A security platform for Industrial Enterprise sustainability and digital transformation

Kaspersky Industrial CyberSecurity Platform

kaspersky BRING ON THE FUTURE

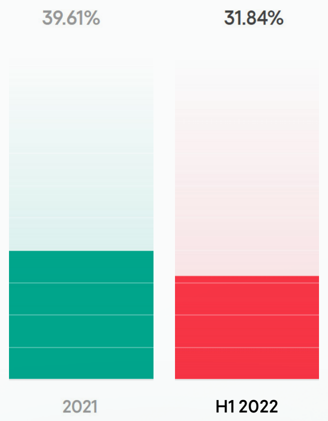
Attacked by malware

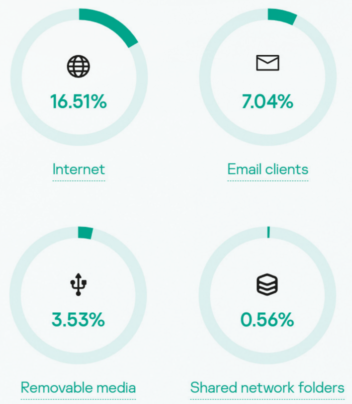
Since the beginning of 2022, nearly 30% of computers related to ICS have been attacked by malware – almost 10% less than the previous year

Kaspersky ICS-CERT, June 2022

Learn more

Percentage of ICS computers on which malicious objects have been blocked since the beginning of 2022





Industrial enterprises approach cybersecurity in their IT and OT (operational technology) infrastructures differently. Most companies already have mature Detection and Response measures in their corporate networks, but when it comes to OT they usually rely on an out-of-date airgapped approach. Industrial companies are becoming increasingly 'digital', investing more and more in smart technologies, new automation systems, and the adoption of digital transformation. This actually erases the traditional gap between IT and OT environments – a gap that used to prevent cyberthreats from reaching industrial automation and control systems.

You may be a target — but don't be a victim

You don't have to be a target to become a victim of accidental airgap breaches or malware infection. A single flash drive, cellphone, phishing email or ransomware brought into the ICS environment can seriously affect the core business of a company. At the same time, a motivated hacking group can penetrate OT networks and cause considerable damage to equipment, processes, production, safety and quality, or steal valuable information.

Essential cybersecurity for OT

Endpoint protection

for standalone and connected systems. A safe and tested solution should help to enforce security policies, support compliance, perform security audits, manage inventory, carry out patching tasks and collect precise telemetry as an endpoint sensor

Network protection

for communication visibility, threat detection and asset management. The Network Traffic Analysis and Intrusion Detection System controls the efficacy of firewall settings, network segmentation and network usage compliance and helps to provide safe manual response

Training programs

for employees to reduce accidents and minimize the human factor (human error)

Expert services

to investigate the infrastructure conduct expert analytics or mitigate the impact of an incident

Global recognition

Frost and Sullivan recognized Kaspersky with the 2020 Global Company of the Year Award based on analysis of the Global Industrial (OT/ICS) Cyber Security market

