kaspersky BRING ON THE FUTURE

Kaspersky Industrial CyberSecurity for Networks 3.0

Recent Kaspersky research has shown that 44% of industrial organizations are working on cybersecurity initiatives for digital OT transformation[1]. These initiatives are essential, because 39% of industrial control systems' (ICS) computers were subjected to cyberattacks in 2020[2]. To ensure these attacks don't affect critical industrial processes, the protection should cover the entire heterogeneous OT environment, with diverse equipment and customized systems. It is also important to be aware of vulnerabilities in ICS software, to prevent them from being used for advanced threats, to reduce the attack surface and minimize possible consequences of a cybersecurity breach.

Enhanced functionality and vulnerability management

The new version of Kaspersky Industrial CyberSecurity for Networks flags vulnerabilities in equipment and gives recommendations for their mitigation in addition to operational technology (OT) traffic monitoring, which reveals unauthorized activity. Added support for the BACnet protocol allows the product to effectively protect smart building systems. Automated learning mode for traffic monitoring, seamless protocol updates, and the new web console also simplify management and improve efficiency in fighting industrial threats.

Kaspersky Industrial CyberSecurity for Networks enables vulnerability management to help customers learn about new weaknesses in their equipment and patch or mitigate them in time. The accurate and comprehensive details, such as CVE-ID, criticality, exploitation conditions, possible consequences and guidance for mitigation, are available in the product management console, so there is no need to inspect dedicated reports in multiple third-party sources that may not necessarily include all background information and practical recommendations. The data for Kaspersky Industrial CyberSecurity for Networks is prepared by Kaspersky Industrial Control Systems' Cyber Emergency Response Team (ICS CERT), a global project devoted to identifying potential and existing threats that target industrial automation systems and industrial IoT.

[1] The State of Industrial Cybersecurity 2020, September 2020, ARC Advisory Group

[2] Threat landscape for industrial automation systems. Statistics for H2 2020, 25 March 2021, Kaspersky ICS CERT

New features

1. Full-featured web console for interacting with the product

- ✓ Dashboard
  - Dashboard customization option;
  - Resource consumption monitoring on server and sensors (resource consumption).
- ✓ Deployment from web console: adding and managing sensors.
- ✓ Dark theme.
- ✓ Dashboard
  - Dashboard customization option;
  - Resource consumption monitoring on server and sensors (resource consumption).
- ✓ Deployment from web console: adding and managing sensors.
- ✓ Dark theme.
- ✓ Network map
  - Support for up to 100,000 nodes;
  - Visualization of security incidents on the network map;
  - Ability to automatically group assets on the map (by subnet, vendor or category).

2. Vulnerability management

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

3. Protocol support (DPI)

- ✓ Regularly updated DPI algorithms. Support for new protocols will now be added by updating the product databases.
- ✓ Support has been added for new industrial protocols: MICOM, Profinet, TASE.2, DirectLogic, BacNet.
- ✓ Enhanced recognition of existing protocols: IEC104, Rockwell EthernetIP, MOXA.
- ✓ Monitoring of process parameter values (tags) in real time. All tags identified during protocol parsing can be viewed simultaneously.
- ✓ Detection of problems in encrypted traffic (weak ciphers, self-signed certificates and certificates with invalid dates).

4. Asset management

- ✓ Support for a large number of assets (up to 100,000).
- ✓ Ability to specify a new parameter for an asset – a subnet, plus filtering by subnet.
- ✓ Support for SCADA project import. Updatable database of supported SCADA systems for import.

5. Improved learning mode

- ✓ Automated generation of process rules has been added. The learning process entails the product analyzing network traffic and generating process rules based on identified patterns.

6. Whitelisting

- ✓ Option to whitelist any event has been added.
- ✓ Ability to view asset properties when creating rules.
- ✓ Templates of popular rules.
- ✓ Adapted event creation for IT networks (generates fewer NIC alerts).

7. New REST API for automation of product operations

- ✓ Extended support for working with assets.
- ✓ Extended tag information support.
- ✓ Retrieval of identified vulnerabilities via API.

8. Ability to create images that include the product (for appliance)

9. New management of external connectors (API consumers)

- ✓ Extendible list of supported types without product reissue.
- ✓ Ability to store connector settings.
- ✓ Ability to display logos for connectors.

