SIMATIC STEP 7. Arbitrary code execution
oval:com.kaspersky.ics-cert:def:454	true	vulnerability	[CVE-2021-31894], [KLCERT-21-222]	Siemens SIMATIC STEP 7. Incorrect permission assignment
oval:com.kaspersky.ics-cert:def:456	true	vulnerability	[CVE-2021-31893], [KLCERT-21-446]	Siemens SIMATIC STEP 7. Remote code execution
oval:com.kaspersky.ics-cert:def:332	true	vulnerability	[CVE-2020-7585], [KLCERT-20-155]	Siemens SIMATIC STEP 7. Arbitrary code execution via DLL hijacking
oval:com.kaspersky.ics-cert:def:333	true	vulnerability	[CVE-2020-7586], [KLCERT-20-156]	Siemens SIMATIC STEP 7. Denial of service due to heap-based buffer overflow
oval:com.kaspersky.ics-cert:def:876	true	vulnerability	[CVE-2020-7580], [KLCERT-20-243]	Siemens SIMATIC STEP 7. Arbitrary code execution with 'SYSTEM' privileges
oval:com.kaspersky.ics-cert:def:2	true	vulnerability	[CVE-2016-8563], [KLCERT-16-067]	Siemens Automation License Manager. Denial of service by specially crafted packets
oval:com.kaspersky.ics-cert:def:3	true	vulnerability	[CVE-2016-8564], [KLCERT-16-068]	Siemens Automation License Manager. SQL Injection
oval:com.kaspersky.ics-cert:def:136	true	vulnerability	[CVE-2018-11455], [KLCERT-18-173]	Siemens Automation License Manager. Remote code execution
oval:com.kaspersky.ics-cert:def:1074	true	vulnerability	[CVE-2018-11456], [KLCERT-18-174]	Siemens Automation License Manager. Port scanning vis specially crafted packets
oval:com.kaspersky.ics-cert:def:33	true	vulnerability	[CVE-2017-17443], [KLCERT-17-086]	OPC Foundation Local Discovery Server (LDS). Denial of service via configuration file
oval:com.kaspersky.ics-cert:def:13	true	inventory		Siemens SIMATIC WinCC is installed
oval:com.kaspersky.ics-cert:def:568	true	inventory		Siemens SIMATIC STEP 7 is installed
oval:com.kaspersky.ics-cert:def:5	true	inventory		Siemens Automation License Manager is installed
oval:com.kaspersky.ics-cert:def:902	false	inventory		ARC Informatique PcVue is installed
oval:com.kaspersky.ics-cert:def:908	true	inventory		OPC Foundation Local Discovery Server is installed
oval:com.kaspersky.ics-cert:def:448	false	vulnerability	[CVE-2015-1594], [KLCERT-15-026]	Siemens SIMATIC STEP 7. Arbitrary code execution
oval:com.kaspersky.ics-cert:def:449	false	vulnerability	[CVE-2015-1594], [KLCERT-15-026]	Siemens SIMATIC STEP 7. Arbitrary code execution
oval:com.kaspersky.ics-cert:def:450	false	vulnerability	[CVE-2015-1594], [KLCERT-15-026]	Siemens SIMATIC STEP 7. Arbitrary code execution
oval:com.kaspersky.ics-cert:def:452	false	vulnerability	[CVE-2015-1594], [KLCERT-15-026]	Siemens SIMATIC STEP 7. Arbitrary code execution
oval:com.kaspersky.ics-cert:def:877	false	vulnerability	[CVE-2020-7580], [KLCERT-20-243]	Siemens SIMATIC STEP 7. Arbitrary code execution with 'SYSTEM' privileges
oval:com.kaspersky.ics-cert:def:878	false	vulnerability	[CVE-2020-7580], [KLCERT-20-243]	Siemens SIMATIC STEP 7. Arbitrary code execution with 'SYSTEM' privileges
oval:com.kaspersky.ics-cert:def:879	false	vulnerability	[CVE-2020-7580], [KLCERT-20-243]	Siemens SIMATIC STEP 7. Arbitrary code execution with 'SYSTEM' privileges
oval:com.kaspersky.ics-cert:def:880	false	vulnerability	[CVE-2020-7580], [KLCERT-20-243]	Siemens SIMATIC STEP 7. Arbitrary code execution with 'SYSTEM' privileges
oval:com.kaspersky.ics-cert:def:36	false	vulnerability	[CVE-2020-26868], [KLCERT-20-016]	ARC Informatique PcVue. Denial of service
oval:com.kaspersky.ics-cert:def:37	false	vulnerability	[CVE-2020-26869], [KLCERT-20-017]	ARC Informatique PcVue. Session information exposure

Note that vulnerabilities in the operating system and other software products were not considered!