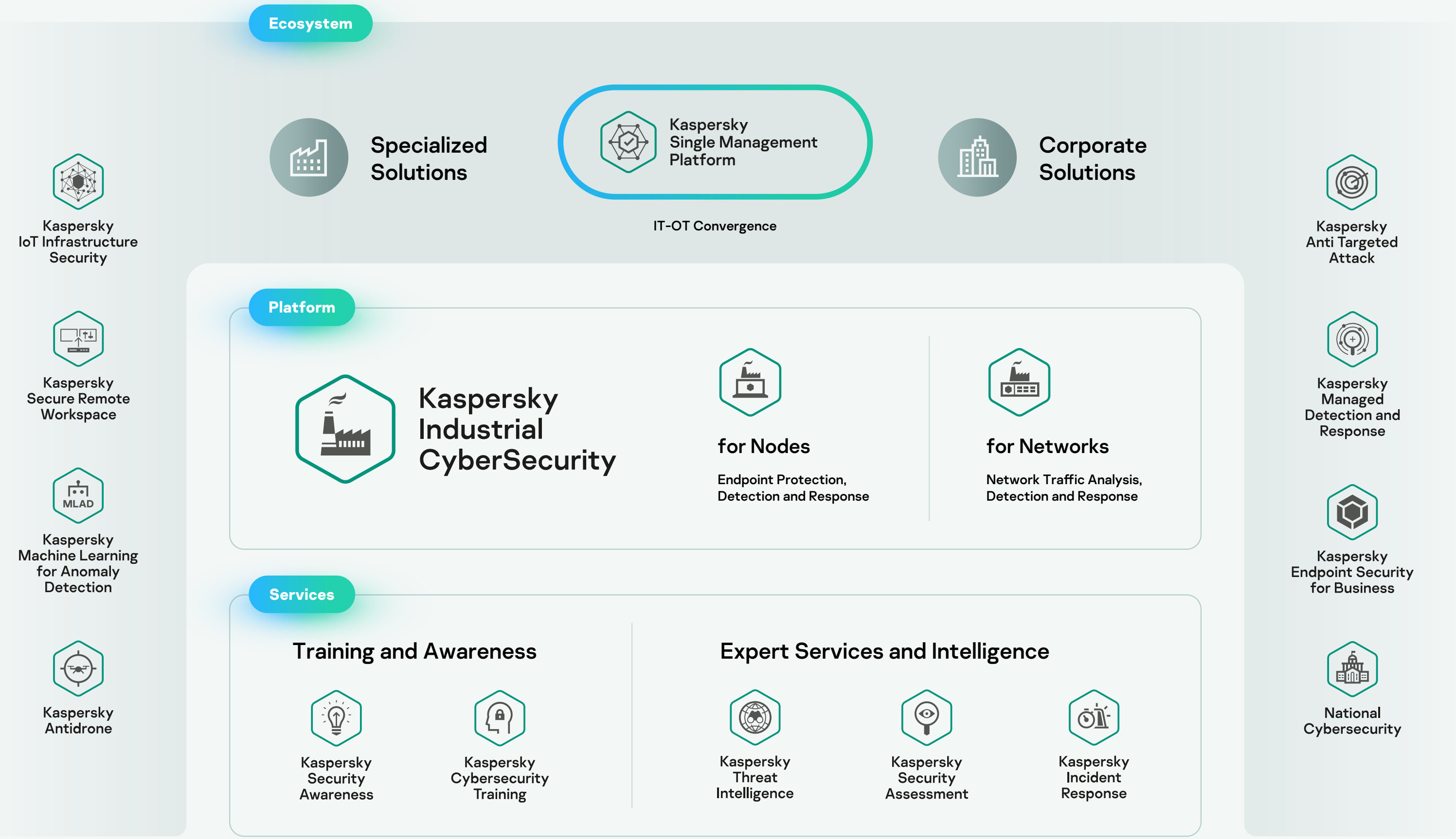
In **VDC's** annual global survey, Kaspersky was the top vendor in the industrial cybersecurity category, based on overall ratings by over 250 qualified professionals in the industrial automation community

What Kaspersky delivers

The Kaspersky Industrial CyberSecurity (KICS) Platform of natively integrated technologies, together with our portfolio of expert training and services address all the cybersecurity needs of industrial enterprises and critical infrastructure operators.

