



Threat landscape analysis on request

The problem

Planning and organizing effective cybersecurity for any enterprise, industry, or country requires detailed knowledge of specific factors, such as the local features of the threat landscape, supply chain characteristics, and third-party networks. Familiarity with the current threat landscape is essential for successful incident response.

The solution

A threat landscape analysis conducted at the request of the customer, including current threats, attacks and vulnerabilities, as well as an analysis of relevant incidents.

Target audience

Cybersecurity teams in industrial enterprises, managed security service providers (MSSPs), computer emergency response teams (CERTs), and government regulatory bodies.

The security challenges

At Kaspersky, we have been observing the ICS threat landscape for years, and it is clear that there are identifiable regional and industry-specific characteristics. Even seemingly insignificant differences in numbers can reveal serious problems and security challenges that require focused analysis.

Differences in production cultures, general cultural traditions, legal requirements, business models, processes and procedures, technological infrastructure, and levels of security awareness among employees make enterprises vulnerable in different ways.

Supply chains and the structure of partnerships between enterprises and industries play an equally important role because they are another channel through which threats can spread.

In order to build an effective and secure shield, all organizations need to know and understand the threats that the enterprise, industry, country or wider region faces.

What we offer

Two types of tailored ICS threat intelligence reports, created individually for each customer: quarterly and annual. The reports differ in how data is gathered and analyzed, and serve different purposes. The quarterly report is useful for solving tactical problems, while the annual report is useful for strategic planning. Both reports contain recommendations for addressing current and potential threats.

Quarterly report: tactical outlook and recommendations

The quarterly report provides an overview of five to 10 of the most relevant threats of the quarter, along with detailed technical information on each threat. This helps detect and prevent current threats to critical assets, ensuring the continuity of technological processes.

Comparing any suspicious activity in an organization's systems with the findings of Kaspersky ICS CERT experts simplifies threat detection and enables immediate action.

This data helps organizations adjust their cybersecurity measures to effectively respond to the latest security threats and challenges.

Annual report: strategic outlook and recommendations

The annual report provides an in-depth analysis of current threats and vulnerabilities, as well as extensive recommendations for security decisions at all levels.

This data helps organizations make informed, strategic cybersecurity decisions. Deep analysis of relevant threats, trends and real-world incidents facilitates the design and implementation of cybersecurity policy changes that mitigate potential risks and ensure the safety and continuity of technological processes. This data also assists in creating a cybersecurity enhancement roadmap and planning cybersecurity investments.

How we work

The process

1. We help the customer identify the focus and timeframe of an investigation.
2. We collect data using automation and, for the annual report, manual methods.
3. All data is analyzed by Kaspersky ICS CERT experts who specialize in threats to industrial organizations.

4. We provide a report in PDF format with an analysis of threats and risks, as well as detailed recommendations.
5. For the annual report, Kaspersky ICS CERT experts provide comments and answer customer questions.

Information sources

Quarterly report

Kaspersky ICS CERT experts use data collected via [Kaspersky Security Network](#) (KSN) exclusively from OT/ICS systems protected by Kaspersky solutions worldwide. These systems include:

- SCADA server;
- Historian server;
- OPC gateway;
- Stationary engineer or operator workstation;
- Mobile engineer or operator workstation;
- Human-machine interface (HMI);
- Computers used by OT network administrators and OT/ICS software developers.

All received data is verified and enriched using various techniques and technologies, such as statistical analysis, analysis by Kaspersky expert systems (e.g., sandboxes, heuristics, similarity analysis, profiled behavior), comparisons against allowlists and manual analysis.

Annual report

During preparation of the report, Kaspersky ICS CERT experts use multiple sources to gather relevant data for a specific customer request based on geography, industry and/or infrastructure.

Incident and attack analysis is conducted using the following sources and methodology:

- Information collected through Kaspersky's own sources, such as telemetry data, automated analysis and manual in-house analysis;
- Incident response, analysis and investigation results*;
- Information obtained through collaboration and cooperation with local and international cybersecurity information-sharing systems, initiatives and groups, as well as affected organizations and product vendors, other cybersecurity organizations, independent security research teams, individuals and other third parties*;

*If not limited by Kaspersky's internal policies, NDAs, contract terms and conditions, or legislation.

- Information from the internet, publications and other public information sources, complemented by Kaspersky's ICS CERT expert analysis.

Vulnerability analysis is conducted using the following sources and methodology:

- Information from public sources, such as OT product vendor websites and public vulnerability databases, with subsequent verification and analysis;
- Results of Kaspersky's vulnerability research and responsible/coordinated vulnerability disclosure work**.

What the customer gets

In both cases, the customer gets a report in PDF format. Kaspersky experts will also comment on the annual report in person and answer customer questions.

The selection of a quarterly or annual report depends on customer needs.

- The quarterly report helps determine which important changes need to be made to information security tools.
- The annual report assists in developing a long-term cybersecurity strategy and updating its implementation methods.

The two report types complement each other, which is why many customers choose to receive both in order to gain a comprehensive understanding of the threat landscape.

**May only be used if the customer can prove a legitimate need to access this information, e.g., a licensed user of the specified product, with respect to the selected vendor vulnerability disclosure policy and relevant contract terms and conditions.

