An Extended Detection and Response (XDR) platform for comprehensive security of industrial enterprises.

Kaspersky Industrial CyberSecurity

kaspersky BRING ON THE FUTURE

Attacked by malware

In Q1 2024, a total of 30 cybersecurity incidents were publicly confirmed by the affected organizations or responsible officials, with the manufacturing sector accounting for 64,5% of those incidents.

Kaspersky ICS CERT, June 2024

Learn more

Industrial threat landscape

The new reality for owners and operators of industrial infrastructures is shaped by factors including hacktivists' growing interest in automation systems, high regulatory requirements, IT-OT convergence, and the rise of cyberattack variety in the industrial sector (in Q1 2024, Kaspersky's solutions blocked malware from 10,865 different families on industrial automation systems).

The proliferation of digital technologies, which is usually seen as a good thing, erases the gap between IT and OT environments that used to protect the latter from cybercriminals. While the single flash drive brought into the ICS environment can seriously affect a company's core business, a motivated hacking group can penetrate OT networks, cause considerable damage, and/or steal valuable information. Combined with the automation standards evolving from common recommendations to legislative requirements and the increasing need to share best practices as well as manage risks, this makes the cybersecurity of industrial enterprises a formidable challenge.

Kaspersky ICS CERT expects organizations from the following industries to face cyberattacks with increasing frequency:

Oil, Gas, and Chemical

Digitalization of exploration, extraction, transportation, and refining — a key competitive factor for these companies — implies integrating IIoT, Drones, and Robots, deploying 5G, blockchain, and VR solutions which broadens the landscape for malicious actions.

Critical Manufacturing

Seeking to improve cost-effectiveness, these enterprises deploy cutting-edge technologies, expand connectivity, tap into the cloud, and explore IT-OT convergence scenarios, all increasing exposure to brand-new and ever-changing threats.

Minerals, Metals and Mining

A cornerstone for critical and nationally important manufacturing, the industry has to balance expenses while introducing automation and digital technologies. Being a tidbit for both hacktivists and high-potential attackers, it cannot compromise on cybersecurity.

Power, Grid, and Utilities

Digital and emerging tech are vital to driving energy transition while maintaining legacy infrastructure, which is still the backbone of most energy facilities. Yet, they are the greatest risk, demanding extra cybersecurity efforts.

Attacks on industrial systems, particularly ICS and SCADA, are on the rise. Meanwhile, today's cyberthreats aimed at industrial environments appear to be resistant to conventional solutions. Against this backdrop, Kaspersky offers a comprehensive approach for these industries. Explore our customer success stories, threat landscape insights, and dedicated scenario-specific offerings on our website.

Choosing a partner you can trust, with a deep knowledge of the overlaps between industrial and corporate cybersecurity and the capacity to provide a full range of cutting-edge security technologies, has never been more important.

The primary targets of APT attacks will include:

Critical infrastructure owners and operators

Strategically important organizations from the Oil and Gas, Chemical, Energy, and Utilities sectors face considerably greater potential consequences from operational interference

Critical manufacturing

From single plant to nationwide or international scale, these companies, including those from the Metals and Mining, Agriculture, and global manufacturing industries, engage in high-risk operations involving significant incident costs

Learn more about APT and financial attacks on industrial enterprises during early 2024

