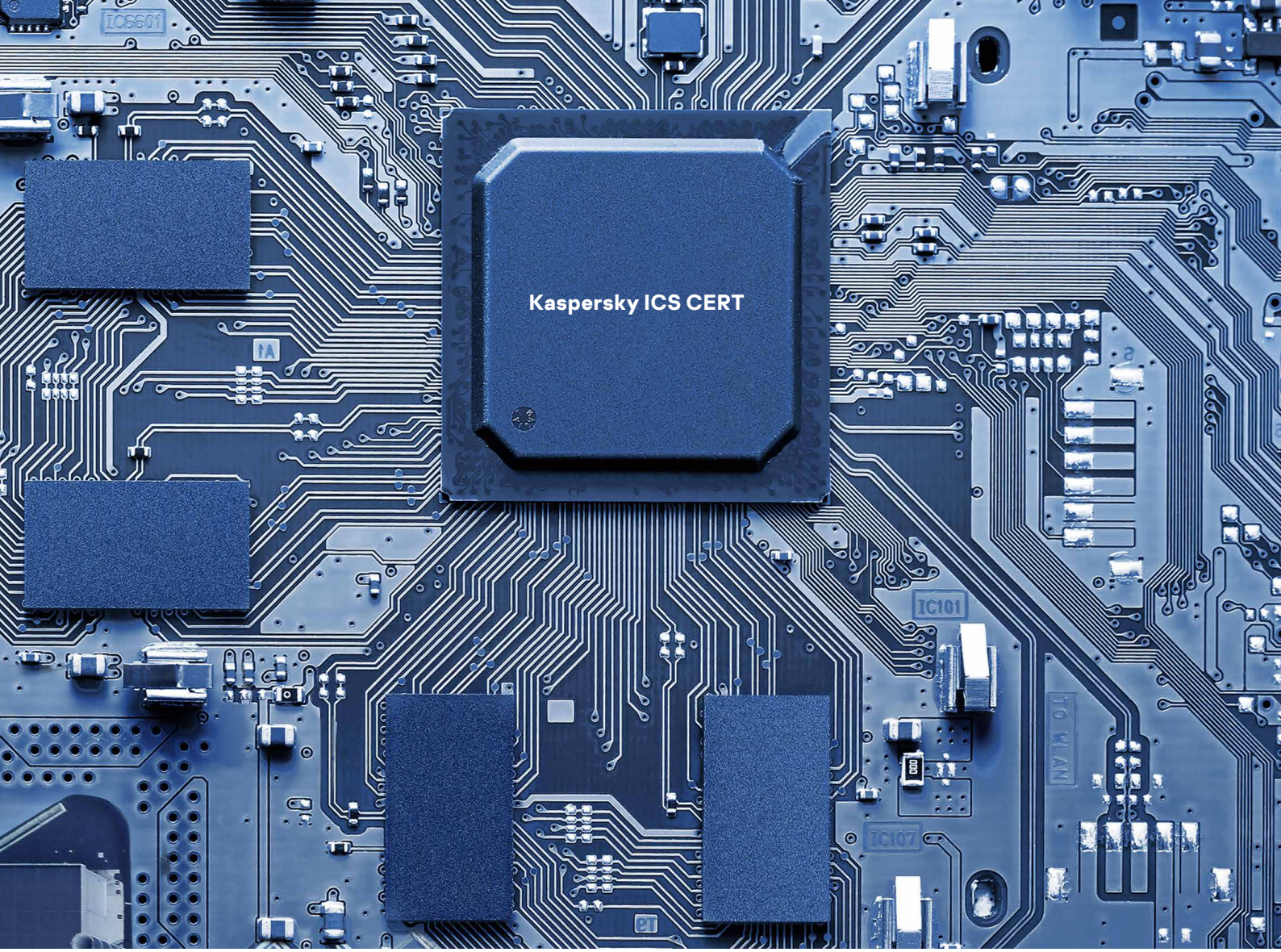


Kaspersky Industrial Cybersecurity Training Program

kaspersky BRING ON THE FUTURE

Table of Contents

Intro

Kaspersky offers Industrial Cybersecurity Awareness Courses based on the latest research and analysis conducted by the entire company.

