



ICS vulnerability and threat intelligence

The problem

The shortage or absence of relevant data on current threats to industrial automation systems and vulnerabilities in industrial software and hardware leaves organizations without an adequate foundation for realistically assessing risks and implementing effective mitigation measures.

The solution

Access to the Kaspersky Threat Intelligence portal, which provides reliable and detailed information about attacks on industrial organizations, as well as vulnerabilities in the most popular ICS and other systems and components commonly used in industrial automation environments. This information helps make effective decisions regarding risk assessment and ensuring the organization's cybersecurity, both in current circumstances and as part of strategic planning.

Target audience

Information security departments of industrial enterprises, Managed Security Service Providers (MSSPs), Computer Emergency Response Teams (CERTs), Security Operations Centers (SOCs), Information Sharing and Analysis Centers (ISACs), national security projects, government regulators, vendors of industrial automation systems and cybersecurity services, and developers of products for protecting industrial control systems.

The security challenges

In a landscape where the level and diversity of cyberthreats are constantly on the rise, protecting an organization's information security and the continuity of its OT processes, proactively identifying potential exposure to emerging threats in the sector and region, and planning budgets appropriately – as well as detecting signs of probable compromise early on and effectively investigating cybersecurity incidents on ICS computers – can only be achieved by relying on verified threat data that includes the necessary technical details.

It is crucial to understand the goals and focus of attackers, along with their methods, tactics, techniques, and tools. In other words, to know who targets enterprises with a similar profile and how, what measures to implement to reduce the risk of a successful attack, and what to do first upon detecting signs of a breach.

Ensuring information security in enterprises often involves a number of challenges:

- Unidentified threats – industry-specific and regional, as well as cross-industry and cross-regional, and blind spots in the threat landscape.
- Ineffective threat hunting; difficulty in identifying real threats.
- Weak forecasting of OT risks: planning protection and long-term security investments based on guesswork.
- Inability to accurately measure and validate the effectiveness of cybersecurity investments; challenges in securing the budget.
- Mismatch between security drills or readiness checks and attackers' actual TTPs; overestimation of the security level.
- Delayed incident response, as the lack of context hinders decision-making and amplifies the consequences of incidents.

Minimizing the risks associated with the exploitation of vulnerabilities in ICS products and other systems and components commonly used in industrial automation environments, and, equally importantly, effectively prioritizing and allocating resources to eliminate these vulnerabilities, requires reliable information, which is crucial for determining the real consequences of a vulnerability's exploitation and deciding on proper measures to eliminate it. This includes complete information about the vulnerability itself and its real severity level (in practice, we often see vulnerabilities with zero severity, as well as those with underestimated severity levels), a list of actually vulnerable products, and actionable recommendations, including risk mitigation measures to be taken during the period before updates are installed or in cases where installing an update is impossible for some reason.

What we offer

Comprehensive information on vulnerabilities and threats to industrial automation systems.

Threat Intelligence

Threat reports containing information about APT groups, mass malware infections, and other campaigns targeting industrial organizations. This type of report serves several purposes: providing organizations with detailed information about threats that may affect their operations or those of their customers, and recommending measures to effectively prevent, detect, respond to, and investigate incidents. Additionally, such reports serve as a high-quality source of expertise for making long-term strategic cybersecurity decisions and raising the awareness and readiness of management and employees for potential attacks of varying structure and complexity.

A report includes:

- Executive summary with brief conclusions;
- Technical details: description of an attack's method and kill chain, tools used, and TTPs (tactics, techniques, and procedures);

- Data on the command-and-control (C2) infrastructure used by attackers to manage infected devices;
- Description of the threat actor behind the attack;
- Profile of affected organizations;
- Conclusions and detailed prevention and containment recommendations with SIEM correlation rules;
- Indicators of Compromise (hashes, IP addresses, URLs, domains) and YARA rules;
- MITRE ATT&CK matrix mapping.

Threat statistics for a range of regions and industries, describing the threat landscape for industrial automation environments over the past month. The purpose of such reports is to provide security specialists with important information about current industrial threat trends and systemic issues requiring special attention.

A report includes:

- Executive summary with key statistics and their changes;
- Regional overview containing statistics for the region as a whole, as well as statistics by country, threat type, and threat source; comparison of statistics for the current month against global figures, as well as year-over-year dynamics;
- Overview of threat statistics and their changes by industry: oil and gas, electric power, building automation, manufacturing, construction, biometrics, and engineering and ICS integrators;
- Recommendations on measures aimed both at reducing all threat statistics and at mitigating risks associated with specific threat types and attack vectors.