The platform is a key element in a unique ecosystem for industrial enterprises that includes:

- Kaspersky's best-in-class Corporate Solutions, which delivers true IT–OT convergence and the multiple benefits of a one-vendor approach
- Various Specialized Solutions for cyber-physical security, industrial IOT security, machine learning, secure remote workspace and many more bring unlimited, agile scalability



Ecosystem

Specialized Solutions

Kaspersky Single Management Platform

Corporate Solutions

IT-OT Convergence

Kaspersky IoT Infrastructure Security

Kaspersky Secure Remote Workspace

Kaspersky Machine Learning for Anomaly Detection

Kaspersky Antidrone

Kaspersky Anti Targeted Attack

Kaspersky Managed Detection and Response

Kaspersky Endpoint Security for Business

National Cybersecurity

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 Awareness

Kaspersky Cybersecurity Training

Expert Services and Intelligence

Kaspersky Threat Intelligence

Kaspersky Security Assessment

Kaspersky Incident Response

Kaspersky Industrial CyberSecurity Platform is a leader in following categories:

OT Endpoint Security

OT Network Monitoring and Visibility

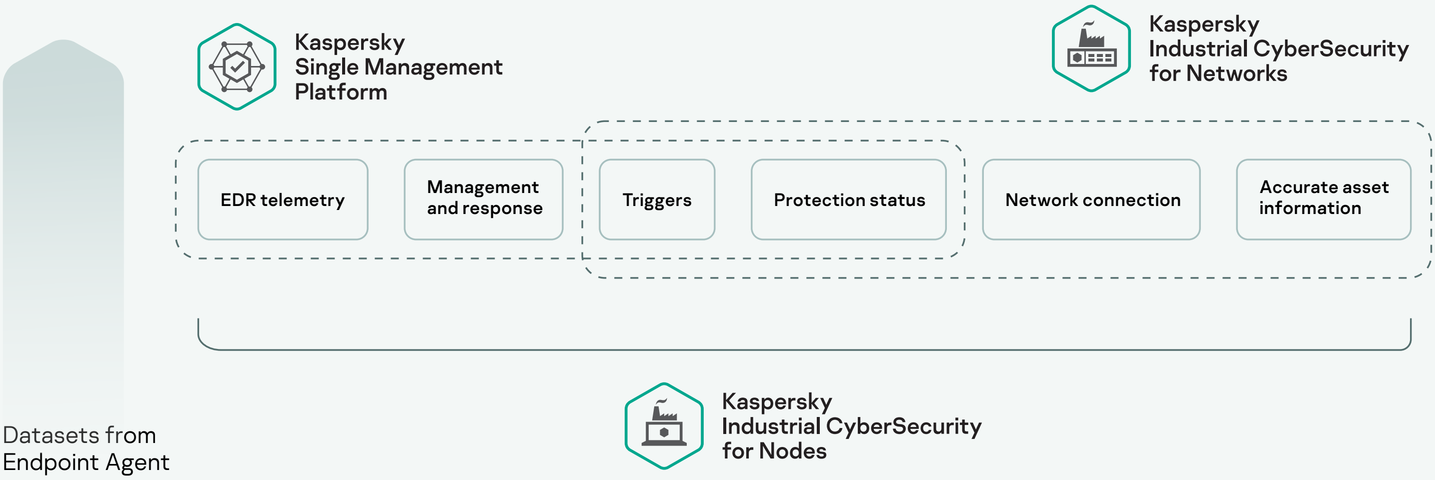
Anomaly Detection, Incident Response and Reporting

OT Security Services

Products

KICS is an OT cybersecurity platform designed for comprehensive protection of core Industrial Automation and Control System components on every level. Seamless integration between platform components provides full visibility of multiple geographically distributed OT networks and automation systems, delivering improved customer experience, situational awareness and deployment flexibility.

When used together, a user sees the bigger picture and broader context: chain of incidents on network and endpoint level, precise asset parameters, network communication and topology maps even from segments where traffic mirroring is not yet available and more.


Kaspersky Single Management Platform

Kaspersky Industrial CyberSecurity for Networks

EDR telemetry

Management and response

Triggers

Protection status

Network connection

Accurate asset information

Kaspersky Industrial CyberSecurity for Nodes

Datasets from Endpoint Agent

KICS for Nodes is endpoint protection, detection and response software with compliance audit and endpoint sensor functionality.