Example **#1** – take away

Kaspersky Industrial OVAL Data Feed for Windows:

- provides high-quality machine-readable vulnerability data
- covers most popular SCADA systems and other industrial software

Supports owner of industrial control system with:

- automated detection of known vulnerabilities in ICS Software
- assessment of existing cybersecurity risks
- choosing appropriate mitigation measures

Example **#2** – Triton Attack – threat from outside

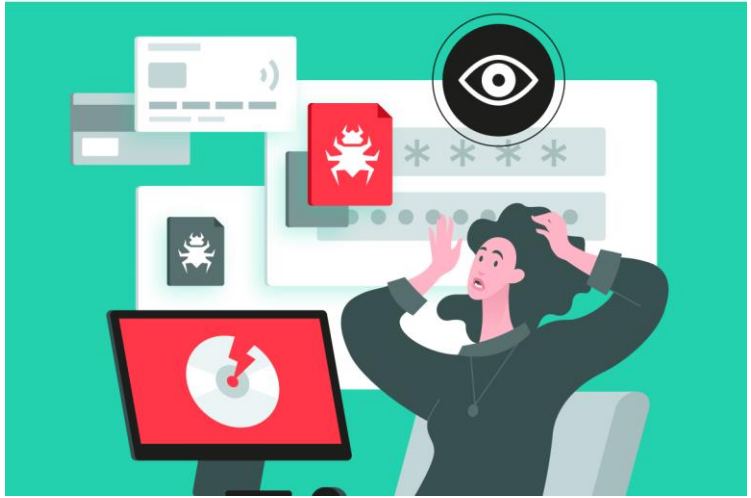
Triton (aka Trisis /Hatman) attack targeted Schneider Electric Triconex safety systems to cause physical damage.

How effective is your north-south network protection?

Are you aware of ‘standard’ network communication?

Do you monitor your production network, e.g. east-west traffic?

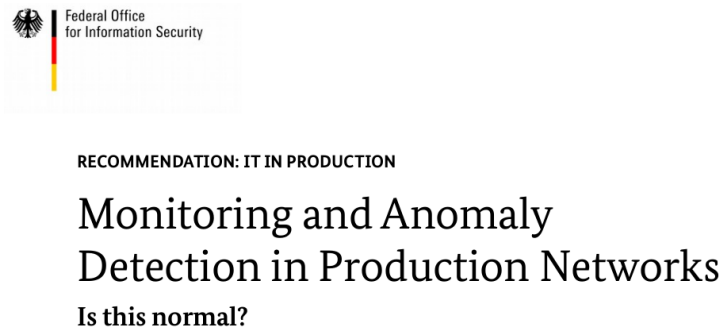
Has your plant been assessed?



