Kaspersky ICS CERT

kaspersky

Recommendations

05.02.2026

Version 1.0

Instead of an introduction

For many years, our team has been finding and analyzing vulnerabilities in industrial automation systems, hunting attacks on industrial enterprises, and investigating related incidents. Based on the results of each study, we prepare a set of recommendations – a list of measures and security controls that, if implemented correctly and fully by the affected organization, would protect it from the attack in question or at least significantly mitigate the resulting damage.

We found that we were increasingly writing recommendations that were very similar to, or even identical to, those written for previous attacks. This was because employees of the affected organizations were making the same mistakes, and the attackers were exploiting those mistakes in very similar ways.

We ultimately decided to compile our most frequently recommended security measures into a single list and publish it as a separate article. This list is by no means exhaustive, nor do we claim that it is the only correct or ideal one. Many of the proposed measures can be replaced with alternatives in specific cases, and some threats can be partially mitigated by measures not included in our list. The list is also not intended as an alternative to those measures recommended by government and industry regulators, international consortiums, and scientific institutes. When compiling it, we did not attempt to cover all threats, regardless of whether they were encountered in real attacks or hypothetical threats deemed technically feasible by experts. The measures we selected were based exclusively on our own experience. When examining the turning points in the development of each attack (how the initial penetration occurred, why it was possible to reach such a critical node, how privilege escalation was achieved, etc.), we asked ourselves two key questions: "What could the affected organization have done to prevent this from happening?" and "What measure would the organization have found most accessible and easiest to implement in this case?"

We will update this list as needed and reference it in our public articles and private reports to save time. We also believe it can be used as a standalone reference for selecting and planning protective measures, independent of any specific article or report.

Core cybersecurity measures

Baseline security controls and practices that help defend against diverse cyberthreats across multiple stages of an attack.

1. **Protect IT/OT endpoints with a comprehensive endpoint solution.**

   - OT hosts: use an industrial-grade solution such as Kaspersky Industrial CyberSecurity for Nodes on engineering workstations, human-machine interface (HMI) stations, and OT servers inside OT segments.
   - IT/DMZ/OT-adjacent hosts: use an enterprise-grade solution such as Kaspersky Endpoint Security for Business.

These solutions detect and block malicious documents, payloads delivered via phishing emails, and malicious scripts by providing on-access malware scanning, behavior-based blocking of suspicious activity, and application and device allowlisting to permit only trusted software and devices.

2. **Enhance network segmentation and limit internet access from OT.**

   - Configure the networks of different divisions (and different enterprises) as separate segments using VLAN technology.
   - Limit data transfers between network segments to only those ports and protocols necessary for the organization's workflows.
   - Enforce an access control list (ACL). Apply these controls on next-generation firewall (NGFW) solutions to restrict outbound connections from OT zones to approved destinations only. Regularly re-approve and document any required exceptions.
   - Monitor OT networks with passive industrial monitoring (e.g., using Kaspersky Industrial CyberSecurity for Networks) to detect and flag unauthorized internet-bound or VPN traffic.
   - Block unapproved VPN/hotspot applications, disable modems (including unauthorized USB devices), and isolate hosts violating these controls, for example, with Kaspersky Industrial CyberSecurity.
   - Where limited internet access is required, route it through an internet gateway security solution, such as Kaspersky Security for Internet Gateway, to apply centralized URL filtering and policy enforcement.
   - If remote access to systems in other network segments is needed, set up demilitarized zones (DMZs) for communication between network segments, and carry out remote access via terminal servers.

3. **Install current versions of operating systems and applications.**

   - Update Microsoft Windows and Unix-like operating systems to versions currently supported by their vendors.
   - Install the latest security updates (patches) for all operating systems and applications.
   - Pay particular attention to installing updates for hypervisors.
   - Update application software such as Microsoft Office and web browsers. Install all available types of updates: cumulative updates (CUs), service packs (SPs) and security updates (patches).
   - Pay particular attention to services that are accessible from the internet.

