2021

Kaspersky Industrial CyberSecurity: What’s new?

kaspersky

BRING ON
THE FUTURE

Kaspersky Industrial CyberSecurity

A lack of visibility and manageability of complex IT and OT environments appears to be the most challenging issue for two-thirds of industrial companies, according to a Kaspersky survey[1]. Having access to a unified platform for the management of security policies, deployment of protection and all security events should help these organizations make their infrastructure more secure and transparent.

Kaspersky Industrial CyberSecurity (KICS) offers a centralized management dashboard for security orchestration of the entire OT infrastructure, with a map of all geographically distributed assets enriched with events, incident analytics and more. Deep integration of Kaspersky Industrial CyberSecurity for Nodes and Kaspersky Industrial CyberSecurity for Networks combines data about events on endpoints and across the network in real-time.

Centralized cybersecurity management
Centralized management of industrial assets for large and geographically distributed enterprises

Visibility across entire OT infrastructure
Combining data about events on endpoints and across the network in real-time

Continuous Vulnerability Management
Allows to continuously acquire, assess and take action on new information in order to identify and remediate vulnerabilities

How does it work?

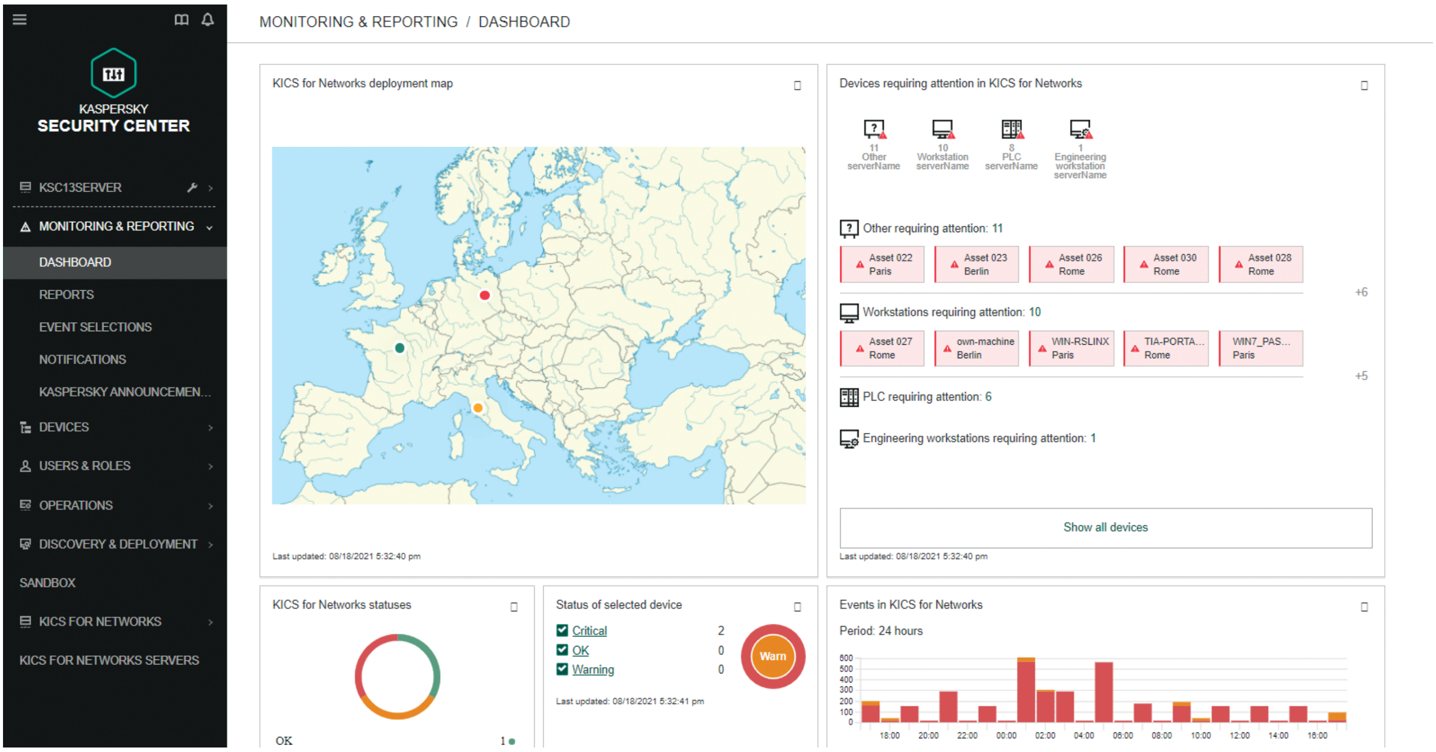
Kaspersky Security Center now provides complete visibility of all protected assets, security events and incident analytics. Customers can search for all infrastructure elements – such as servers or controllers – and their characteristics and see them on a geographic map where all assets across different subsidiaries can be set up. The map works in real-time and highlights any assets which might be affected by an incident. An administrator can then immediately investigate the problem by clicking on it and going to the dedicated web console of the server.