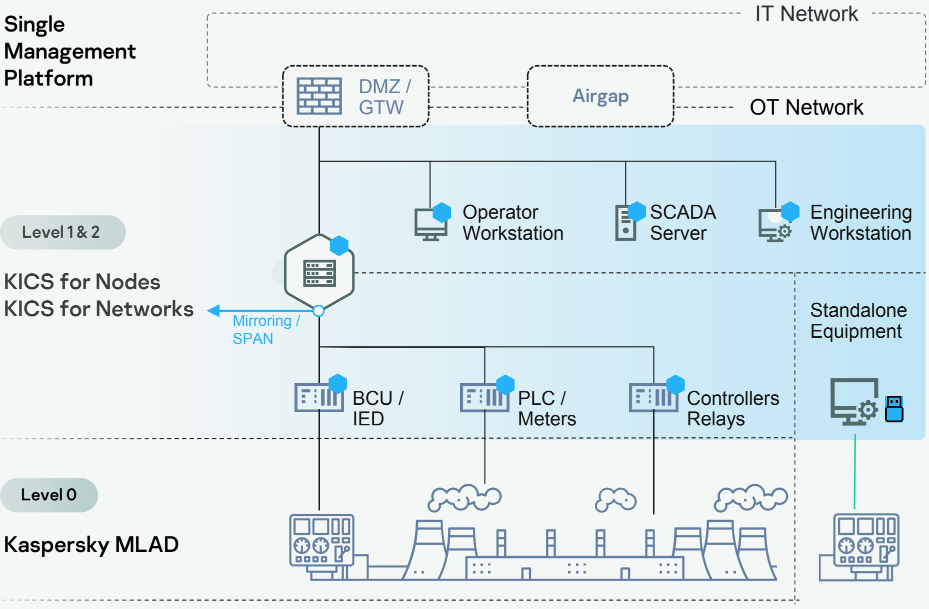
KICS for Networks is designed for OT network-traffic analysis, detection and response.

The Single Management Platform brings an advanced EDR interface and quick scalability to numerous locations.

Additional functions

The solution provides numerous additional functions. Network **Active Polling** technology enables quick and precise collection of network topology and assets settings. The **Endpoint Audit** function helps to ensure security policy compliance, including the safety of current settings, and control vulnerabilities. The **Portable Scanner** delivery method of KICS for Nodes helps to establish best practices of standalone, airgapped equipment security audits. **Machine Learning for Anomaly Detection** is an early anomaly detection system deep in the technological process.

Solution Architecture



● Protected by Kaspersky products

Features

Asset discovery

Passive OT asset identification and inventory

Deep packet inspection

Near real-time analysis of technical process telemetry

Network integrity control

Detects unauthorized network hosts and flows

Intrusion detection system

Sends alerts about malicious network activities

Command control

Inspects commands over industrial protocols

External integration

Flexible API integration adds detection and prevention capabilities

Machine learning for anomaly detection (MLAD)

Finds cyber or physical anomalies through real-time telemetry and historical data mining (recurrent neural network)

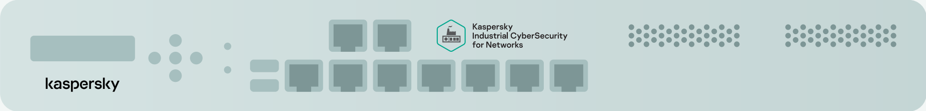
Vulnerability management

Updatable database of vulnerabilities in industrial equipment, powered by Kaspersky ICS CERT