Our ICS training program was developed specifically to enable - information technology (IT), operational technology (OT) and information security (IS) professionals, as well as executives and other staff, to enhance their knowledge of industrial cybersecurity.

Our Trainers and Partners

- **ICS experts**
- **Highly motivated**
- **Provide in-depth knowledge**
- **Flexible**
- **Offer customization**

Kaspersky Industrial Cybersecurity Training Program – At a Glance

- Changes behavior – stimulates individual employees' commitment to working safely and responsibly; builds a corporate environment where everyone believes that "I care about cybersecurity because everyone does – it's part of the job".
- Combines a motivational approach; gamification, different learning techniques, simulated attacks based on real-life industrial situations with in-depth, interactive cybersecurity skills training.
- Grows your organizational expertise. Training courses enable organizations to improve their cybersecurity knowledge pool in five main areas:
  - Basic knowledge of Industrial Control System (ICS) cybersecurity
  - ICS penetration testing
  - ICS digital forensics
  - Secure Internet of Things
  - Expert workshops and tech talks
- You can request to have our training programs provided on a one-time basis or at regular intervals. Details of exact topics to be covered during each session can be discussed and adapted for your organization's specific needs.

Testing and Certification

We provide evaluations and certificates for all of our programs. At the end of each training program we conduct a 'Lessons Learned' session. We also administer knowledge tests to provide actionable feedback for everyone: the students, the trainers and the customer's management.

Our careful analysis of course results ensures that your organization can be certain that your staff members internalized the course materials. We also include course surveys , which provide feedback to both the customer and the trainers, ensuring that everyone understands the overall impact of the course. This allows you to evaluate the training success and provides our trainers with information to continue improving of our courses.

For Engineers and Other Technical Personnel

Industrial Cybersecurity Awareness Training

Helps your non-IT/OT specialists to increase their awareness of the current industrial cybersecurity issues by learning about IT/OT differences and similarities, general cyber security basics and industrial cybersecurity specifics.

Course Contents

- Differences between IT & OT and IT/OT convergence, discovering the OT architecture Information security basics: attacks, vulnerabilities, exploits & malware, threats, exposures, APTs (kill chain)
- Attacker profiles for IT & OT
- Third party trust relationships
- Roles & responsibilities
- Security policies & procedures
- Countermeasures

Takeaways

- Information security basics: attack, attacker profiles, threats, vulnerabilities, etc.
- How to recognize cyber security incidents, malware and social engineering attacks
- Cybersecurity rules and measures & recommendations for daily work

Duration

1 day

For IT/OT Professionals

Industrial Cybersecurity Awareness Training

Raises awareness for your IT/OT specialists of current industrial cybersecurity trends; both attacks and protection techniques. Your staff members will learn to identify the main types of ICS vulnerabilities, clarify the key differences between typical ICS and pure IT malware, and understand how the on-going evolution of the Internet of Things can impact ICS security.

Course Contents

- Discovering the OT architecture
- Network basics: the architecture and topology of IT and OT, IT and OT components, IT & OT protocols, differences between IT & OT and IT/OT convergence
- How the evolution of the Industrial Internet of Things (IIoT) can affect ICS security
- Attacker profiles for IT & OT
- Information security basics: attacks, vulnerabilities, exploits & malware, threats, exposures, APTs (kill chain)
- Third party trust relationships
- Roles & responsibilities
- Security policies
- Countermeasures

Takeaways

- Network basics: typical topology, components, protocols, design practices
- Information security basics: attack vectors, attacker profiles, threats, vulnerabilities, etc.
- Malware attacks + APT (Advanced Persistent Threat) + social engineering
- Countermeasures: segmentation, firewalling, access control for devices, users, services, etc.
- Hardening measures & recommendations

Duration

1 day

For Executives

Industrial Cybersecurity Awareness Training for Executives and Managers

Helps executives and managers developtheir awareness of current industrial cybersecurity issues and recent incidents, identify the main types of ICS vulnerabilities, clarify the key differences between typical ICS and pure IT networks, and understand how the evolution of the Internet of Things can impact ICS security.