Learn more

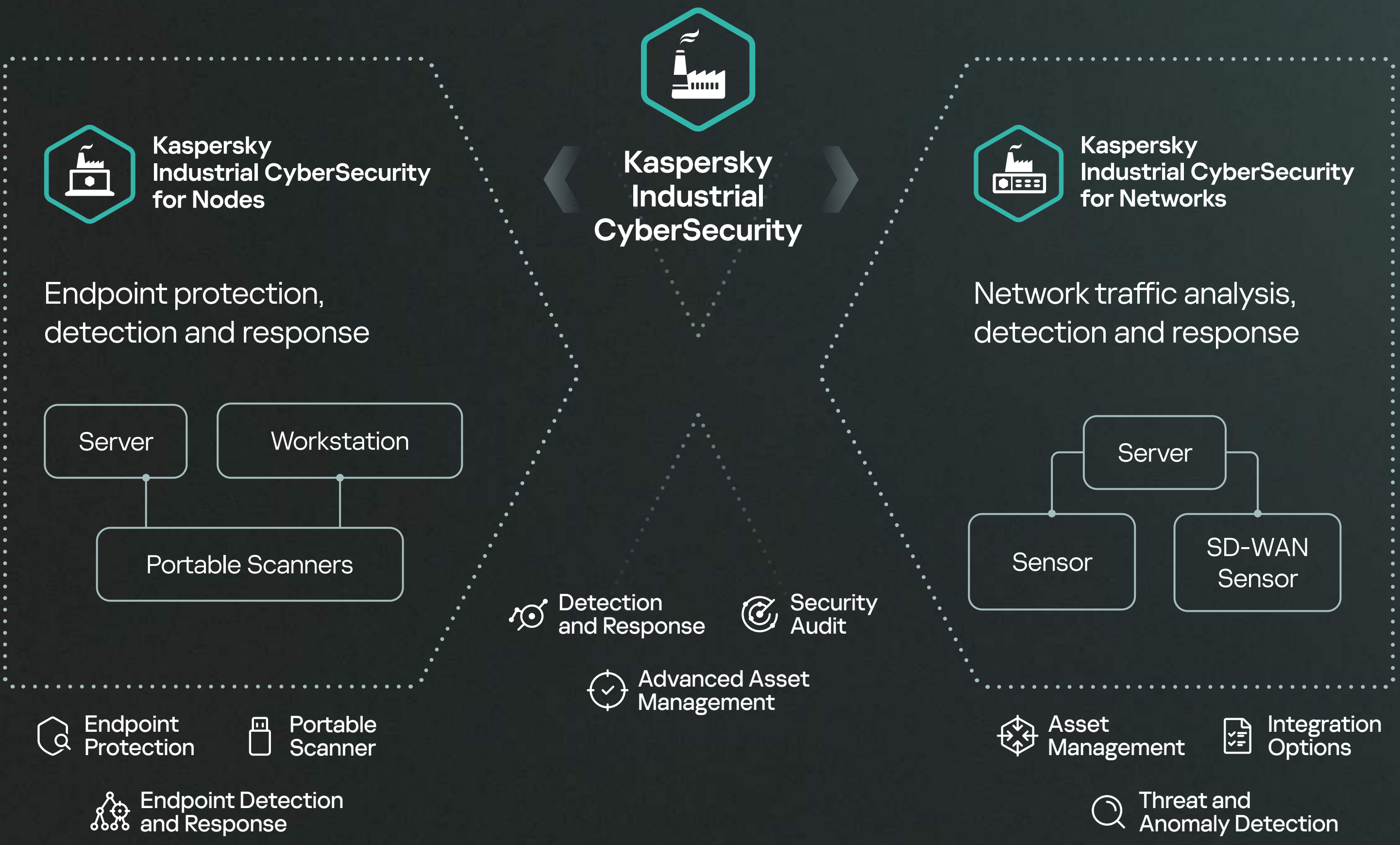
Advanced ICS security technologies

The gap between IT and OT environments that used to protect the latter from cybercriminals keeps becoming increasingly narrow, which is why a comprehensive enterprise-grade single-vendor security solution to safeguard critical infrastructure is now a must-have for owners and operators of Cyber-Physical systems. **Kaspersky Industrial CyberSecurity (KICS)** native XDR platform comprising KICS for Networks and KICS for Nodes components protects industrial automation systems and networks.

KICS for Networks is a traffic analysis, detection and response product that offers industrial network monitoring, intrusion detection, and risk management while also featuring a centralized audit of industrial network nodes for vulnerabilities and compliance with industry standards. **KICS for Nodes** offers industrial-grade endpoint protection, detection and response with OVAL*-based compliance auditing. This modular, low-impact solution is compatible with Linux, Windows, legacy, standalone systems, and PLCs. The Portable Scanner version protects standalone machinery and contractor devices installation-free.