4. **Implement multi-factor authentication.**

   - Enable two-factor authentication (2FA) for logging in to the administration consoles and web interfaces of security solutions. In Kaspersky Security Center, for instance, this can be done manually.
   - Implement two-factor authentication for authorization (RDP, SSH or other protocols) on systems that contain confidential data and on systems critical to the organization's IT and OT infrastructure, such as domain controllers and SCADA servers.
   - Use two-factor authentication to log in to internet-accessible services, such as an email web interface.

5. **Strengthen password policies for operating systems and services.**

   - Require employees to use different passwords for different domains, services and systems.
   - Establish the following password complexity requirements in service and system policies:
     - Password length of at least 12 characters for unprivileged accounts and 16 characters for privileged accounts.
     - A password should contain uppercase and lowercase letters, digits, and special characters:
       (! @ # $ % ^ & * ( ) – _ + = ~ [ ] { } | \ : ; ‘ ” < > , . ? /)
     - A password should not contain dictionary words or personal data that could be used to crack the password, such as the user's name(s), telephone numbers, or memorable dates (birthdays, etc.);
     - A password should not contain sequential keyboard characters (“12345678”, “QWERTY”, etc.), or common abbreviations and terms (“USER”, “TEST”, “ADMIN”, etc.).
   - Passwords should be valid for no more than 90 days.

6. **Prohibit the storage and sending of passwords and other secrets (private keys, certificates and access tokens) in plain text.**

    - Use dedicated password management software to store and transfer passwords, keys, certificates etc.
    - Share master passwords for password databases when needed using a second communication channel, e.g., SMS or end-to-end encrypted chat messenger.
    - Delete messages containing secret phrases (passwords, keys, etc.).
    - Regularly search user computers and shared folders for files containing plaintext passwords by name and content.
    - Regularly check the source code of in-house developed systems and configuration files of IT and OT systems.

7. **Strengthen your domain security policies.**

    - Restrict the use of accounts with local administrator and domain administrator privileges.
    - Make it the responsibility of administrators to avoid using privileged accounts except when their duties can only be performed using them.
    - Use different dedicated accounts to administer different groups of systems, such as database servers, email servers, etc.
    - Restrict user access to the system. Check Active Directory policies: users should only be allowed to log in to the systems they need to perform their job responsibilities.
    - Implement a practice whereby regular users' domain accounts do not have local administrator rights. This will help reduce the risk of privilege escalation if such an account is compromised.

8. **Maintain offline, immutable backups of critical OT systems, and test restorability.**

    - Store backups on a separate server that is not part of the domain and limit deletion/modification rights to a dedicated non-domain account.
    - Increase backup frequency to minimize data loss.
    - Store at least three copies, keeping at least one on an autonomous device.
    - Use RAID arrays on backup servers to improve fault tolerance.

These measures are especially crucial for mitigating the risk of severe consequences of a ransomware attack.

9. **Manage security solutions.**

- Minimize the number of exceptions specified in security solution policies. Avoid using wildcard (*) exceptions; instead use exceptions for specific files or extensions.
- Configure security solutions to block the launch of remote administration utilities, except for those used by administrators. Both the Kaspersky Industrial CyberSecurity for Nodes and Networks products have the ability to detect remote administration tools used in OT environments (search for "Remote administration tools (RAT) execution" events).
- Check that all security solution components are enabled on all systems and that active policies prohibit the disabling of protection and the termination or removal of solution components without entering the administrator password.
- Check that security solutions receive up-to-date threat information from the Kaspersky Security Network for groups of systems where the use of cloud services is not prohibited by legislation or regulations.
- Make sure all devices are distributed into groups (no systems in the Unknown devices group), security solution license keys are distributed to all devices, and periodic system scanning tasks are created for all groups of devices.
- Segregate services for maintaining the organization's information security into a dedicated segment, and into a separate domain if possible.
- For Kaspersky security solutions, follow the Hardening Guide.