Kaspersky
Industrial CyberSecurity
for Networks

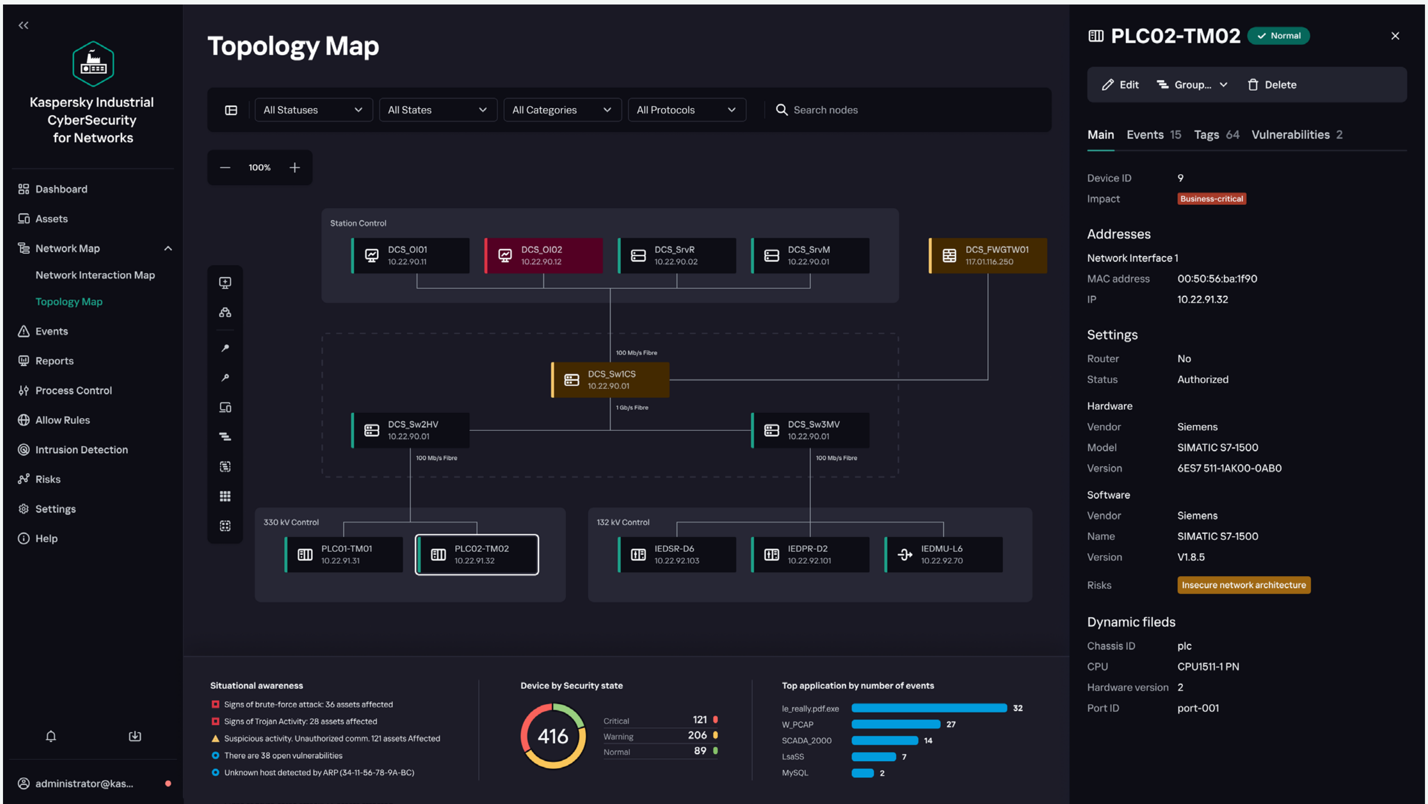
OT Network Traffic Analysis, Detection and Response. Clear risk visibility with passive traffic monitoring, active polling and endpoint sensors.

Detects anomalies and intrusions inside ICS networks in their early stages and ensures the necessary actions are taken to prevent any negative impact on industrial processes.



Appliance-agnostic solution that can be quickly and optimally integrated into the established sourcing, integration and warranty practices of our customers.