Combined, these components form the KICS XDR platform that offers centralized asset inventory, risk management, and audit, enabling security scalability across diverse, distributed infrastructure via a single platform with a comprehensive graph of incidents, analytics, and more.

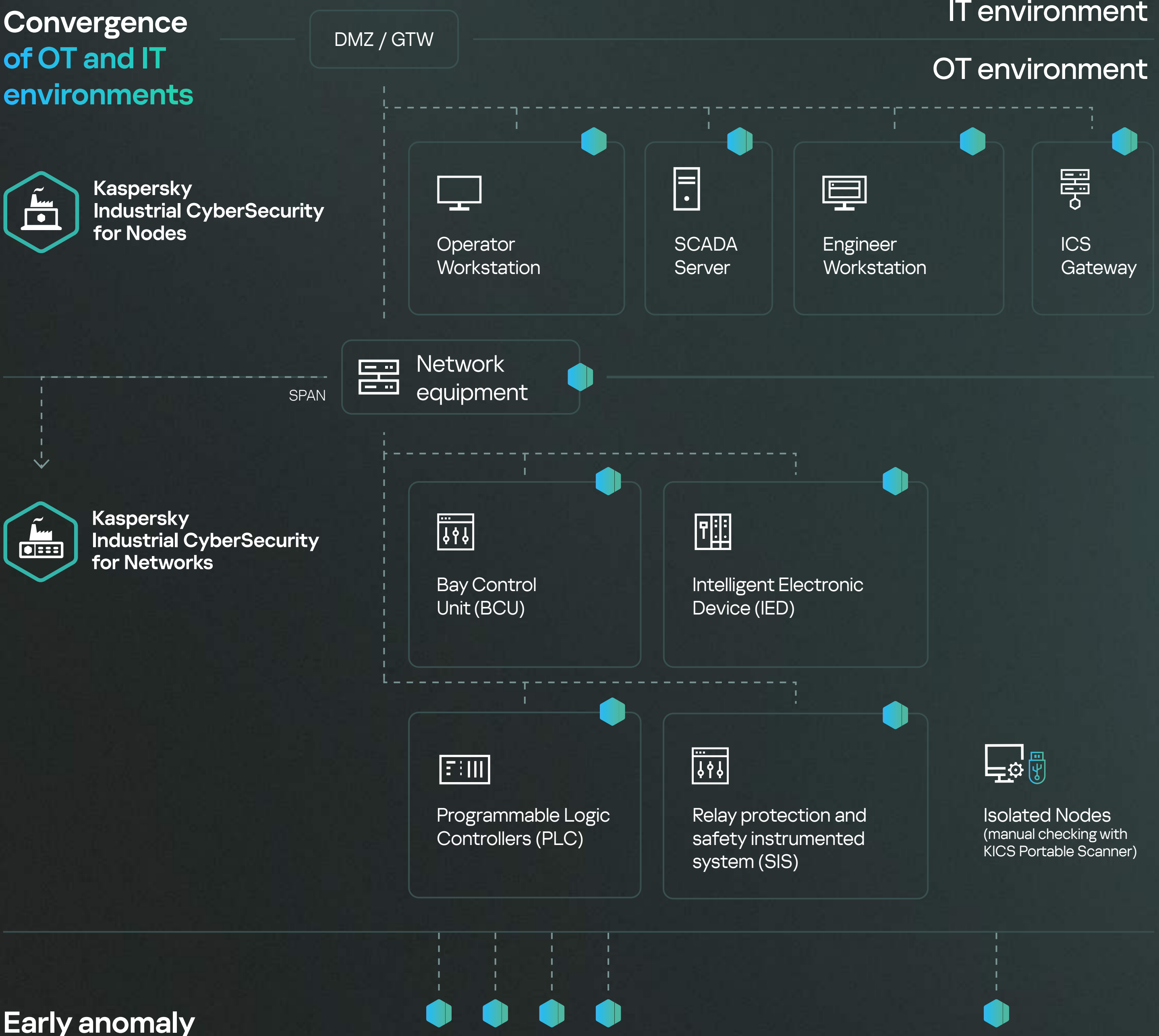
The KICS XDR platform enables users to see the bigger picture and broader context: the chain of incidents on network and endpoint levels, precise asset parameters, network communication and topology maps even from segments where traffic mirroring is not yet available, and more.