10. **Minimize the attack surface of OT endpoints.**

- Disable USB ports using operating system settings and BIOS/UEFI settings. Make exceptions only for authorized devices and use BadUSB protection, e.g., the Device Control module in Kaspersky Industrial CyberSecurity for Nodes.
- Use designated transfer points with dual control and tamper-evident logging for all inbound media. Scan files at a controlled station before they enter the OT environment. Retain logs and require two-person verification for exceptions.
- Allow only trusted applications to run in OT. You can use Kaspersky Industrial CyberSecurity for Nodes Application Launch Control for this purpose.
- Use network monitoring to detect noncompliant network activity and anomalies, such as connections to suspicious servers. A specialized OT

cybersecurity solution, such as Kaspersky Industrial CyberSecurity for Networks, can be used for this purpose.
- Configure the endpoint security solution to only allow connections to authorized web resources. For example, use Firewall Management in Kaspersky Industrial CyberSecurity for Nodes to create allowlist rules for permitted web servers. Alternatively, use the Web Control module in Kaspersky Industrial CyberSecurity for Linux Nodes.

11. **Strengthen email security and pre-delivery analysis to reduce your phishing attack surface.**

- Configure filtering of content sent via email and set up multi-tier filtering of incoming email traffic.
- Strengthen protection against spam and phishing emails at the internet gateway to block malicious messages before delivery (e.g., with Kaspersky Secure Mail Gateway).
- Detonate high-risk attachments before delivery and quarantine them based on verdict (e.g., with Kaspersky Anti Targeted Attack).
- Rescan delivered mailboxes for delayed activation of phishing URLs (e.g., using post-delivery rescans in Kaspersky Security for Mail Server).

12. **Educate employees.**

- Conduct simulated phishing exercises and explain the consequences of downloading/executing files from unverified sources.
- Train employees to securely use the internet, email, and other communication channels.
- For engineers and operators, conduct Kaspersky industrial cybersecurity awareness training.
- Conduct training on incident response in ICS for information security specialists.
- Develop instructions for responding to various types of incidents, or use our incident response handbook service.

13. **Deploy and use a SIEM system with focused correlation rules** (e.g., Kaspersky SIEM) and supplement it with the following correlation rules:

- Connection of a new USB mass-storage device to an OT endpoint.
- Creation of a scheduled task or startup item on an OT endpoint.
- RDP or SSH logon outside of working hours.
- Successful logon of a user with administrator rights on a new system.
- Clearing of Windows Event Logs or disabling of logging services.
- Endpoint security solution malware detections.
- Blocking access to malicious web resources with security solutions.

- Unapproved/unknown remote administration tool (RAT) usage.
- Creation of a new Windows service.
- Shutdown of security solution processes.
- Appearance of hidden users in the system.
- Tracking of PsExec utility launch events and similar events.
- Successful VPN logon to OT from an unapproved source network or without two-factor authentication (2FA).
- Logon attempt using an account that is locked out or disabled.
- Account lock due to multiple incorrect password entries.
- New user in a privileged group, e.g., a domain administrator.
- Execution attempts of an unauthorized application on an OT endpoint if allowlists are enabled.
- Outbound connection attempts from OT segments bypassing the approved proxy or NGFW.
- Outbound connection attempts to unknown external hosts from OT segments if allowlists are enabled.
- Mass connections to known ports on several systems (network scan).
- Huge amount of outbound traffic from OT segments.
- Mass DNS queries from OT segments.
- Unauthorized VPN connections originating from OT segments that are not permitted to use a VPN.
- A new device detected inside the OT network by Kaspersky Industrial CyberSecurity for Networks.
- Incorrect data packets detected by Kaspersky Industrial CyberSecurity for Networks.

Targeted security measures

Controls and recommendations crucial for protecting against particular types of cyberthreats.