KICS for Networks can now retrieve important data from industrial endpoints protected with KICS for Nodes to improve customer experience, situational awareness and deployment flexibility. Security administrators can investigate accidents with a broad context: EPP-enriched incident details, precise asset parameters detection, and network communication maps from segments where traffic mirroring is not yet available.

Moreover, with the addition of a network attack blocker, Kaspersky Industrial CyberSecurity for Nodes protects against port scanning, denial of service and brute force attacks and threats exploiting vulnerabilities or misconfigured applications, services, and operating systems. To help customers further decrease the chance of a vulnerability exploitation with timely patching or mitigation, Kaspersky Industrial CyberSecurity for Networks has now expanded the vulnerability database provided by Kaspersky ICS-CERT with new sources: National Vulnerability Database (NVD), and US-CERT. Administrators can filter vulnerabilities by source and switch off detection from any of the databases.

[1] A role-based approach to overcoming this year's challenges, 2021, Kaspersky

KSC-based centralized management console interface



KICS for Networks deployment map

Last updated: 08/18/2021 5:32:40 pm

Devices requiring attention in KICS for Networks

Other requiring attention: 11

Workstations requiring attention: 10

PLC requiring attention: 6

Engineering workstations requiring attention: 1

Last updated: 08/18/2021 5:32:40 pm

KICS for Networks statuses

Status of selected device

☑ Critical 2
☑ OK 0
☑ Warning 0

Last updated: 08/18/2021 5:32:41 pm

Events in KICS for Networks

Period: 24 hours

KICS for Networks 3.1. New features

1. KSC-based centralized management console for KICS for Networks servers

Feature	Description
Dashboard for monitoring KICS servers	Widget with a list of connected servers and their status Widget with analytics on all server assets Widget with a list of recent events from servers Widget with a mini-map that displays servers and their statuses
Special items of the main KSC menu for KICS	Search across all servers, events and assets Geo map with servers and their security status
A separate selection of managed devices	The ability to create a separate selection of managed devices with KICS for Nodes and KICS for Networks
Role-based access	Users can get administrator or operator rights

2. Integration with KICS for Nodes

Feature	Description
Defining attributes of a protected host	Hostname, domain, OC, MAC, network interfaces (name, MAC, IP, subnet mask)
Determining the availability of a solution	Determining the availability and status of KICS Nodes, licenses, database versions
Relationship of the network interface to the host	Determining whether the network interface belongs to the host
KICS for Nodes triggers	Collecting KICS for Nodes triggers and displaying them in the list of KICS for Networks events Accounting for these events when calculating the device security status
Nodes communication map	Building nodes communication map with an installed agent (only for TCP and UDP)