Kaspersky Industrial CyberSecurity for Nodes
Endpoint protection, detection and response
Server
Workstation
Portable Scanners
Endpoint Protection
Portable Scanner
Endpoint Detection and Response
Kaspersky Industrial CyberSecurity
Detection and Response
Security Audit
Advanced Asset Management
Kaspersky Industrial CyberSecurity for Networks
Network traffic analysis, detection and response
Server
Sensor
SD-WAN Sensor
Asset Management
Integration Options
Threat and Anomaly Detection

* Open Vulnerability and Assessment Language (OVAL)

Platform Application Points

Convergence of OT and IT environments


DMZ / GTW
IT environment
OT environment
Operator Workstation
SCADA Server
Engineer Workstation
ICS Gateway
Network equipment
SPAN
Bay Control Unit (BCU)
Intelligent Electronic Device (IED)
Programmable Logic Controllers (PLC)
Relay protection and safety instrumented system (SIS)
Isolated Nodes
(manual checking with KICS Portable Scanner)

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Networks

Physical Level

Early anomaly detection and predictive analytics

Kaspersky Machine Learning for Anomaly Detection (Kaspersky MLAD) is an innovative system that uses a neural network to simultaneously monitor a wide range of telemetry data. It detects equipment faults and human error, helping to prevent failure and accidents, identifies atypical employee actions or equipment operations as signs of a specialized attack or sabotage, and combines anomaly detection with predictive analysis of equipment condition and life cycle.

Learn more

⬢ Protected by Kaspersky products

Kaspersky Industrial CyberSecurity for Networks

KICS for Networks

Industrial network monitoring and traffic analysis solution. Enables a Deep Packet Inspection (DPI) of the proprietary industrial protocols. Shipped as software or virtual appliance.

KICS for Networks identifies anomalies and intrusions in the ICS at an early stage, shows how the attack develops over the network and in the nodes (EDR kill chain and telemetry), and ensures the necessary actions are taken to prevent any negative impact on industrial processes.

Asset management

Asset discovery

Gain insights into your assets with a vulnerability database, risk prioritization, and safe active polling

Network visibility

Monitor traffic, form topology maps, and track network posture over time for ultimate visibility

Traffic analysis toolset

Track and analyze network sessions, enabling detailed traffic data export and storage

Advantages

- Specialized for industrial applications and protocols. Out of the box support for a wide range of OT protocols, devices, and network attacks + allows import from external projects
- Preset rules for security audit configuration
- User-friendly interface and customizable reports
- Complete risk awareness across distributed infrastructure
- Ingests traffic samples from multiple sources: own network sensors, SD-WAN sensors, endpoint sensors, and portable probes

Ecosystem and integrations

Ecosystem

Unlock the extensive capabilities of Kaspersky's ecosystem through integration with the following solutions and our unified cross-product cybersecurity approach:

- Kaspersky Next XDR Expert
Learn more

- Kaspersky IoT Secure Gateway (KISG)
Learn more

- Kaspersky Machine Learning for Anomaly Detection (MLAD)
Learn more

- Kaspersky Software-Defined Wide Area Network (SD-WAN)
Learn more

Manage all the elements of the ecosystem via a single console

Third-party integrations

Enjoy seamless compatibility with a multitude of external security tools and platforms

Threat and anomaly detection

Intrusion detection

Signature-based detection and a statistical engine that detects brute force or scanning attempts

Network integrity control

The system learns normal network interactions and alarms every deviation

Anomaly detection

Detects basic packet and protocol level anomalies. Could be enhanced with MLAD

DPI of industrial protocols

Upholds process and command control, and efficiently tracks telemetry data

Event correlation

Associates security events with the MITRE classification and a single kill chain

Kaspersky Industrial CyberSecurity for Nodes

KICS for Nodes

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

KICS for Nodes protects every endpoint in today's digital, managed and distributed automation systems. The solution collects 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.

