Kaspersky ICS CERT

kaspersky

Incident response at industrial enterprises

The problem

A cyberattack on an industrial enterprise that could result in the theft of confidential data, a production shutdown, or physical damage. The scale, primary cause and goals of the attack, as well as the capabilities of the attackers, are not always immediately clear. Effective measures must be taken quickly to stop the attack.

The solution

Coordination of actions to collect and analyze artifacts quickly, develop a defense strategy and assist in its implementation, determinate the sequence of steps to counteract an attack and minimize its consequences, search for primary causes and set a list of measures to prevent similar incidents in the future.

Target audience

Industrial enterprises of all kinds.

What we offer

Timely assistance in investigating and eliminating the consequences of cyberincidents at industrial enterprises by implementing the following actions.

- Collection of information from both OT and IT systems. Taking into account expert knowledge about how these systems function, their features and their key limitations, this can be done while minimizing the need to stop technological processes and production activities.
- Detection and examination of samples of new, previously undiscovered malware used in the attack, as well as identification and analysis of information about the malicious infrastructure used. These measures help compile a list of indicators of compromise, identify affected systems, determine the extent of network compromise within the organization, and obtain additional data for further investigation.
- Search for artifacts that can be used to attribute the attack to the activity of a specific threat actor. This may help detect additional tools used in the attack and provide insights into the tactics, goals, and capabilities of the attackers.

- An assessment (if necessary) of the probability of a negative impact on technological network systems, operations, and industrial equipment in the event of a denial.
- Development of tools (if necessary) to detect threat actor tools and collect information for investigation that is compatible with the operation of the company's IT and OT systems.
- Detection and recovery of hidden and erased traces of the threat actors' malicious activity in the enterprise network. Detailed analysis of the collected data and reconstruction of the attack pattern. Identification of the primary cause and the main circumstances that influenced its development.
- Detection and investigation of enterprise security issues exploited by attackers, including vulnerabilities in hardware and software, configuration errors, network security issues, incorrect security settings, deficiencies in security practices and procedures, and a lack of employee awareness about threats and common cyber hygiene rules.
- Compilation of a list of recommended security measures and means to ensure adequate protection against the threat based on information obtained during the investigation and knowledge of the attackers' tactics, techniques and toolsets, as well as expertise in setting up protection against such attacks.
- Preparation of recommendations to correct other information security issues discovered during investigation of the incident, including those not directly related to the incident.

Together we find answers to the following questions

- What happened?
- What assets were affected and what damage did they suffer?
- What technical and organizational deficiencies led to the incident? In particular, how did the attackers gain access to and spread through the infrastructure (what tools and tactics did they use)?
- How can the consequences of the incident be mitigated, and how can the damage be minimized?
- How can similar incidents be prevented in the future?

Help with mitigating the following types of incident damage

- Direct financial loss
- Loss of profits
- Reputational loss
- Damage to raw materials, products and equipment, loss of access to critical information
- Threat to human life and environmental damage

- Legal risks and penalties from regulators

What we do

We promptly respond to requests

We respond to requests left on our website or received via email at ics-cert@kaspersky.com to let the customer know that support is on the way.

We provide recommendations for identifying assets affected by the incident and containing the attack

Within 24 hours, we:

- Clarify details, obtain the customer's approval for our methodology, and together define the investigation's high-priority objectives (blocking the attack, identifying/mitigating the damage, determining the root cause of the attack, reconstructing the incident, and developing recommendations for preventing similar incidents in the future).
- Provide, if possible, an initial assessment of the situation, including an estimate of the incident's scope and possible damage, how the attack could develop, and recommendations for top-priority measures and actions.
- Reach an agreement on the scope (coordination, evidence collection and/or analysis) and format (on-site or remote) of the work to be performed by Kaspersky ICS CERT experts.

We collect digital evidence

We either go to the incident site to collect digital evidence ourselves or explain how the customer can do it on their own.

We conduct an investigation

As a rule, the following objectives should be achieved in the process of investigating an incident:

- Find, analyze and neutralize the entire malicious arsenal used in the attack. Some of it may not be identified in the early stages of the investigation and may require the development of updates for security solutions or dedicated detection tools.
- Identify and analyze compromised systems to ensure the attackers have no remaining presence on the attacked organization's network.
- Detect and analyze all traces of malicious activity to assess the scope of the damage inflicted.

- Determine the attackers' objectives to predict the options for further development and choose measures to prevent worst-case scenarios.
- Reconstruct the incident and attack timeline to determine which existing enterprise security issues were abused by the attackers, protect the enterprise from the attack's escalation as quickly as possible and develop a list of measures to prevent similar situations in the future.

We help minimize the consequences of the incident

We provide instructions for returning enterprise systems to normal operation. If necessary, we develop utilities designed to search for compromised systems and remove malicious toolsets.

We prepare a detailed report

We explain the results of our analysis of the collected materials and identified facts.

> The entire process usually takes between seven days and a month, depending on the scope of the incident, its technical complexity, and the degree to which the victim organization is prepared for joint and coordinated activity.

What the customer gets

During the incident response process

- Expert assessment of the situation;
- Step-by-step recommendations on the measures and actions required to achieve the investigation's objectives, prioritized by level of importance;
- Technical assistance and consultations, or coordination of the incident response team's activities.

Following the investigation

A report that includes:

- Incident reconstruction, including the main circumstances discovered, timeline, attack vectors, tactics and techniques, root causes of the attack and the security issues exploited by the attackers.
- Assessment of the incident's consequences for the enterprise's information assets.
- Description of the main properties and capabilities of the identified malware.
- Recommendations on how to improve the enterprise's security level to prevent similar incidents from occurring in the future, including technical

and organizational measures, events designed to increase personnel awareness of safe practices for securely working with information assets, and refresher courses for specialists.

We guarantee the confidentiality of data received as part of an incident investigation.

Request a consultation

Learn more

- Updated MATA attacks on industrial companies in Eastern Europe
- Common TTPs of attacks against industrial organizations. Implants for remote access
- Common TTPs of attacks against industrial organizations. Implants for gathering data
- Common TTPs of attacks against industrial organizations. Implants for uploading data
- Targeted attack on industrial enterprises and public institutions

Related services

- Development of incident response handbook and training
- Advanced incident response training
- ICS malware data feed
- ICS vulnerability data feed
- Analytical reports on ICS threats and vulnerabilities on the Kaspersky Threat Intelligence Portal

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