Course Contents

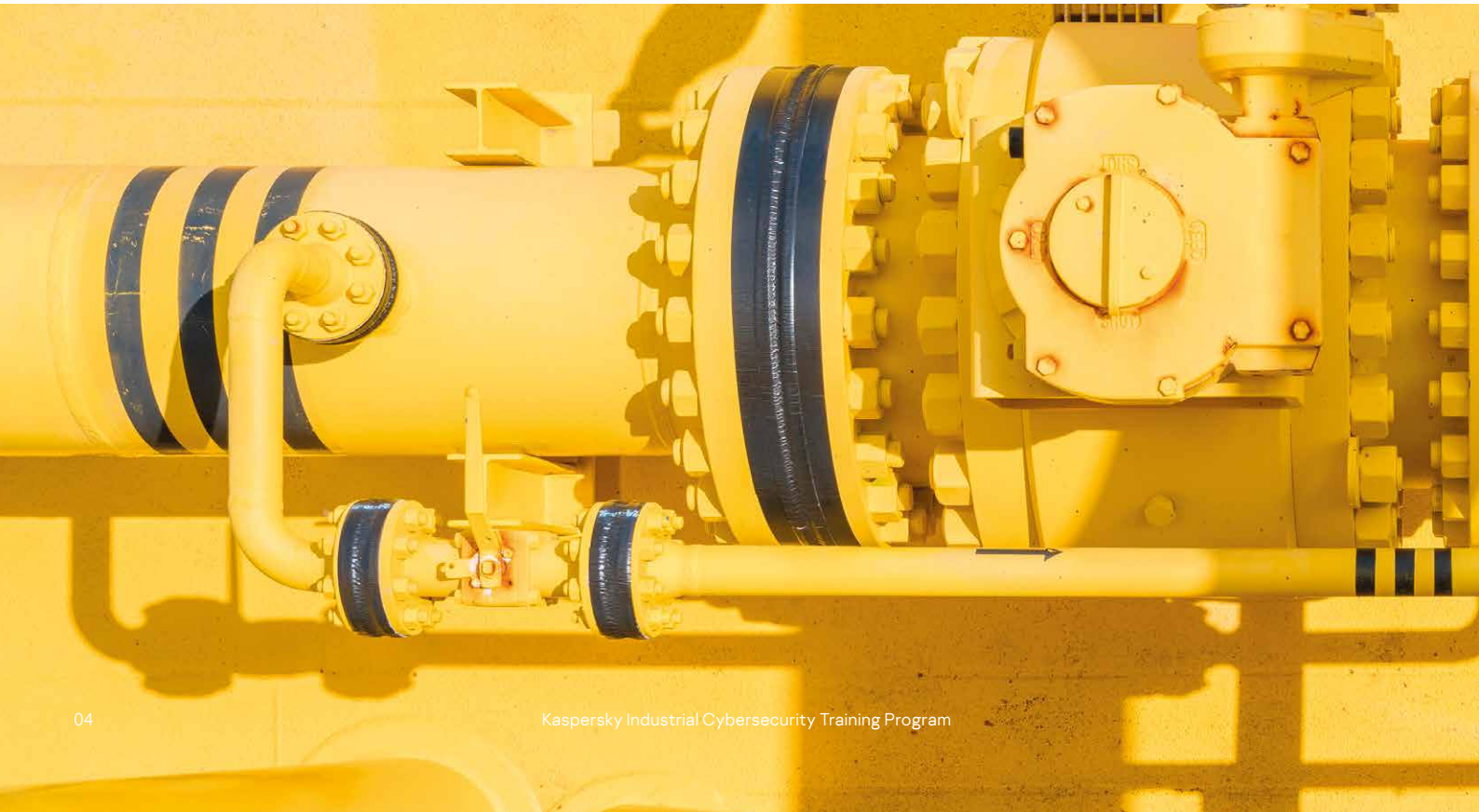
- Awareness about current cybersecurity issues in industrial control systems
- Clarify key differences between typical ICS and pure IT etworks
- Awareness about the possible attacks on SCADA systems
- Understanding the principles of network protection
- Recognition of social engineering
- Providing recommendations on the implementation of Defense in Depth
- Organizing an efficient cybersecurity department
- Handling security incidents properly and in a timely manner
- Detailed investigation of real SCADA cybersecurity incidents
- How the evolution of the Industrial Internet of Things (IIoT) can affect ICS security