Example **#2** – attack detection / network monitoring recommended in ICS

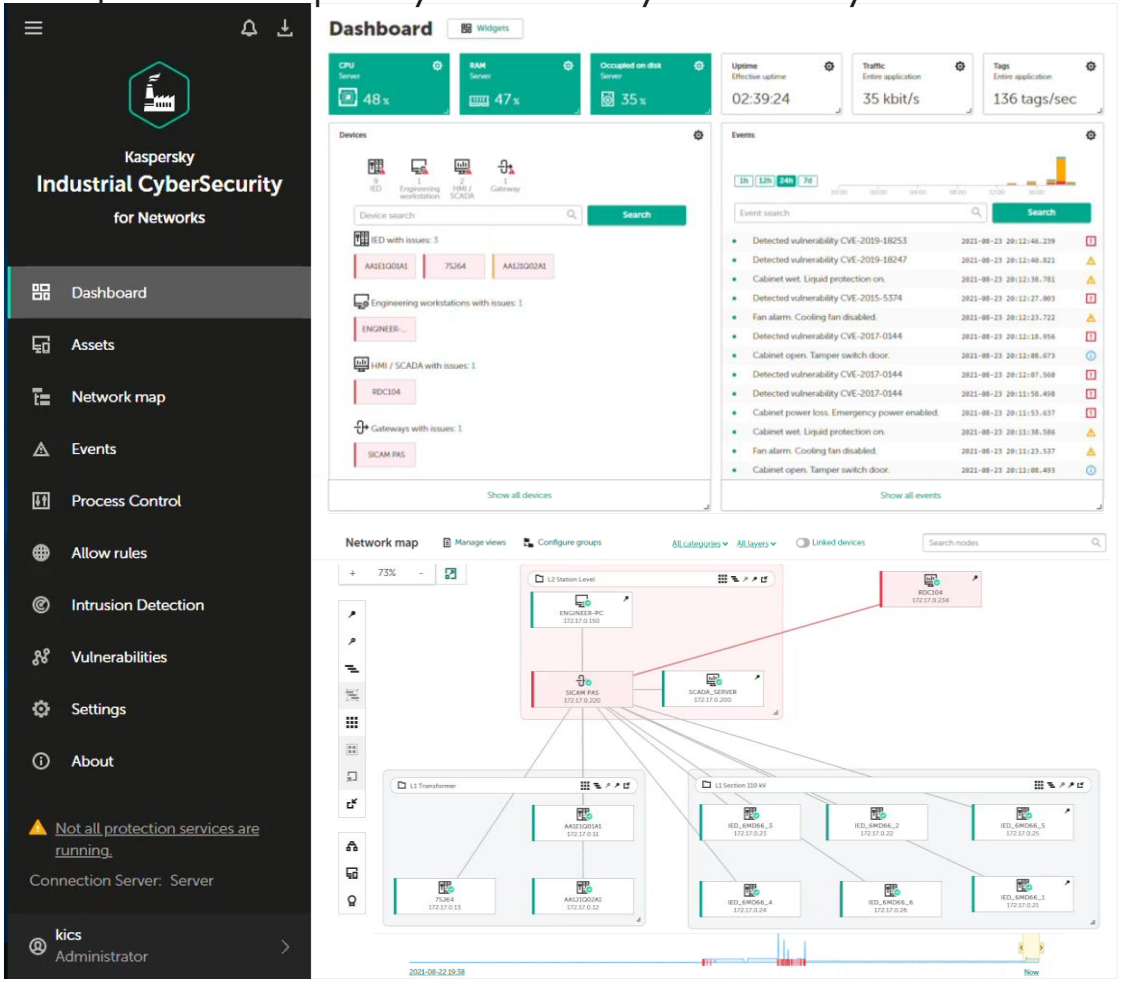
The German Federal Office for Information Security (BSI) recommends, monitoring and anomaly detection in production networks.

Critical Infrastructures Ordinance (*KRITIS*-Verordnung) of German IT Security Act 2.0 obliges the operators:
"...to use attack detection systems [...] from 1 May 2023 according to the legislation."



Source: BSI - Recommendations for ICS Operators

Example **#2** – Kaspersky Industrial CyberSecurity for Networks



OT Intrusion Detection

Ability to detect APTs on the lowest level (ICS Protocols DPI and specific signatures)

Asset Inventory

Passive detection of OT components, their communications and known vulnerabilities

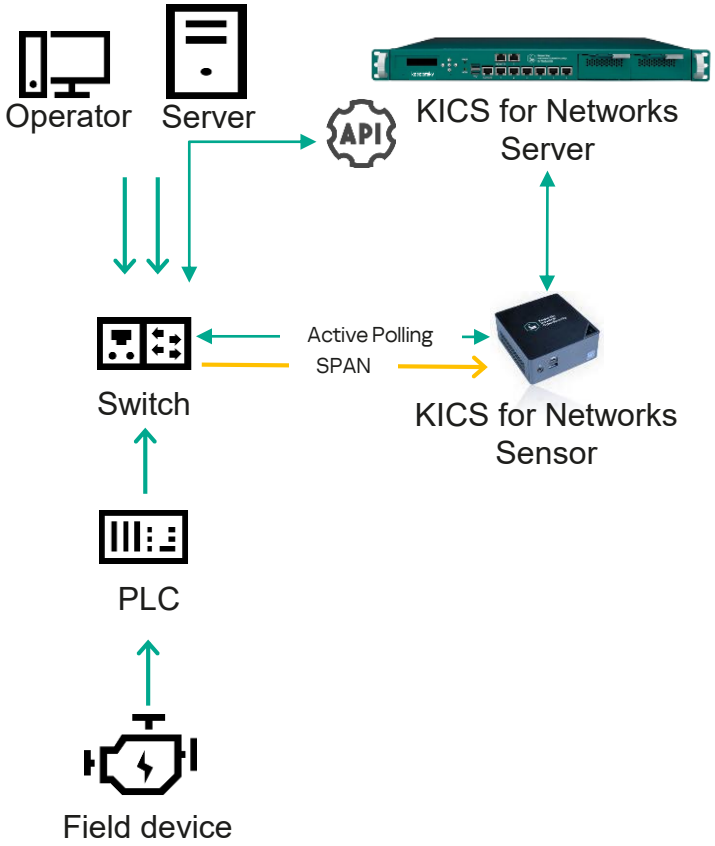
Visibility

Situational awareness and reporting, identifying deviations from the normal state

Response and audit

Assists in root cause analysis for OT incidents, provides value to incident responders/SOC personal

Example **#2** – active / passive network monitoring technologies and capabilities