Interface



Situational awareness

- Signs of brute-force attack: 36 assets affected
- Signs of Trojan Activity: 28 assets affected
- Suspicious activity. Unauthorized comm. 121 assets Affected
- There are 38 open vulnerabilities
- Unknown host detected by ARP (34-11-56-78-9A-BC)

Device by Security state

416

Critical	121
Warning	206
Normal	89

Top application by number of events

le_really.pdf.exe	32
W_PCAP	27
SCADA_2000	14
LsaSS	7
MySQL	2

PLC02-TM02 ✓ Normal

Device ID	9
Impact	Business-critical

Addresses

Network Interface 1

MAC address	00:50:56:ba:1f90
IP	10.22.91.32

Settings

Router	No
Status	Authorized

Hardware

Vendor	Siemens
Model	SIMATIC S7-1500
Version	6ES7 511-1AK00-0AB0

Software

Vendor	Siemens
Name	SIMATIC S7-1500
Version	V1.8.5
Risks	Insecure network architecture

Dynamic fileds

Chassis ID	plc
CPU	CPU1511-1 PN
Hardware version	2
Port ID	port-001

Kaspersky Industrial CyberSecurity for Nodes

KICS for Nodes was specifically designed for the harsh requirements of distributed automation systems: mixed and complicated environments, extended time in operation, standalone and connected use cases, attended and maintenance-free instances and priority of control availability at all costs

Benefits

Low impact
on protected device for best system performance

Compatible
with low-performance computers from previous generations, and systems from Windows XP SP2 and Windows Server 2003 SP1 and above

Extended lifecycle
up to 5 years licensing and extended support

Full functionality
for all MS Desktop, Server and Embedded Windows OS

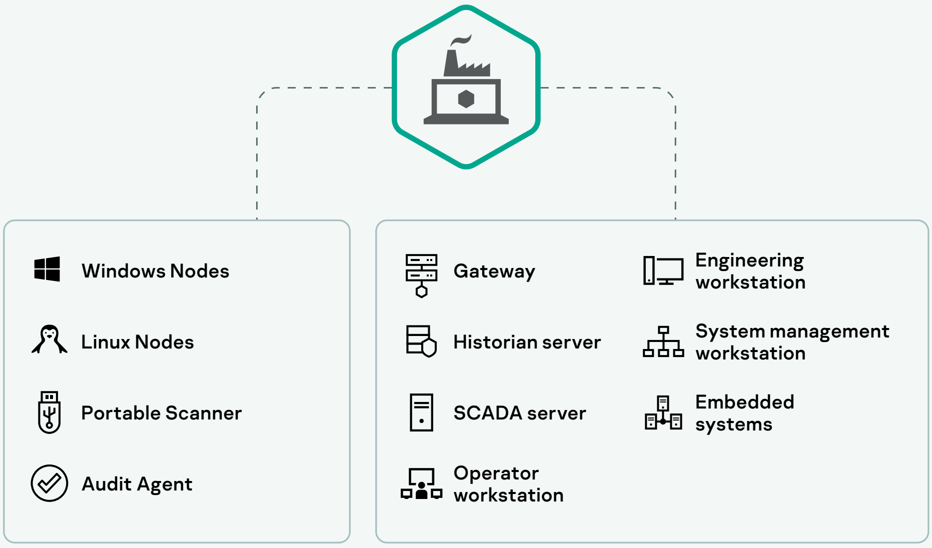
Modular deployment
Flexible options and safe non-intrusive settings

Covers mixed infrastructures
Windows, Linux and Portable variants

Industrial-grade, tested and certified Endpoint Protection, Detection and Response. A low-impact, compatible and stable solution for Linux, Windows and standalone systems.

Industrial Endpoint Protection, Detection and Response

Protects every endpoint of a modern, digital, managed and distributed automation system. It reveals new levels of incident visibility in the root cause analysis process. The agent collects the endpoint telemetry to create a clear and detailed visual representation of an incident's progress on workstations, servers, gateways and other endpoints, reassuring automation system administrators that an incident has been fully dealt with and won't happen again.