Takeaways

- After completing the course, the participantswill know about:
- Information security essentials: attack, attacker profiles, threats, vulnerabilities, etc.
- Countermeasures: segmentation, firewalling, access control for devices, users, services, etc.
- Malware attacks + APT (Advanced Persistent Threat) + social engineering
- Hardening measures & recommendations

Duration

3 hours



For IT/OT Security Professionals

Advanced Industrial Cybersecurity in Practice

Raises awareness for your IT/OT specialists of current industrial cybersecurity trends; both attacks and protection techniques. Your staff members will learn to identify the main types of ICS vulnerabilities, clarify the key differences between typical ICS and pure IT malware, and understand how the on-going evolution of the Internet of Things can impact ICS security.

Course Contents

- Overview of the current threat landscape, security issues, human factors, ICS network attacks
- Network security in IT and ICS environments – special considerations
- Case study demonstrating the use of prevention, detection and mitigation techniques
- Compliance with industrial standards and legislation
- Network topologies and how network security technologies work
- Cybersecurity roles and team structures
- Common security mistakes

Takeaways

- Understanding current industrial cyber threats and how to combat cybersecurity incidents targeting your industry or organization
- Recognizing and identifying security incidents
- Performing simple investigations
- Drawing up and implementing an effective incident response plan
- This course includes highly customized elements and can be adapted to run for 1 or 2 days, as preferred
- Leads to certification

Duration

2 days

For IT/OT Security Professionals

Digital Forensics and Incident Response in ICS

Enables IT/OT security professionals to conduct successful forensic investigations in industrial environments and to provide expert analysis and recommendations.

Course Contents

- Introduction to ICS components, architectures and deployment in industries including electric power generation & distribution, oil & gas, transportation
- Recognizing and working with the challenges and constraints of ICS
- Digital forensics techniques as applied to ICS environments
- Creating an ICS digital forensics plan
- Manual forensic data acquisition and preservation – working with RTOS and ICS protocols
- Artifact analysis and anomaly verification
- Reporting
- Practical labs

Takeaways

- Conducting successful forensic investigations in ICS environments
- Creating an effective digital forensics plan for ICS
- Collecting physical and digital evidence and dealing with it appropriately
- Applying the tools and instruments of digital forensics to SCADA and PLC
- Finding traces of an intrusion based on the artifacts uncovered
- Reconstructing incidents and using time stamps
- Providing expert reporting and actionable recommendations.
- Leads to certification

Duration

Standard course – 5 days
Course with in-depth practice – 10 days

For IT/OT Security Professionals

IoT Vulnerability Research and Exploitation

Raises awareness for your IT/OT specialists of current industrial cybersecurity trends; both attacks and protection techniques. Your staff members will learn to identify the main types of ICS vulnerabilities, clarify the key differences between typical ICS and pure IT malware, and understand how the on-going evolution of the Internet of Things can impact ICS security.

Course Contents

- Overview of the current threat landscape, security issues, human factors, ICS network attacks
- Network security in IT and ICS environments – special considerations
- Case study demonstrating the use of prevention, detection and mitigation techniques
- Compliance with industrial standards and legislation
- Network topologies and how network security technologies work
- Cybersecurity roles and team structures
- Common security mistakes

Takeaways

- Understanding current industrial cyber threats and how to combat cybersecurity incidents targeting your industry or organization
- Recognizing and identifying security incidents
- Performing simple investigations
- Drawing up and implementing an effective incident response plan
- This course includes highly customized elements and can be adapted to run for 1 or 2 days, as preferred
- Leads to certification

Duration

3 days

Industrial Cyber-Safety Games

On-site and online interactive training modules and cyber-safety games conducted at all levels of technical expertise. These games are always modified for the appropriates levels of technical expertise ranging from executives and management to IT/OT personnel, to any employees who interact with industrial automation systems – on production lines, in the control room or in the back office.