OT Network Security Monitoring - Key Technologies and Capabilities

Passive:

Asset Discovery – executes passive & detailed OT infrastructure inventory
Risk Scoring – alarms on asset, infrastructure or process risks in OT infrastructure
Network Integrity Control – detects unauthorized network hosts and flows
Command Control – inspects commands over industrial protocols
Network Interactions Map – visualizes network communication flow
Intrusion Detection System – alarms on signs of offensive network actions
ICS Deep Packet Inspection – inspects OT traffic for process parameter values
PLC Integrity Control – learns PLC program state and tracks changes from traffic

Active:

Active Polling – permits to clarify attributes which are not found passively
Network Topology – represents schematic network topology diagram
API – provides external system integration and response capabilities

Example **#2** – take away

The Trition attack would be detected, even without knowing about details of the attack.

Just by the deviation from the normal state (baseline) of network communication, the unknown communication would be discovered and reported by Kaspersky Industrial CyberSecurity for Networks.

Later on the Federal Office for Information Security provided a SNORT IDS rule and description about the detection methodology.

Source: BSI - Recognizing Anomalies in Protocols of Safety Networks: Schneider Electric's TriStation (RAPSN SETS)

Example **#3** – Visit of manufacturer – threat from inside

Visit of the manufacturer service personnel on the production line, to troubleshoot an issue. To analyze the problem the technician needs access to machine debug interface which is connected to your network.

How effective is your north-south network protection?

Do you monitor your production network, e.g. east-west traffic?

What could happen if a foreign laptop is plugged into the production network?

Network baseline available?

Example **#3** – take away

While entering the plant the service technician bypassed all your north-south network protection measures.

With OT monitoring and anomaly solutions like Kaspersky Industrial Cybersecurity for Networks in place, you would detect threats and store information for retrospective analysis.

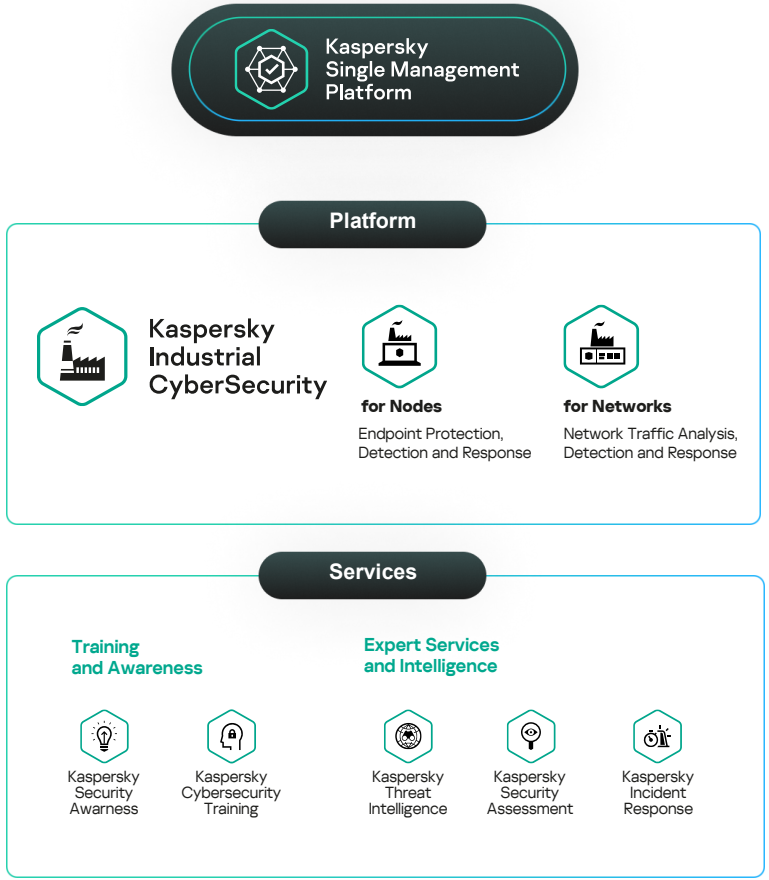
- network scans
- malware communication (IDS rules)
- communication with PLCs
- record all the communication
- store pcap files in case of an incident

Source: BSI - Recognizing Anomalies in Protocols of Safety Networks: Schneider Electric's TriStation (RAPSN SETS)

Products & Services

Solution for industrial enterprises

Platform of natively integrated technologies, training and expert services.



Thank you!

Click here for more information about
Kaspersky Industrial CyberSecurity
or contact our Swiss team.

Kaspersky Lab Switzerland GmbH
Bahnhofstrasse 69
8001 Zürich
Rene Bodmer <Rene.Bodmer@kaspersky.com>

kaspersky