



Industrial cybersecurity awareness

Instructor-led training

Training focus

Designed for participants of different skill levels, these in-person courses provide an introduction to industrial cybersecurity essentials and offer practice-oriented knowledge on various aspects of industrial cybersecurity.

Skills gained

Depending on the attendees' objectives, these courses provide a general understanding of industrial cybersecurity or allow the participants to acquire or enhance their knowledge and skills to address particular enterprise cybersecurity challenges.

Target audience

IT and information security professionals, OT engineers and operators, middle-level managers and executives.

The security challenges

Industrial cybersecurity is a specialized discipline focused on protecting industrial control systems (ICS) that manage critical infrastructure and industrial processes. Its key difference from traditional information security lies in ensuring process continuity and preventing the physical consequences of cyberattacks.

ICS environments are sensitive to disruptions affecting availability and integrity: even minor interference can lead to cascading physical failures, safety risks, or extended downtime.

The primary line of defense is the security of industrial networks. The training covers the stages of designing, upgrading, and protecting industrial networks and addresses specific OT aspects such as the use of specialized industrial network protocols. The training addresses issues related to maintaining equipment availability, preventing unauthorized access to ICS equipment and safety instrumented systems, and ensuring the integrity of device software.

It is essential that technical measures be complemented with organizational measures. These include developing security policies and incident response plans tailored to industrial processes and technologies, as well as comprehensive training programs to foster a culture of security awareness among the OT related personnel including engineers, operators, and managers.

Understanding the nature of attacks on industrial systems is fundamental to building effective defenses. A cyberattack may aim to manipulate setpoint

values, disable safety systems, or spoof control signals, potentially leading to equipment damage, process shutdown, or harm to human life and health. Defense strategies are developed to detect and prevent the relevant attack vectors.

During the training, instructors explain how an attack occurs and why conventional safety instrumented systems may not help counteract it. Participants also learn the most effective ways to defend against different types of attacks; they are taught how to use security measures and tools, select and configure cybersecurity solutions, and foster a cybersecurity culture within the enterprise to achieve the best results and gain confidence that the industrial environment is properly protected.

What we offer

Instructor-led, in-person courses, ranging from three-hour intensive training to a full-day deep dive program.

Basic training: “Cybersecurity of modern industrial systems”

The course introduces participants to the essentials of information security in industrial enterprises, helps them understand the nature of security incidents and incident response approaches, and teaches secure day-to-day operational practices.

Course topics

1. Key aspects of industrial cybersecurity, industrial network architecture, classification of main ICS threats, vulnerabilities, exploits, and attacks.
2. Overview of the industrial threat landscape, security issues, the impact of the human factor, and attacks on industrial networks.
3. Attacker profiles.
4. Security policies and procedures.
5. Incident response essentials.
6. Social engineering techniques.

Duration: 1 day

Group size: 10–25 people

Core course: “Industrial security”

The course introduces key security measures and recommendations on applying security mechanisms in industrial systems, provides recommendations on organizing a cybersecurity team at an enterprise, provides participants with a dive into various aspects of ICS cybersecurity, such as detecting security

incidents, developing and implementing effective incident response plan, implementing countermeasures (including network segmentation, using a firewall, and protecting an air-gapped network), and conducting incident investigations. The training includes an analysis of real-world ICS incident investigations and explains the key aspects of attacks on industrial organizations.

Course topics

1. Overview of the industrial threat landscape, security issues, the impact of the human factor, and examples of attacks on industrial networks.
2. Attacker profiles.
3. Differences between IT and OT network security.
4. Defense-in-depth concept.
5. Network security in IT and OT networks.
6. Industrial network protocols.
7. Threat prevention and detection methods, and threat mitigation.
8. Compliance of protected industrial systems with cybersecurity standards and regulatory requirements.
9. Information security team structure and role descriptions.
10. Security considerations when working with suppliers.
11. Security of air-gapped networks.
12. Approach to cybersecurity incident response.
13. The development of the industrial internet of things (IIoT) and its impact on cybersecurity.

Duration: 1 day

Group size: 10–25 people

Express course: “Industrial security”

The course introduces key cybersecurity concepts (attacks, threat actors, threats, vulnerabilities, etc.), the modern cyberthreat landscape, and approaches to incident prevention and investigation. It teaches participants to understand the differences between IT and ICS security and covers the basics of cybersecurity regulation and compliance.

Course topics

1. Introduction to the key issues of cybersecurity in industrial environments.
2. Main differences between security in OT and IT networks.
3. Organizing and managing an effective enterprise information security team.
4. Compliance of protected industrial systems with cybersecurity standards and regulatory requirements.

Duration: 3 hours

Group size: 5–10 people

Courses prerequisites

The courses are customized according to the composition and background of each group.

Certification

Participants receive a certificate of course completion.

Our trainers

Ekaterina Rudina, Security Analysis Group Manager at Kaspersky

Ekaterina specializes in threat research, threat modeling, and risk assessment. She has 12 years of experience in industrial cybersecurity. Expert in regulatory documents (standards, laws, guidelines, requirements, etc.) related to the protection of critical infrastructure organizations. Author of documents developed under the auspices of the International Organization for Standardization (ISO), the Institute of Electrical and Electronics Engineers (IEEE), the International Telecommunication Union (ITU), and the Industrial IoT Consortium (IIC, now Digital Twin Consortium), as well as national standards on security-by-design. Holds a Ph.D. in Engineering.

Semen Kort, Principal Security Analyst at Kaspersky

Semen specializes in industrial cybersecurity and internet of things (IoT) security. Author of information security standards and a regular participant in working groups of international standardization organizations, as well as the Industrial IoT Consortium (IIC, now Digital Twin Consortium). Lead author of the industrial cybersecurity awareness course, teaching it at companies worldwide. Holds a Ph.D. in Engineering.

Alexander Nikolaev, Senior Security Analyst at Kaspersky

Alexander specializes in threat modeling, risk analysis, and the design of cybersecurity architectures for industrial control systems. He has 15 years of experience in industrial cybersecurity (in the oil and gas, agricultural, and banking sectors, as well as in shipping and aviation). Member of the Aviation Register of the Russian Federation working group on developing cybersecurity documents for the aviation industry at the State Research Institute of Aviation Systems (GosNIIAS).

Denis Babaev, Lead Security Analyst at Kaspersky

Denis specializes in threat modeling, risk assessment, and the design of cybersecurity architectures for industrial control systems, primarily for nuclear and thermal power plants. Has over 20 years of experience in engineering and

cybersecurity of cyber-physical systems. Member of technical committees of the International Electrotechnical Commission (IEC).

Related services

- Digital forensics and incident response in ICS
- Self-study on the Kaspersky Automated Security Awareness online platform

[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