Course Contents

- Fun, engaging and fast
- Team-work builds cooperation
- Competition fosters initiative & analysis skills
- The gameplay develops the understanding of cybersecurity measures

Takeaways

- Cyberattacks hurt revenues and need to be addressed at the top-management level
- Cooperation between IT and Business people is essential for cybersecurity
- An effective security budget is much smaller than the revenue you risk losing and does not amount to millions
- People adjust to specific security controls and their importance (audit training, antivirus, etc.)

Duration

2 hours

Further Training for All Levels

Industrial cybersecurity technical workshops and tech talks

These sessions are provided by Kaspersky CERT experts and can be conducted as a single course or as separate webinars.

They include:

- Industrial and IIoT cybersecurity insights and case studies
- Real-world examples, explaining vulnerabilities identified by Kaspersky experts
- Introduction to vulnerability research concepts

Current ICS workshops and technical talks

Detailed descriptions are available on request (talks and workshops are from 20 minutes to 2-3 hours long).

- IoT the Hard Way: Introduction to IoT Security and Hands-On Exercises
- Real-world binary exploitation
- Sandbox Redemption: escaping process isolation
- Security analysis into the Linux kernel
- The cyberthreat landscape – general
- ICS cyberthreat landscape
- Advanced persistent threats
- Attack attribution – analyzing 'artifacts'
- Reverse engineering binary applications (basics) – Win32, Win64, dotNET, ELF32, ELF64, Android
- Creating YARA rules
- Creating SNORT/Suricata rules
- Forensics in Windows
- Advanced reverse engineering: fighting packers, obfuscation and anti-debugging
- Threat modeling for Internet of Things solutions
- Security capabilities supporting the safety of the Internet of Things systems
- Security maturity. How to focus on vital security enhancement practices
- The architecture of trust and trustworthiness
- Critical infrastructure protection – governance around the world
- Critical infrastructure protection and reliability standards for electric utilities
- ICS Forensic Workshop
- ICS Incident Response case study
- Unusual effects of usual malware in ICS networks
- RATs in ICS attacks - direct and indirect usage

Capture the Flag with Kaspersky ICS CERT

Why a Capture the Flag (CTF) Competition at your Company

CTFs are an integral part of our ICS training portfolio. We organize CTFs based on your company needs and provide the materials and staff. CTFs can be conducted as a jeopardy game, simulated attack/defense scenarios or a mix of the two.

The Kaspersky ICS CERT experts begin by conducting an on-site meeting to agree on the format of the CTF and other general aspects of the event. During the meeting, Kaspersky experts will provide a brief overview of potential CTF scenarios and will help define the goals for your company. We will develop an initial outline and budget based on this preliminary meeting. To achieve a successful outcome, the Customer will need to involve management, sponsors and specialists with the relevant roles and expertise, such as IT, Information Security, HR, PR, etc. as appropriate.

What is an ICS CTF

An ICS capture the flag (CTF) contest is a competition for people with an interest or existing skills in ICS cybersecurity. The CTF is organized in the form of a contest, in which the participants solve general cyber security and specifically ICS security problems and thus win flags. They must either capture (attack/bring down) or defend computer systems in a CTF environment. Typically, these competitions are team-based and attract a diverse range of participants, including students, IT/OT professionals and even amateur cybersecurity enthusiasts. A CTF competition can be conducted for various levels of expertise and can last from a few hours to several days.

The winner is usually the team or individual scoring the most points at the end of the game. As in many sporting events, prizes are commonly awarded for first, second and third places. In the interest of contest integrity and respect for the game platform, CTF ground rules are shared with participants prior to the event. Violation of these rules may result in restrictions or even elimination from the competition.

What does a CTF achieve

There are many reasons for organizing a CTF contest, including general awareness and education of an industrial enterprise's management and technical staff about cyberthreats before the company experiences them first-hand.

The attack-defense scenario can be used both to train OT specialists in responding to cyberattacks and to test the **IT/OT security staff's skills in near-real-world attack scenarios.**

A CTF offers a good chance to introduce security specialists to modern attack vectors, kill chains, as well as defensive tactics and technologies used by different cyber security expert teams from around the world.