14. **Deploy specialized solutions to protect against targeted attacks** (APTs/Hacktivists/Sophisticated cybercrime using advanced spyware and ransomware tooling and LOTL techniques).

    - Implement a comprehensive solution for detecting complex threats on endpoints and at the network level. This solution should include behavior analysis capabilities using a sandbox and incident response functionality. For example, Kaspersky Anti Targeted Attack could be deployed.
    - Use in-depth monitoring of application behavior on endpoints to promptly identify threats. A solution such as Kaspersky Next EDR Expert can be used for this purpose.
    - You can also delegate incident hunting and response tasks in your infrastructure to our experts by using the Kaspersky Managed Detection and Response service.
    - Keep track of changes in the threat landscape and adjust your cybersecurity measures to address new challenges by utilizing adequate threat intelligence sources, including Kaspersky Threat Intelligence Services.
    - Regularly check the login pages of your services that are available for remote access have not been modified with a malicious implant, and ensure that you are the only party controlling your companies' DNS zone.
    - Regularly monitor your remotely available service accounts to ensure they have not been compromised. Use dedicated threat intelligence services such as Kaspersky Digital Footprint Intelligence.
    - Reduce exposure to supply chain and trusted-partner attacks by: vetting critical vendors; enforcing minimum security requirements in contracts; limiting and segmenting partner access to what is necessary; and installing updates only via official channels while verifying digital signatures.

15. **BYOVD — focused measures** (APTs/Hacktivists/Sophisticated cybercrime).

    - Regularly review driver inventories, for example, with Kaspersky Industrial CyberSecurity for Nodes, to update or remove outdated vendor drivers.
    - Detect driver-abuse by monitoring system activity to identify attempts to load drivers or disable security tools using with their help. Use

EDR/XDR grade security solutions (such as Kaspersky Next XDR Expert). If internal capability is limited, use an MDR service (e.g., Kaspersky Managed Protection and Response) to provide 24/7 triage and response.
- Use a SIEM system with the following correlation rule**:** Installation of a new driver on the system.

16. **Securing virtual environments and focused measures against hypervisor-level attacks.**

- Isolate and harden the hypervisor management plane (separate management network, dedicated admin accounts with MFA, least privilege principle).
- Restrict and monitor access to virtualization consoles/APIs.
- Back up hypervisor configs/VM images with immutable/offline copies.
- For virtualized IT/DMZ workloads that support OT environments (VDI/jump servers/historians, etc.), consider using Kaspersky Security for Virtualization Light Agent for efficient VM protection.
- For endpoints directly involved in industrial control processes, prioritize Kaspersky Industrial CyberSecurity for Nodes over generic virtualization security tools.

17. **Legacy/out-of-date operating systems and focused measures using compensating controls.**

- Keep legacy/outdated operating systems (e.g., FreeBSD, old versions of Windows) in tightly controlled zones. Allow only the required protocols/peers, disable unused services, and enforce jump-server-only administration via a hardened and tightly monitored jump server.
- Where EDR isn't supported, add network-based monitoring (e.g., Kaspersky Industrial CyberSecurity for Networks), perform frequent integrity/log reviews, and rely on tested restore procedures (gold images and backups) rather than "in-place" patching.

18. **DLL hijacking – focused measures.**

- Use EDR/XDR grade security solutions to quickly detect and contain suspicious DLL loads. If internal capability is limited, use an MDR service (e.g., Kaspersky Managed Protection and Response) to provide 24/7 triage and response.
- Use the allow-listing features of endpoint protection solutions, such as Application Launch Control included in Kaspersky Industrial CyberSecurity for Nodes and Application Control in Kaspersky Endpoint Security for Windows, to monitor and block execution of executable

objects and DLL loads. Promptly investigate, while forwarding high-fidelity events to the SIEM for correlation and response.
- Apply DLL search hardening where supported by keeping or enabling Safe DLL Search.
- Preference should be given to running applications from read-only, vendor-controlled install paths.