10. Ability to export and import product configurations and list of assets

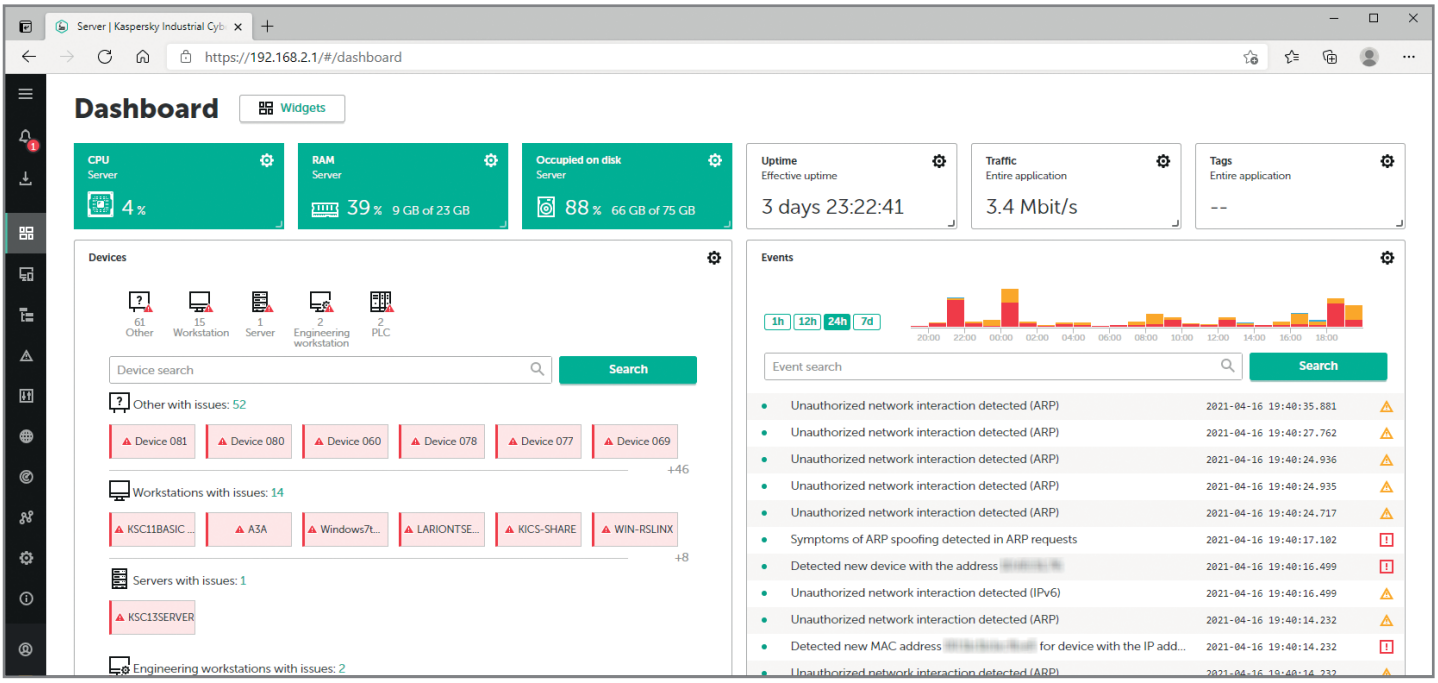
How it works

To ensure protection of diverse OT environments and devices, the platform enhances protocol support and adds new ones, such as MICOM, Profinet, TASE.2, DirectLogic, and BACnet, thanks to which, Kaspersky Industrial CyberSecurity for Networks can now be used for smart building automation system protection. The new protocols and DPI (deep packet inspection) algorithms for traffic inspection are being delivered seamlessly through automatic database updates.

In terms of incident prevention, the enhanced product significantly simplifies the task of rules creation to detect deviations in OT traffic. During the new learning mode, Kaspersky Industrial CyberSecurity for Networks analyses how the manufacturing process parameters (tags) change and automatically creates the rule for normal work of the equipment. This is so the IT security operator doesn't need to create them manually.

Kaspersky Industrial CyberSecurity also suggests numerous usability and manageability enhancements. A brand new web console offers extended incident visualization capabilities for more detailed threat analysis. Information about detected incidents is now mapped to MITRE ATT&CK for ICS attacks tactics and techniques, so security experts can have additional insights for attack investigation. In the web console, the administrator can quickly deploy the platform to new industrial equipment and add connectors to third-party systems, such as SIEM, firewalls or SCADA via REST API.

KICS for Networks interface



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