Another objective of a CTF could be to test ICS equipment and system configurations already used at an enterprise's facilities or being considered for installation / upgrade. This is also a good chance to test ICS security products and solutions already used at the enterprise or those which are being considered for installation on its IT and OT networks.

More information is available on request.

Our Partners

The ICS CERT team at Kaspersky collaborates with researchers and educators to conduct awareness and in-depth training about industrial cybersecurity.

Today there is a significant shortage of qualified ICS IT/OT security professionals, making it very important to make quality training available for professional development in this field.

We at the Kaspersky ICS CERT team and our partners develop new and interactive training materials for IT/OT managers and non-technical staff that leverage the knowledge and technical expertise of both the ICS CERT experts and our partners.

ABIROY CYBERSECURITY

Abiroy has been implementing turn-key projects in recruitment, training and full board project management since 1998.

Our key areas of business are:
- Management skills development
- Technical training
- Health, safety & environment

Our projects secure your investment in business development, equipment and technology through competent personnel training.

Fraunhofer IOSB

Established on January 1, 2010, the Fraunhofer Institute of Optronics, System Technologies, and Image Exploitation IOSB grew to become Europe´s largest research institute in the field of image acquisition, processing and analysis.

IOSB´s other areas of activity are control and automation technology, and information and knowledge management. Three core competencies of Optronics, System Technologies and Image Exploitation give the institute its distinctive profile.

Fraunhofer IOSB's IT security lab for industrial automation provides an ideal test environment to simulate real-world scenarios and analyze the effects. To this end, the IT security lab includes a specific smart factory with genuine automation components controlling a simulated production plant. All the network levels of a factory environment, including their typical components such as Industrial Ethernet, industrial firewalls and wireless components, are in place.

АИС
АКАДЕМИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

The Academy of Information Systems (AIS) is a center for continuing vocational education licensed by the Moscow Department of Education.

AIS was founded in 1996 as a non-governmental educational institution, providing training and professional retraining of specialists with a postgraduate degree.

Our main areas of study:
- Information Technology
- Information Security
- Enterprise Security
- Business Management
- Personal development

During its existence, the AIS has trained more than 20 thousand professionals. We work with major companies and public institutions in Russia such as the Bank of Russia, the Federal Treasury, the Federal Tax Service, the State Pension Fund, JSC Russian Railways, JSC Gasprom, JSC Sberbank, JSC Rostelecom, JSC Rostec Corporation and many others.

We offer original courses, developed by AIS trainers, methodologists and our partners, as authorized courses from leading Russian and international vendors in the IT and Information Security sector. We currently offer over 200 courses and training sessions. We also organize business and scientificconferences, both at the national and international levels.
Web-sites: www.infosystems.ru, www.vipforum.ru

Become a Trainer – Train the Trainer

Sometimes an organization might need in-house trainers to maintain basic ICS awareness. The reasons might include effective use of resources; addressing a larger number of employees while staying on budget; or the ability to initiate multiple learning tracks or classes going on at the same time.

For these situations the ICS CERT team at Kaspersky provides a Train the Trainer session to prepare in-house IT/OT professionals to conduct Industrial Cyber Security Awareness Training – both the One Day or the concentrated 2–3 hours versions.

The Train the Trainer session takes 2–3 days and includes presentations, discussions and hands-on experience. During the session all required training materials will be provided. The session will end with a knowledge test and exam by individual Skype sessions.

About Kaspersky

Kaspersky is a global cybersecurity company, which has been operating in the market for over 20 years. Kaspersky's deep threat intelligence and security expertise is constantly transforming into next generation security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 270,000 corporate clients protect what matters most to them.

Learn more at www.kaspersky.com

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity is a portfolio of technologies and services designed to secure operational technology layers and elements of your organization – including SCADA servers, HMIs, engineering workstations, PLCs, network connections and even engineers – without impacting on operational continuity and the consistency of industrial process.

Learn more at
www.kaspersky.com/ics

About the Kaspersky ICS CERT Team

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) is a global initiative of Kaspersky 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.

Learn more at: https://ics-cert.kaspersky.com/

Contact Information

Are you interested in learning more about our training?

Please contact us:
ics-cert-query@kaspersky.com

kaspersky

www.kaspersky.com

GBD-5702 Q2/20 V3