19. Malware for AutoCAD — focused measures.

- Restrict AutoCAD from loading scripts or plug-ins outside approved directories, permit only vendor-signed components, and enforce application allow-listing and device control (e.g., Application Launch Control included in Kaspersky Industrial CyberSecurity for Nodes and Application Control in Kaspersky Endpoint Security for Windows).
- Inspect archives and attachments containing AutoCAD files before delivery, detonate risky email-borne CAD attachments and analyze unknown objects (e.g., using Kaspersky Anti Targeted Attack), and quarantine based on sandbox verdicts.
- Scan incoming CAD files at transfer points and endpoints before opening them (e.g., using Kaspersky Industrial CyberSecurity for Nodes on OT endpoints and Kaspersky Endpoint Security for Business on adjacent hosts and email gateways where applicable).
- Back up CAD repositories at regular intervals with offline copies, test restores and record outcomes.
- Keep Autodesk software up to date, verify hashes, and test in a staging zone prior to production rollout.
- Use a SIEM system with focused correlation rules**:**
  - Detection of malicious or suspicious verdicts on files with DWG/DXF extensions.
  - Execution of a previously unknown plug-in launched by AutoCAD.
  - Creation or modification of AutoCAD startup folders or macro directories.
  - Email attachments with DWG/DXF extensions quarantined by security solutions.
  - File access to CAD repositories followed by unexpected outbound connections.

20. Additional miners — focused measures.

- Deny access to known mining pools on perimeter security devices such as NGFW and adjacent hosts (e.g., using Kaspersky Endpoint Security for Business Web Control for domain/category blocks and monitoring of hits).
- Harden exposed services in DMZ/adjacent zones, audit and close unused services/ports, and monitor for sustained CPU/network anomalies, as well as unusual outbound connections.
- Detect and remove miners on OT endpoints (e.g., using Kaspersky Industrial CyberSecurity for Nodes); contain and remediate per incident.
- Use a SIEM system with focused correlation rules**:**
  - Sustained high CPU utilization by a process with an untrusted reputation.
  - Outbound connections to known mining pools or cryptocurrency protocols.

21. Additional ransomware — focused measures.

- Implement strong backup policies (see "Maintain offline, immutable backups of critical OT systems, and test restorability").
- Implement measures to protect against targeted attacks (see "Deploy specialized solutions to protect against targeted attacks").
- Implement measures to protect against BYOVD (see "BYOVD — focused measures").
- Implement measures to protect against DLL hijacking (see "DLL hijacking – focused measures").
- Implement protection of virtual environments (see "Securing virtual environments and focused measures against hypervisor-level attacks").
- Implement protection of legacy and outdated operating systems (see “Legacy/out-of-date operating systems and focused measures using compensating controls").
- Use a SIEM system with focused correlation rules (e.g., Kaspersky SIEM).
  - New logon or logoff script group policy.
  - New processes on several hosts.
  - Execution of tools or commands linked to shadow copy or backup deletion (vssadmin delete shadows, wmic shadowcopy delete, wbadmin delete catalog, etc.).
  - Mass file deletion, modification or renaming events within a short period across file shares.
  - Mass SMB connections.
  - Termination of backup agents, database services, web servers, etc.

- Detection of backup/snapshot deletion commands or snapshot API calls on backup infrastructure.
- Detection of executable or script deployment via SMB, PsExec, or WinRM to multiple hosts.
- Abnormal hypervisor management activity (new admin roles, unusual API calls, mass VM power-off/reconfig, mass snapshot create/delete).
- Legacy-zone anomalies (new inbound paths opened, unexpected outbound connections from legacy hosts, repeated auth failures, new remote admin services enabled).

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) is a global Kaspersky project aimed at coordinating the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the industrial internet of things.

Kaspersky ICS CERT ics-cert@kaspersky.com