Kaspersky ICS CERT

kaspersky

Digital forensics and incident response in ICS

Training

Training focus

Participants study the tools and methods used to conduct all stages of an ICS incident response and investigation – from confirming the cybersecurity event and collecting evidence to analyzing artifacts and preparing the final report.

Skills gained

Participants acquire hands-on skills that allow them to investigate incidents at industrial enterprises using unique approaches and become ICS digital forensics experts.

Target audience

Information security specialists, analysts from computer security incident response teams (CSIRTs), security operations centers (SOCs), private and national computer emergency response teams (CERTs). It is also intended for any other specialist interested in learning about the specifics of ICS incident investigation.

The issue

Cyberattacks on industrial organizations can have unpredictable and serious consequences for the victim organization. In the ICS environment, downtime due to a cybersecurity incident can result in direct financial losses caused by interrupted production and unfulfilled contract obligations, as well as wasted raw materials and damage to expensive equipment.

Enterprises need to regain full control of their infrastructure as quickly as possible and resume normal operations. Therefore, the cybersecurity incident response team must be able to react quickly and efficiently to resolve numerous technical and organizational tasks, including:

- Identifying, examining and disarming all malware elements used in the attack. As some elements may not be uncovered in the initial stages of the investigation, this requires updating security solutions and/or using specialized detection tools.

- Assessing the possible negative effects of the detected malicious tools on OT network systems and identifying connections between the attack and equipment malfunctions, if any.
- Identifying and comprehensively investigating all compromised systems and quickly developing and implementing measures to eliminate any criminal presence.
- Identifying and collecting data containing traces of malicious activities from IT and OT systems without stopping the enterprise's technological processes, if possible.
- Analyzing the collected data rapidly and evaluating the damage.
- Identifying the threat actors' goals, predicting the likelihood of the incident developing further, and selecting a strategy to prevent the worst-case scenarios.
- Reconstructing the incident scene, including determining the primary cause, main circumstances and timeline of the attack, as well as identifying which security weaknesses in the organization were exploited by the threat actors.
- Promptly implementing protection to prevent the attack from spreading and developing a plan with measures to prevent similar incidents in the future.

> Many of the tools and methods used for investigations in the IT world are not suitable for ICS. Identifying and collecting evidence requires extra care because many standard IT tools can cause a denial of service in an ICS environment. Therefore, responding to an ICS incident (or one that could affect the ICS infrastructure) requires additional knowledge and skills.

What we offer

We train experts in ICS digital forensics. Having digital forensics specialists in-house allows an organization to react faster and more effectively to cybersecurity incidents, minimizing negative consequences and saving resources by only involving external experts in the most complicated instances.

Course description

1. Basics of incident response and the differences between digital forensics in IT and ICS/OT.
2. Understanding ICS network protocols and architecture.

3. Threat hunting in industrial/OT networks.
4. Digital forensics on workstations and servers with a specific focus on ICS software, threats and risks.
5. Digital forensics focusing on ICS components – workstations, servers, and specialized software and equipment.
6. Lab work. Investigation of a simulated ICS cybersecurity incident.

The training program can be modified based on customer needs.

The theory section examines real-world incidents at industrial organizations using publicly available information and technical information from Kaspersky investigations.

The practical section consists of exercises that consolidate the theoretical materials from each section through relevant hands-on tasks. On the final day, participants conduct their own independent investigation of an ICS cybersecurity incident in a lab setting.

The scenarios used in the practical section are based on analyses of real-world attacks on industrial organizations, incident investigations and ICS component vulnerability research.

Knowledge and skills gained

Theory

1. Measures required to prepare for incident response, including:
   - A knowledge of infrastructure requirements to facilitate rapid incident response.
   - An understanding of the requirements for OT cybersecurity incident response team personnel.
   - An understanding of the possibilities associated with using Cyber Threat Intelligence data, enterprise security posture evaluations, vulnerability research and threat modelling information to plan and execute cybersecurity incident prevention and prepare for such incidents.
2. Organizing effective IT and OT incident response process in industrial organizations, including:
   - Understanding the roles and zones of responsibility of the organization's employees and contracted experts, as well as the rules for organizing effective communication between the two groups.
   - Understanding the differences in organizing and investigating cybersecurity incidents in IT enterprise networks versus OT enterprise

networks, including requirements for toolsets and procedures for using them.
- Identifying priorities during investigations and creating plans for ICS incident investigations.
- Planning measures to prevent similar incidents in the future.

3. Typical errors in incident response preparation and investigation and how to avoid them.

Hands-on skills

1. Identifying incidents in the OT environment using available tools, publicly available utilities, commercial solutions and indicators of compromise (IoCs).
2. Responding to incidents in enterprise OT networks, including:
   - Gathering and handling digital evidence.
   - Using specialized ICS digital forensics tools and methodologies.
   - Searching for traces of intrusion using the collected evidence.
   - Reconstructing an incident using timestamps.
   - Selecting methods and tools to contain and halt the incident, as well as minimize its consequences.
   - Compiling an investigation report.

Course duration

- 5 days – standard course
- 10 days – standard course + additional hands-on practice

The training is conducted in person.

Course prerequisites

The training program can be adapted to the participants' level.

Minimal prerequisites for the basic course:

- General knowledge of networking
- Basic system administration skills in Windows, Linux and virtualization systems
- Knowledge of information security theory
- Practical skills in information security and IT asset security
- Basic IT incident response knowledge

Prerequisites for the advanced course:

- Experience conducting malware analysis
- Experience of reverse engineering executable files
- Deep knowledge of networking technologies and network protocol stacks
- Experience investigating cybersecurity incidents in IT networks
- Experience of threat hunting in IT networks

Course description

Certification

Theoretical knowledge is consolidated during a hands-on lab session on the final day, and participants receive a certificate upon completion.

Our trainers

Vyacheslav Kopeytsev, Principal Security Researcher, Kaspersky ICS CERT

Vyacheslav specializes in investigating attacks on industrial infrastructure, digital forensics and incident response in various types of systems, as well as malware analysis. He regularly speaks at industry conferences in addition to authoring articles and threat analysis reports.

Pavel Nesterov, Lead Security Researcher, Kaspersky ICS CERT

Pavel specializes in deep vulnerability analysis of software and hardware for automated process control systems, as well as research on current threats. He implements infrastructure projects and develops educational and methodological materials on control system safety, including practical exercises and specialized demonstration stands. Pavel has extensive expertise working with SIEM systems, from analytics to implementation and deployment.

Request a consultation

Learn more

- Vulnerability in FortiGate VPN servers exploited in Cring ransomware attacks
- Lazarus targets defense industry with ThreatNeedle
- Attacks on industrial enterprises using RMS and TeamViewer: new data

Related trainings and services

- Incident response at industrial organizations
- Development of incident response handbook and training
- ICS malware data feed
- ICS vulnerability data feed
- ICS threat intelligence reports

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