Training

Kaspersky Industrial Cybersecurity training program

kaspersky BRING ON THE FUTURE

Learn more:
ics-cert.kaspersky.com

Contents

Industrial cybersecurity essentials

Professional development

The Kaspersky ICS CERT team delivers all training programs outlined in this brochure.

Kaspersky ICS CERT is a global project established in 2016 to coordinate the efforts of industrial automation system vendors and industrial facility owners and operators. The team includes more than 30 experts in ICS threat and vulnerability research, incident response and security analysis.

We provide training in industrial cybersecurity essentials and practical skills to investigate cybersecurity incidents and perform vulnerability research. Our programs are based on the practical experience and real-life cases.

Kaspersky ICS CERT experts:

- Research cyberthreats and detect attacks on industrial facilities providing early alerts to those in danger
- Investigate cybersecurity incidents at industrial enterprises and critical infrastructure facilities helping to mitigate similar cases in future
- Analyze popular industrial control system products and technologies for vulnerabilities and help eliminate any vulnerabilities identified
- Develop industrial cybersecurity methodologies, frameworks, and standards
- Consult industrial organizations on industrial cybersecurity issues
- Help developers make their products more secure.

We are highly interested in collaboration with universities in the following areas: lecturing – exclusive ICS training for students, professors and researchers; virtual or real talks with Kaspersky ICS CERT experts; joint research projects and joint PR.

Contact us at ics-cert@kaspersky.com.

Industrial Cybersecurity Essentials

Basic training

on industrial cybersecurity

Course topics

- Differences and similarities between IT & OT security, discovering OT architecture information security basics: attacks, vulnerabilities, exploits & malware, threats
- Overview of the current threat landscape, security issues, human factors, ICS network attacks
- Attacker profiles for IT & OT
- Security policies & procedures
- Handling security incidents properly and in a timely manner
- Recognition of social engineering

Takeaways

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

Course format

Onsite instructor led lessons with presentations, case studies and hands-on exercises

Duration

1 day

Group

10 - 25 people

More training options

For bigger groups of people, we recommend considering the online training on the Kaspersky Automated Security Awareness Platform, where all basic cybersecurity topics are covered, including a dedicated module on industrial cybersecurity. Visit k-asap.com for a free trial.

Advanced training

on industrial cybersecurity

Course topics

- Overview of the current threat landscape, security issues, human factors, ICS network attacks
- Attacker profiles for IT & OT
- Differences and similarities between IT & OT security
- Providing recommendations on the implementation of Defense in Depth
- Network security in IT and ICS environments – special considerations
- Industrial network protocols
- Prevention, detection and mitigation techniques
- Compliance with industrial standards and legislation
- Cybersecurity roles and team structures
- Third party trust relationships
- Isolated network security
- Security incident response plan
- How the evolution of the Industrial Internet of Things (IIoT) can affect ICS security

Takeaways

- Hardening measures & recommendations
- Recognizing and identifying security incidents
- Performing basic investigations
- Handling security incidents properly and in a timely manner
- Detailed investigation of real SCADA cybersecurity incidents
- Drawing up and implementing an effective incident response plan
- Countermeasures: segmentation, firewalling, access control for devices, users, services, etc.
- Malware attacks + APTs (Advanced Persistent Threat) + social engineering
- This course includes highly customizable elements and can be adapted to run for 1 or 2 days, as preferred

Course format

Onsite instructor led lessons with presentations, case studies and hands-on exercises

Duration

2 days

Group

10 - 25 people

Training for executives

on industrial cybersecurity

Course topics

- Awareness about current cybersecurity issues in industrial control systems
- Clarify key differences between typical ICS and pure IT networks
- Organizing an efficient cybersecurity department
- Compliance with industrial standards and legislation

Takeaways

- Information security essentials: attack, attacker profiles, threats, vulnerabilities, etc.
- Understanding current industrial cyber threats and how to combat cybersecurity incidents targeting your industry or organization
- Understanding difference between IT/OT security
- Information about cyber security legislation

Course format

Onsite instructor led lesson

Duration

3 hours

Group

5 - 10 people

More training options

For C-level executives, we also recommend Kaspersky Interactive Protection Simulation (KIPS), the interactive game to challenge decision-makers perceptions of cybersecurity and enhance cooperation between business units.
Learn more at https://www.kaspersky.com/enterprise-security/security-awareness.

Professional development

Digital forensics and incident response in ICS

ICS presents many specific challenges and constraints when it comes to digital forensics. Tools and technologies developed for IT environments are often inappropriate or simply useless. Thus evidence collection, for example, becomes a manual process. In addition, special attention must be given to rapidly regaining control and bringing the system or devices back to a safe state. Working with our digital forensics specialists, participants will explore the unique aspects of ICS digital forensics. The course content ranges from identifying a genuine incident to data collection, examination, analysis and reporting in industrial environments, developing the hands-on skills and approaches required to become an expert investigator of ICS incidents.