Endpoint protection

Real-time threat prevention
Custom and on-demand scans for removable drives and critical areas to prevent exploits and protect files

Local activity control
Device and Wi-Fi control features. Ensure PLC project integrity for full local activity awareness

Network activity control
Manage host firewalls and block network sessions, ensuring protection from network threats

System monitoring
Verify file integrity, track registry access, detect threats in system logs to ensure the security of the OS

Endpoint detection and response

Detection
Scans for Indicators of Compromise (IoCs), comprehensive monitoring and reporting features

Response
Prevent execution, quarantine/delete files, start/terminate processes, isolate networks, and more

Windows Nodes

Portable Scanner

Linux Nodes

Audit Agent

Portable scanner

Malware scanner
Anti-malware scans of standalone equipment and all computers brought to the industrial site

OVAL scan
Enforce cybersecurity policy on standalone machines with manual vulnerability and compliance scans

Packet capturing
Capture and analyze network traffic to unlock ultimate awareness even for isolated infrastructure

Basic asset inventory
Collect comprehensive data on hardware and software using zero-footprint solution

Advantages

- Low impact on protected devices, tunable resource consumption
- Compatibility with legacy OS and industrial automation vendors
- Basic security configuration, as well as advanced options for protecting your hosts from any type of threat
- Modular deployment and non-intrusive settings
- PLC support: Siemens SIMATIC S7-300, S7-400, S7-400H, S7-1500, S7-1200, SIPROTEC 4; Schneider Electric Modicon M340, M580; CODESYS V3 devices; Fastwel CPM723-01
- Flexible licensing options, from 1 month to 5 years
- Verified and efficient configuration presets for the most popular ICS

Gateway

Historian server

SCADA server

Operator workstation

Embedded systems

System management workstation

Engineering workstation

KICS Platform and beyond

Unified cybersecurity across the industrial and corporate segments of your enterprise

Native OT XDR

Core components of Kaspersky Industrial Cybersecurity, KICS for Networks and KICS for Nodes are purpose-built to seamlessly work together within our ecosystem, enabling unified and cohesive experience. When purchased together, they form a native XDR Platform that offers additional valuable cross-product functionality.

Advanced asset management

Endpoint hardware inventory
Comprehensive visibility into all connected devices across your infrastructure, ensuring accurate asset tracking and enhancing security management

Applications, users, and patches inventory
Detailed insights into software deployments, user access, and patch status within your environment. Enriched data for proper management and reduced potential vulnerabilities

Endpoint traffic monitoring
Continuous monitoring of data flows at each endpoint to quickly detect unusual patterns or potential threats, ensuring prompt response to suspicious activity

Security audit

Vulnerability scan
Thoroughly scan your assets to assess security weaknesses, enhance risk awareness, enable timely response, and strengthen your security posture overall

Compliance audit
Agent-based and agentless audit for compliance with OVAL and XCCDF* industry standards. A fully functional editor, centralized reports database, protected vault for node credentials, and more

Configuration control
Ensure secure asset configurations, track changes for security risks, and maintain baseline integrity for hardware and software assets

Detection and response

Detection
Enhanced and streamlined threat identification through host-network events correlation with a single kill chain view. Network alert data enrichment for deeper insights into incidents

Response
Robust threat mitigation through execution prevention, host isolation, and file quarantine. Seamless firewall integrations further enhance your ability to respond quickly and effectively to security incidents