Monthly overviews of threats, attacks, and incidents related to industrial organizations worldwide and disclosed in the reporting month. The purpose of such reports is to provide organizations with up-to-date information on recent cyberthreats that could affect their operations, as well as data to identify signs of an attack within the organization and to take effective primary protection measures.

An overview includes:

- Executive summary with brief conclusions;
- Descriptions of cybersecurity incidents;
- Indicators of Compromise: hashes, IP addresses, URLs, domains, etc.

Early threat alerts enable organizations to quickly gear up their defenses before full threat and attack reports appear.

Vulnerability Intelligence

Analysis by the Kaspersky ICS CERT team of known vulnerabilities in ICS or related software and hardware, where existing assessments and recommendations are inaccurate. The main goal of such reports is to provide

organizations with accurate data on vulnerabilities, enabling informed assessment of cybersecurity risks and planning adequate measures to mitigate or accept them.

A report contains initial information from the vendor, an analysis of the reliability of this information by our experts, conclusions, a final assessment of the vulnerability, and actionable recommendations for remediation based on the vulnerability's real severity level identified during the analysis.

A report includes:

- Executive summary with key conclusions;
- Technical analysis: detailed description and validation of data obtained during the analysis, including specifics of affected products, as well as adjusted CVSS vector and rating;
- Conclusions;
- List of affected products and related updates, including products that are no longer supported;
- Risk mitigation measures: actionable recommendations from Kaspersky ICS CERT and the vendor, Suricata, OVAL;
- ICS MITRE ATT&CK matrix mapping.

Vulnerability alerts to prevent exploitation before official patches are released.

Vulnerability research reports on zero-day vulnerabilities in the most popular products and technologies used in OT environments and ICS, as well as the Industrial Internet of Things (IIoT) across various industries.

Advantages of Kaspersky Threat Intelligence reports and overviews

- **Verified facts only.** The information provided in the reports and overviews can serve as a foundation for risk assessment and for developing measures to mitigate and eliminate vulnerabilities.
- **Kaspersky ICS CERT.** Reports are prepared by a team of practitioners with extensive experience in ICS threat and vulnerability research and cybersecurity incident investigation.
- **Big telemetry data.** Threat research leverages proprietary telemetry data on threats blocked by Kaspersky security solutions on more than 3 million ICS computers worldwide.
- **Detailed vulnerability analysis by experts.** Through this analysis, we assist vendors in assessing vulnerabilities and selecting measures and approaches to eliminate and prevent them. We are guided by the principle of responsible disclosure and support the exchange of expertise.
- **Deep understanding of regional and industry specifics.** We identify regional and industry-specific threats and determine trends based on monthly, quarterly, and annual statistics.

- **Proprietary ICS vulnerability database.** Each record in the database is the result of meticulous analysis by Kaspersky ICS CERT experts.

What the customer gets

An effective tool for addressing operational and tactical, as well as strategic, cybersecurity issues

Detailed information on threats that can affect a specific organization, an entire sector, or several sectors, and on vulnerabilities in the software and hardware components of industrial systems is an effective tool that can and should be leveraged when addressing operational and tactical, as well as strategic, issues.

This tool helps to:

- Proactively manage OT risks – predict and prioritize threats and vulnerabilities more accurately based on reliable data;
- Protect critical assets and OT process continuity – identify and prevent known threats and thereby avoid downtime;
- Detect and respond faster – correlate suspicious activity in industrial environments with known campaigns and attacker TTPs, accelerating incident investigation and containment;
- Manage vulnerabilities meaningfully – make informed decisions, factoring in the assessment of the scale and severity of vulnerabilities: install updates, implement workarounds, or change configurations;
- Reduce the number and duration of incidents – and, consequently, reduce potential losses by decreasing unplanned downtime and lowering recovery costs;
- Demonstrate the organization's information security maturity level to its management, as well as regulators and insurers;
- Invest with real threats in mind – which makes it easier to justify budgets and CAPEX, and demonstrate the return on investment (ROI) in cybersecurity;
- Boost team readiness – develop realistic scenarios based on real-world attacks for red/blue/purple team exercises and effective coordination.

Start for free

We invite you to try the [Kaspersky Threat Intelligence](#) service in operation before making an informed decision about purchasing a subscription.

As part of the demo access, we provide about 10 sample reports covering attacks against industrial organizations, results of vulnerability research in industrial solutions, and threats relevant to industrial automation systems.

In addition, demo access enables you to evaluate the interface's information search capabilities, as well as the range and format of the data provided,

specifically Indicators of Compromise (IoC) and YARA rules, which can be downloaded and used in security solutions.

[Request demo access or consultation](#)

Related services

- Development of incident response handbook and training
- Analysis of known ICS vulnerabilities for critical information security decision-making
- ICS malware data feed
- Threat landscape analysis on request
- Ask the analyst

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