



Ask the analyst

The problem

Threat actors target industrial organizations using increasingly sophisticated techniques and tools. An organization's internal resources alone are not always enough to successfully counter complex attacks: an experienced cybersecurity team needs up-to-date information on threats that may not be publicly available, as well as support from external experts. In situations that call for decisive, rapid, and precise action, it is critical to get exclusive access to information and top-level expert support without delay.

The solution

A subscription to the Ask the analyst service. By subscribing, you can quickly obtain information on OT-related threats and vulnerabilities, as well as recommendations or expert advice from Kaspersky ICS CERT.

Target audience

Industrial organizations in various sectors, managed security service providers (MSSPs), security operations centers (SOCs), industrial control system (ICS) vendors, cyber emergency response teams (CERTs), and information sharing and analysis centers (ISACs).

The security challenges

The threat landscape is constantly evolving as threat actors continue to advance their technical skills and toolsets. Increasingly sophisticated techniques are used in attacks on industrial organizations. Cybersecurity incidents are ever more often the result of fileless attacks, non-malware attacks, or attacks leveraging legitimate tools, zero-day vulnerabilities and architectural security weaknesses of traditional IT and OT technologies, as well as complex attacks that combine multiple tactics. The consequences of a cyberattack against an industrial enterprise may include theft of confidential data, production downtime, and physical damage.

In this environment, the role of a competent cybersecurity team cannot be overstated. However, even experienced specialists are not always able to keep up with rapidly evolving threats on their own: they need highly specialized information and support from external experts. External expertise helps identify the most likely vectors of complex and targeted attacks and develop actionable recommendations to counter them effectively.

What we offer

The Ask the analyst service is an extension of Kaspersky ICS CERT's threat and vulnerability intelligence service portfolio. After subscribing to the service, you can turn to our experts for support and actionable information on specific threats and vulnerabilities. This enables you to tailor Kaspersky ICS CERT's powerful analytical capabilities and Kaspersky in-house automated analysis pipelines to your specific needs and enhance your cybersecurity system.

Key benefits

Expert support

You can reach out at any time for data or consultation to specialists with expertise in the relevant aspect of OT cybersecurity, eliminating the need to search for and hire scarce, highly specialized full-time professionals.

Faster, more accurate detection and response

Speed up threat detection and improve your response to threats and vulnerabilities to block identified attack vectors in line with recommendations from Kaspersky ICS CERT experts.

Efficient investigations

Prioritizing and effectively investigating incidents is much easier with personalized, in-depth contextual information about an identified threat.

Extending knowledge

You can increase your competence in vulnerability analysis, threat analysis, and incident response through interaction with Kaspersky ICS CERT experts, who are happy to share their knowledge and expertise by answering specific questions from our customers.

What the customer gets

The threat and vulnerability information they need, including insights that are not available from public sources, as well as personalized recommendations and consultations with Kaspersky ICS CERT experts.

Key capabilities

Requests related to ICS and other OT systems

- Detailed analysis of available information on known incidents and attacks;
- Additional information to complement published reports;

- Information on vulnerabilities in a product or a technology;
- OT threat landscape analysis and emerging trends relevant to your organization;
- Information on regulatory requirements and standards.

Malware analysis

- Analysis of malware related to OT environment;
- Mitigation and remediation recommendations.

Dark web intelligence*

- Dark web research for specific artifacts, IP addresses, domain names, filenames, email addresses, links, or images;
- Search for and analysis of information that may indicate information security incident risks for the customer.

Descriptions of threats and vulnerabilities, and related indicators of compromise

- General descriptions of specific malware families;
- Additional context for indicators of compromise (related hashes, URLs, command-and-control servers, geographical spread, affected industries and infrastructure types, etc.);
- Information on specific vulnerabilities (their actual severity assessment, list of effected product versions and configurations, specific mitigation recommendations from Kaspersky ICS CERT such as which mechanisms implemented in Kaspersky products protect against them, and other technical controls and security measures in case patching is not an option or the patch is ineffective).

Use cases

1. Clarifying information from previously published threat reports.
2. Obtaining additional information on indicators of compromise that have already been identified.
3. Obtaining unique vulnerability descriptions and recommendations on preventing vulnerability exploitation.
4. Gaining insights into activity on dark web resources that may pose a threat to the customer.
5. Obtaining an overview report on a specific malware family, including its capabilities and the potential impact of attacks involving that malware, as well as a detailed description of related activity known to Kaspersky.

* Already included in the [Kaspersky Digital Footprint Intelligence](#) subscription.

6. Achieving more effective prioritization of threat and/or incident alerts using detailed contextual information and categorization of related indicators of compromise.
7. Requesting assistance in determining the nature of suspicious activity (targeted attack or massive infection, assumptions about the attackers and their objectives).
8. Submitting malicious files for comprehensive analysis to understand the functionality of the samples provided.
9. Requesting and emerging threat landscape trends analysis related to your organization for tactical and long term cybersecurity adjustments planning.

[Request a consultation](#)

Related services

- Analytical reports on ICS threats and vulnerabilities on the Kaspersky Threat Intelligence Portal
- Analysis of known ICS vulnerabilities for critical information security decision-making
- ICS Vulnerability Data Feed
- Threat landscape analysis on request
- Incident response at industrial enterprises
- Digital forensics and incident response in ICS. Training
- Development of incident response handbook and training

[Request a consultation](#)

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