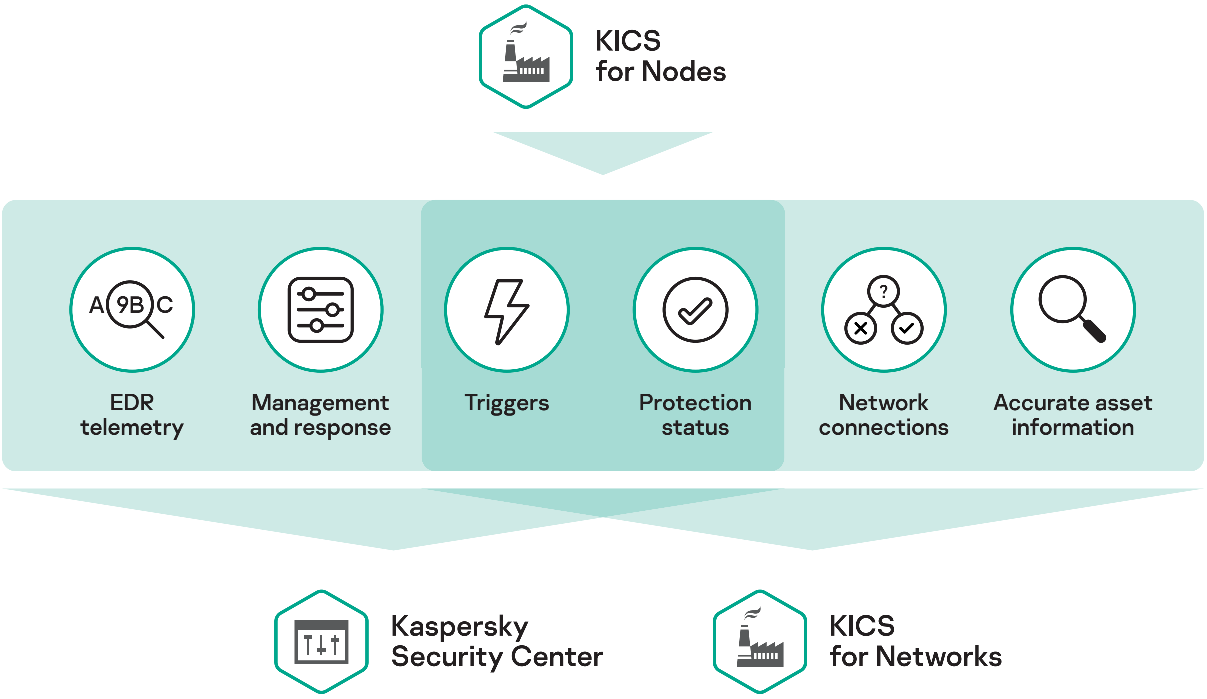
3. Vulnerabilities

Feature	Description
New vulnerability sources	Vulnerabilities from NVD, US-CERT will be added to the vulnerability database
Removing outdated vulnerabilities in Vulnerability Assessment	Removing outdated vulnerabilities with the remediated status that are not linked to assets
Improvements to the Vulnerability Assessment from ICS CERT	The ability to filter and sort vulnerabilities from different sources The ability to disable vulnerability detection from some sources (if there are many false positives)

KICS for Nodes 3.0. New features

Feature	Description
Support for the KSC web console	Plugin for managing KICS for Nodes from the KSC web console
Trusted zone templates for industrial software	For certain versions of industrial automation and control systems, the product offers pre-configured rule templates that can reduce the product configuration time
Support	Support for USB 3.1 (UAS) drives in Device Control Support for activation codes and subscription licenses
New security component of Network Attack Blocker (IDS)	Detects and protects against threats such as port scanning, DoS, brute force and intrusion attacks (attempts to remotely exploit vulnerable or misconfigured applications, services and operating systems to execute arbitrary code and implement unauthorized network activity)
Statistics mode	Device Control can work in statistics mode (no blocking, only notifying about the use of devices)
New message format	Improved format for transmitting messages from security components in KSC
New default product settings	The default product settings have been changed to simplify and speed up initial setup

Enriched data through product integration



www.kaspersky.com

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity is a portfolio of technologies and services designed to secure operational technology layers and elements of your organization - including SCADA servers, HMIs, engineering workstations, PLCs, network connections and even engineers - without impacting on operational continuity and the consistency of industrial process.

Learn more at www.kaspersky.com/ics