Learning objective

- Conduct successful forensic investigations in ICS environments
- Create an effective Digital Forensics plan for an ICS environment
- Collect physical and digital evidence and deal with it appropriately
- Apply the specific tools and instruments of digital forensics to ICS software (SCADA) and hardware (PLC)
- Find traces of intrusion based on uncovered artifacts
- Reconstruct incidents and use timestamps, including timestamps from ICS software and hardware
- Provide expert reporting and actionable recommendations

Who can benefit

- IT and OT IS professionals
- Fraud Investigators
- Auditors
- CSIRT and SOC analysts who would like to become ICS Digital Forensics professionals and understand the major differences between IT and ICS digital forensics strategies
- Police and military personnel and other security personnel who deal with cyber investigations in ICS environments

Resources

- Course material
- Handbooks

Training prerequisites

All course participants need to an understanding of IT administration, networking and security practices. System administration skills for Windows, Linux, and Virtual Systems are also necessary.

It is desirable, but not necessary to have malware analysis skills, as well as knowledge about the architecture of industrial control systems, their protection and security problems.

Course topics

Day 1: Incident response basics and differences between IT and OT digital forensics

Day 2: ICS network protocols and device architecture, threat hunting in ICS networks

Day 3: Digital forensics in X86/X86 systems, including ICS-specific software, threats and risks

Day 4: Digital forensics in OT devices, case study based on publicly known attacks and Kaspersky investigations

Day 5: Lab work simulating real-world investigations

Course format

Onsite instructor led lessons with presentations and case studies, hands-on exercises

Duration

5 days

Group

Up to 10 people

IoT vulnerability research and exploitation

Nowadays, most companies and individuals own one or more smart devices. Internet of Things (IoT), essentially includes such embedded devices and their ecosystem. For security professional, new skillsets such as firmware reverse engineering, hardware communications and radio frequency analysis are now essential to fully encompass the whole attack surface during a security assessment.

Learning objective

We will guide you through systematic analyses of IoT devices to identify vulnerabilities. You will interact directly with hardware interfaces, and become comfortable with using hardware and software tools to evaluate IoT devices and their firmware. After having experimented with different devices, you will have a chance to apply your newly acquired skills by conducting a penetration test against a simulated environment.

After the training, you will be able to analyze and exploit the hardware and software attack surfaces of IoT devices to secure them. Going forward you will tackle most situations confidently, including when the firmware is not publicly available. You will also develop an instinct for approaching uncommon targets.

Who can benefit

- Security researchers
- Penetration testers
- Product security teams
- Software and security architects
- Technical product managers

Resources

- Course materials
- Target IoT devices and firmware
- Hardware toolbox for device analysis
- Lab manuals

Training prerequisites

- Experience with C/C++, Python or any other programing language
- Familiarity with basic Linux commands
- Basic reverse engineering skills
- Knowledge of the most common network protocols
- Experience using a disassembly tool would be helpful, but not necessary

Course topics

- Vulnerability research methodologies
- Hardware reconnaissance and PCB reverse engineering
- Hardware interfaces security (UART, SPI, I2C, JTAG)
- Firmware extraction, analysis and emulation
- Reverse engineering custom of binaries and protocols
- Wireless protocols security
- Automation of static binary analysis tools
- Fuzzing embedded targets executables and libraries

Course format

Onsite instructor led lessons, workshop, hands-on sessions. A hybrid or online format is possible

Duration

3 days

Group

Up to 10 people

Vulnerability discovery through fuzzing

Fuzzing is a powerful and effective technique for finding vulnerabilities in software. Despite the best efforts of security researchers and software developers, complex software still ships with bugs. Fuzzing helps to discover hard-to-find vulnerabilities that may not be caught by manual code review, static code analyzers, or unit tests.

Each year, thousands of vulnerabilities are responsibly disclosed by security researchers. By using fuzzing, you can join their ranks and help make the software we use every day more secure and reliable.

With fuzzing, you can also tailor your testing to your specific needs and requirements. You can use different fuzzing tools and techniques to target specific parts of your software, or to test for specific types of vulnerabilities. This flexibility and customization make fuzzing a valuable addition to any software testing toolkit.

Learning objective

Vulnerability discovery through fuzzing aims to introduce professionals involved in defining, developing, and testing software products to the practice of fuzzing. This training will show attendees how to use fuzzing to identify vulnerabilities in their own software, as well as in third-party products, with or without access to the source code.

During the training, attendees will learn about the fundamental concepts of fuzzing, including corpus mutation, coverage, feedback, and instrumentation. We will also discuss the importance of these concepts and how they apply to the practice of fuzzing.

In addition to learning the theoretical aspects of fuzzing, attendees will also have the opportunity to apply their knowledge in hands-on exercises using real-world examples. These examples will illustrate the concepts discussed in the training and will cover both white box and black box scenarios. By the end of the training, attendees will have the skills and knowledge they need to use fuzzing effectively to discover vulnerabilities.

Who can benefit

- Software engineers
- QA testers
- Security researchers
- Developers
- Penetration testers

Resources

- Course materials
- Lab manuals

Training prerequisites

- Being able to read and write some snippets of C/C++ code
- Familiarity with basic Linux commands
- Basic reverse engineering skills
- Experience using a disassembly tool preferable but not mandatory

Course topics

- Introduction to fuzzing techniques, how and when to use it
- Writing a custom fuzzer
- Getting hands-on existing tools such as libfuzzer, AFL++, DynamoRIO, WinAFL
- Conducting fuzzing against both source code and binary targets
- Emulation for fuzzing other architectures
- Effective corpus generation and mutation
- Crash analysis and triaging

Course format

Onsite instructor led lessons, workshop, hands-on sessions. A hybrid or online format is possible

Duration

3 days

Group

Up to 10 people

kaspersky

ics-cert.kaspersky.com