Key differences of the reports

	Quarterly report	Annual report
Focus	Tactical	Strategic
Format	Top 5-10 detected threats with basic technical analysis	Detailed information on relevant threats, attacks, incidents and vulnerabilities with analysis by experts
Threat landscape		
Registered targeted attacks	Only on selected infrastructure	All potentially relevant
Registered APTs	Only on selected infrastructure	All potentially relevant
Phishing and social engineering threats	Only on selected infrastructure	All potentially relevant
Malware, actor's tactics, techniques and procedures (TTP)	✓	✓
Top initial infection sources (attack vectors)	✓	✓
Indicators of compromise (IoCs)	✓	
Cyberattack methods		Most dangerous to potentially relevant
Latest cybersecurity incidents		All potentially relevant
Updates on past cybersecurity incidents		By prior arrangement
Vulnerability information on selected infrastructures including mitigation measures		✓

Data collection	Automated	Automated + manual
Sources of information		
Kaspersky	✓	✓
Third-party information		✓
Public sources		✓
Analysis	Automated + manual	Automated + manual
Recommendations from Kaspersky ICS CERT experts	✓	Recommendations to remediate current threats and to prevent similar attacks in future
Deliverables	PDF report plus IoCs	PDF report plus follow-up meeting or call depending on customer preference
Volume	3–10 pages	30–150 pages

Details

Quarterly report contents

- 1. Executive summary** describing the threat landscape and providing a statistical analysis of anonymized data on threats blocked by Kaspersky products on OT computers in the selected geography and industry during the reporting period, including:
 - General attack statistics compared to global and/or regional numbers;
 - Analysis of threat sources targeting OT infrastructure;
 - Threat landscape dynamics, including comparisons to previous reporting periods.
- 2. Threat landscape analysis** of five to 10 of the most dangerous and/or widespread campaigns or threat types that have affected IT infrastructure computers in specified industries and regions. Each type of threat is

accompanied by an analysis of the attackers' tactics, techniques and procedures (TTPs).

- Initial attack vectors used to penetrate the victim infrastructure;
 - Reconnaissance and propagation inside the victim infrastructure (if available);
 - Interaction with the attacker-controlled infrastructure: C&C, malware hosting, etc. (if applicable);
 - Key features/capabilities of the malicious toolset;
 - Attack objectives (if available);
 - Attribution (if available);
 - Potential impact on OT/ICS and process safety/continuity;
 - Most prevalent initial infection sources (attack vectors).
- 3. Indicators of compromise** (IoCs) for the malicious toolset, including hashes, URLs, YARA rules and STIX.
 - 4. Recommendations** for remediating current threats and preventing similar attacks in the future.

Annual report contents

- 1. Executive summary** enables top management to quickly evaluate the risks associated with the reported threats and, if necessary, compile a list of actionable points for planning and implementing risk mitigation strategies.
- 2. Customer-specific threat landscape** in line with specified preferences (industries, regions, period), as detected by Kaspersky on OT-related infrastructures and potentially affecting industrial control systems, including:
 - Targeted attacks and APTs that have affected the specified industrial infrastructures;
 - Top five to 10 most significant threats detected in industrial control systems, their potential impact, analysis of tactics, techniques and procedures (TTPs), recommended remediation measures;
 - Most prevalent initial infection sources (attack vectors);
 - Other factors that influenced the threat landscape for the specified infrastructures.

If an identified threat requires an urgent response from the customer, it will be reported to them promptly as an Early Alert containing the information available at that time.

- 3. Study of cyberattack methods** employed against specified targets (industries, geography), including those used in attacks on the specified OT infrastructures and those that could potentially be used against them.

4. **Overview of the latest cybersecurity incidents** that affected industrial infrastructures (both IT and OT systems) during the reporting period. Includes updates on past incidents if new information has come to light. Detailed information on incidents may include:
 - Date, time and location of incident;
 - Overview of targeted/affected infrastructures and information systems;
 - Overview of the incident;
 - Tactics, techniques and procedures (TTPs) used by the adversary;
 - Information on the cybersecurity state of the affected infrastructure at the time of the attack/incident (evaluation of the infrastructure's exposure to cyberthreats and the cybersecurity measures applied);
 - Overview of the motives and intentions of the adversary;
 - Level of attack sophistication and estimation of adversary capabilities and skills;
 - Problem areas highlighted by the incident and recommended measures to protect specified infrastructures from similar situations in the future.
5. **Overview of selected past cybersecurity incidents**, including the same information as in point 4 above.
6. **Detailed information on vulnerabilities** in OT products and technologies used in the specified infrastructures (and according to the product list explicitly specified by the customer) that were identified and/or fixed by vendors during the reporting period.

This information is provided as a set of vulnerability advisories in the Kaspersky ICS Vulnerability Advisory format and may include:

- Vulnerability type;
- Short description;
- Reference to the vulnerability advisory provided by the vendor;
- Reference to the vulnerability CVE record;
- List of products (lines, versions) affected, according to Kaspersky data;
- Information on exploit availability in public and/or private sources;
- Severity (according to CVSS v3 and other metrics, if applicable);
- Signs of vulnerability exploitation (or exploitation of a similar vulnerability in the same or similar products) in real-world cyberattacks;
- Information on vulnerability exploitation results (if available) in ICS red/blue team exercises, CTF competitions, ICS security product tests, etc.;
- IDS rules (if available) to detect vulnerability exploitation attempts;
- Vulnerability mitigation measures recommended by Kaspersky.

[Request a consultation](#)

Related services

- ICS malware data feed
- ICS vulnerability and threat intelligence
- Analysis of known ICS vulnerabilities for critical information security decision-making
- 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