Windows Nodes

Linux Nodes

Portable Scanner

Audit Agent

Gateway

Engineering workstation

Historian server

System management workstation

SCADA server

Embedded systems

Operator workstation

KICS for Nodes Portable Scanner
Enforces a cybersecurity policy on standalone machinery, automation systems or equipment on which security software cannot be installed. Ultimate situational awareness and OT-visibility even from a standalone infrastructure.

Installation-free solution
KICS for Nodes can be activated on a number of additional Portable Scanner flash drives. This helps to perform simultaneous on-demand scans on multiple machines during maintenance windows, to collect endpoint data and organize it into a convenient summary report.

Regulatory and internal policy compliance
KICS for Nodes Portable Scanner conducts anti-malware compliance checks of equipment accessing an OT site, including computers of third-party contractors. It has a very low operational footprint and does not interfere with existing security solutions.

Kaspersky Single Management Platform

Benefits

- Situational awareness
- Systems / policy management
- Kill-chain and response
- Reporting and notification
- SIEM integration
- HMI / MES integration

The Single Management Platform is a centralized security management solution for security orchestration of the entire OT infrastructure, with a map of all geographically distributed assets enriched with events, incident analytics and more. It boosts the efficiency of mixed OT and IT security teams. A place where all your security controls work in harmony, enabling a rapid and precise response.

Expert services

Our suite of services forms an important part of the KICS portfolio. We provide the full cycle of security services, from industrial cybersecurity assessments to incident response.

Industrial Cybersecurity Assessment

Industrial Cybersecurity Assessment: Kaspersky provides a minimally invasive industrial cybersecurity assessment, including external and internal penetration testing, OT security assessment and automation solution security assessment. Kaspersky experts provide significant insights into a company’s infrastructure and recommendations on how to strengthen the ICS cybersecurity posture.

Threat Intelligence

Up-to-date analytics collected by Kaspersky experts help enhance the customer’s protection from targeted industrial cyberattacks. Delivered as TI feeds or tailored reports, they meet specific customer needs according to regional, industry and ICS software parameters.

Incident Response

In case of incident, Kaspersky experts collect and analyze data and malware, reconstruct the incident timeline, determine possible sources and motivation, and develop a detailed remediation plan. Plan include recommendations on removing malware from customer’s systems and rolling back its malicious actions.

> Their experience in the ICS cybersecurity domain, professionalism and the complexity of their solution, in comparison with other suppliers, has given us great value and ensured a bright future for our company’s security strategy.
>
> Ondřej Sýkora,
> C&A manager, Plzeňský Prazdroj

> By undertaking the exercise and learning from the Kaspersky team’s knowledge, we have increased our protection against cyber security threats.
>
> Yu Tat Ming,
> CEO, PacificLight

Training and awareness

Industrial cybersecurity awareness training

On-site and online interactive training and cybersafety games for employees who work with industrial computerized systems and their managers. Participants gain new insights into the current threat landscape and the attack vectors specifically targeting industrial environments, explore practical scenarios and acquire cybersafe skills.

Expert training programs

ICS Penetration Testing and ICS Digital Forensics training courses are aimed at cybersecurity professionals. Participants gain all the advanced skills needed to conduct comprehensive pentests or digital forensics in industrial environments.

> Kaspersky was the best possible company to deliver professional industrial cybersecurity skills training for our ICS group.
>
> Søren Egede Knudsen,
> Chief Technical Officer

Specialized solutions ecosystem

Kaspersky IoT Infrastructure Security

Protects the Internet of Things at gateway level based on Kaspersky's Cyber Immunity approach

Learn more

Kaspersky Antidrone

Protects airspace from drones at facilities of any size

Learn more

Kaspersky Secure Remote Workspace

Functional thin client infrastructure with Cyber Immunity

Learn more

Kaspersky Machine Learning for Anomaly Detection

MLAD

Early anomaly detection system in industrial technological processes

Learn more

Kaspersky Industrial CyberSecurity

Learn more

www.kaspersky.com