Open OT XDR

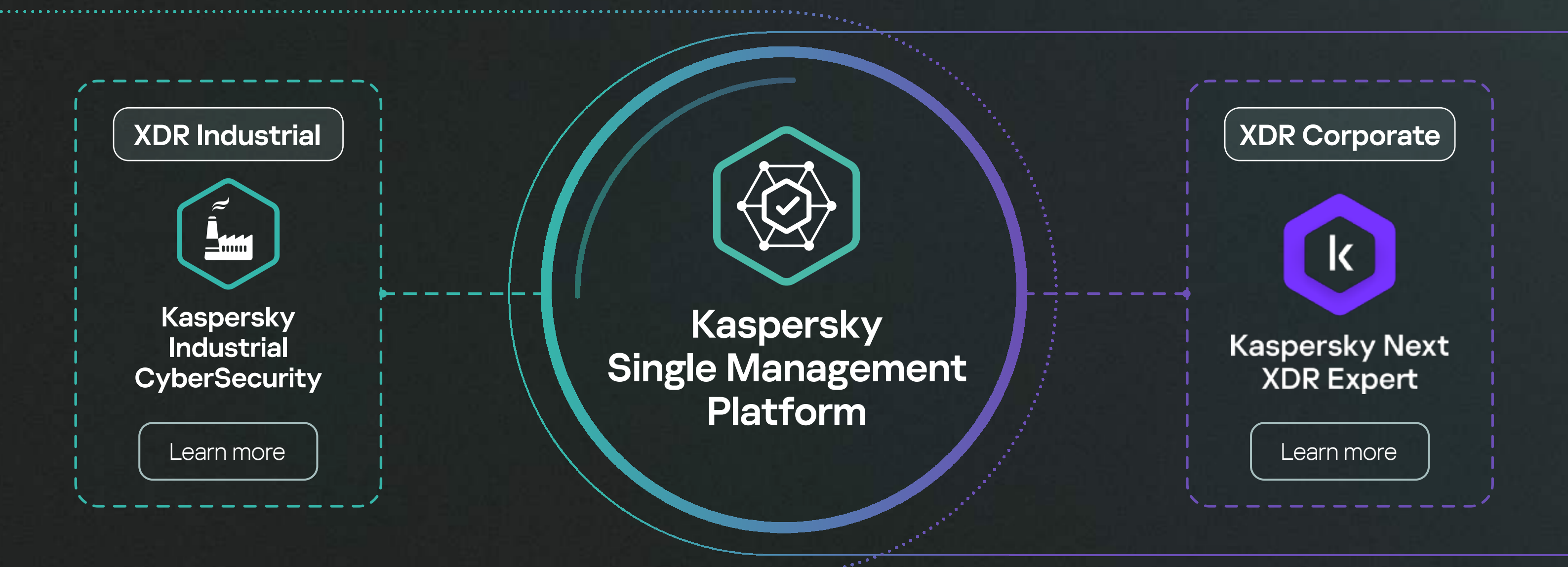
Extend the functionality of your EDR solutions with a correlation engine, automated responses, and third-party connectors — augment your KICS Platform with the Kaspersky XDR Core solution to unlock:

- Comprehensive monitoring and correlation of information security events (SIEM), integration with various systems
- Threat Intelligence enrichment and management

Single IT-OT XDR

Go beyond and embrace the ultimate IT-OT convergence. Combine your KICS Platform with our Kaspersky Next XDR Expert package — leverage Kaspersky's best-in-class endpoint protection functionality and reap the benefits of the following features:

- A single investigation graph, playbooks, and incident management by Kaspersky Single Management Platform
- Complex protection for IT infrastructure (IT XDR)



XDR Industrial

Kaspersky Industrial CyberSecurity

Learn more

Kaspersky Single Management Platform

XDR Corporate

Kaspersky Next XDR Expert

Learn more

* Extensible Configuration Checklist Description Format (XCCDF)

27 years of world-class experience and petabytes of threat data

ICS CERT

ICS CERT — own international OT / IoT security research division

Proven expertise in the IT/OT security industry with numerous awards and achievements

Over 200 certificates of compatibility with automation vendors' solutions

Proven technology effectiveness, compliance with standards and requirements

Customers around the world

ROSATOM NORNICKEL EUROCHEM

NLMK TATNEFT ROSSETI Wintershine

alperia PacificLight КазМунайГаз AGC

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Networks

Learn more

www.kaspersky.com

#kaspersky
#bringonthefuture