Enhance your cybersecurity skills with practical training from world-renowned experts

Kaspersky Cybersecurity Training

kaspersky bring on the future

Lack of specialists

41%

of InfoSec professionals say their organization's cybersecurity teams are "somewhat" or "significantly understaffed"[1]. Information security research and malware analysis are the most understaffed roles globally (39%)

48%

of InfoSec professionals claim it takes more than six months to fill an information security position. According to analysts, this is way above average[1]

70%

of respondents looking to hire for cybersecurity positions seek people with hands-on training[1]

The latest skills for your cybersecurity specialists

Cybersecurity mistakes can bankrupt a business. Today, training specialists in information security, teaching new skills and maintaining a high level of expertise is more than just the smart choice: it's essential.

Well-trained employees effectively identify and prevent incidents, and promptly respond to and investigate them to fix potential vulnerabilities and prevent attacks in the future.

By investing in your specialists' qualifications, you ensure reliable protection for your company and save on third-party experts. Investing in training is a strategic decision to strengthen your business's cybersecurity and build a highly-qualified team of experts in the company.

Current challenges in cybersecurity: When to invest in training?

Lack of IT infrastructure transparency, insufficiently consistent management

Ever-increasing complexity of IT systems

IT skills need to be maintained at a high level in line with the newest attack vectors and technology

Lack of technical specialists qualified to detect and respond to complex incidents

Financial benefits

up to $1.49 million

savings in organizations with a high level of planning and testing of incident response measures[2]

$258.629

average cost savings on breaches due to employee training[2]

[1] Based on a Kaspersky study by Grand View Research, 2024. Read more: https://www.kaspersky.com/blog/portrait-of-modern-infosec-professional-research-2024-labor-market

[2] Based on the Cost of a Data Breach 2023 report, IBM

For more information about self-paced training programs, to purchase a course, or to try a demo, please visit our web page

Kaspersky Cybersecurity Training

Kaspersky Cybersecurity Training covers a wide range of cybersecurity topics, from basic to expert level. Our world-class experts share their experience and teach today's newest effective strategies for detecting threats and mitigating risks.

Training includes theory and practice to keep employees engaged and involved, especially when using what they learn in real scenarios. At the end of each course, material is summarized in a test.

Kaspersky Cybersecurity Training is designed to increase the qualifications of cybersecurity teams and improve the skills of individual specialists.

Why choose cybersecurity training from Kaspersky?

Kaspersky's cybersecurity solutions are built on people, knowledge and experience. Our expertise spans 30 years of protecting and arming our customers against all forms of cybercrime. Our rich database of global data, advanced proprietary technology and teams of senior experts (with global accolades) serve as the basis for innovative, highly effective solutions backed by unique threat intelligence and comprehensive expert services and training. Our deep expertise helps us provide our customers with the latest tools and insights to navigate the complex cyberthreat landscape and make their businesses more secure.

All of our training programs are designed by industry-leading cybersecurity experts and have a hands-on approach.

Training formats

We offer several formats to choose from:

Offline format

For full concentration and immersion with direct communication with our experts. Any of our programs can be adapted to the specific requirements of any organization, including more attention to specific aspects of cybersecurity

Live online format

Direct communication with our experts without needing to go anywhere in person. Training is held in groups as an online workshop

Self-paced format

The most convenient and accessible option. Video lectures from Kaspersky experts guide you through the program any time that's convenient for you at a comfortable pace. Practice in virtual labs provides practice for new skills using specific tools on real attack scenarios and exclusive samples of malware

Offline Cybersecurity Training

Cybersecurity Training in Offline format is delivered in group sessions at customer's premises or at our local Kaspersky office, ensuring a focused and hands-on learning experience, first-hand knowledge and best practice from our renowned experts.

Each course requires a minimum of 5 participants and allows for a maximum of 15. The duration of the training depends on the selected course – most of the programs are designed to run for 5 days.

For Industrial CyberSecurity training the number of participants and duration of courses varies depending on the program. For exact information, please consult the webpage: **ics-cert.kaspersky.com**

Training programs

Program name	Live online	Self-paced (online)	Offline
Cyber capacity building program		●	
Reverse engineering 101		●	
Malware analysis and reverse engineering		●	●
Advanced malware analysis and reverse engineering		●	●
Advanced reverse engineering with Ghidra		●	
Mobile malware reverse engineering		●	●
Security operations and threat hunting	●	●	●
Hunting for APT threats with YARA		●	●
Suricata for incident response and threat hunting		●	●
Windows incident response	●	●	●
Digital forensics in Windows	●	●	●
Basic training on industrial cybersecurity	●		●
Advanced training on industrial cybersecurity	●		●
Training for executives on industrial cybersecurity	●		●
Advanced digital forensics			●
Digital forensics and incident response in ICS			●
IoT vulnerability research and exploitation			●
Vulnerability discovery through fuzzing	●		●

Kaspersky Cybersecurity Training helps:

1. Improve qualifications or refresh skills in SOC, CERT, cybersecurity departments and development teams
2. Form your own SOC team
3. Comply with regulatory requirements in your industry to improve cyber literacy among employees and/or hold regular training for cybersecurity employees.
4. Improve the qualifications of individual specialists

The latest skills for your IT/cybersecurity specialists

Training programs	Knowledge and skills acquired
Malware Analysis training	
Reverse engineering 101	• Learn assembly language basics • Master the translation of high-level code structures using compilers • Work with containers: from simple custom lists in C to templated maps and C++ vectors in Rust • Take your first steps using reverse engineering tools • Learn to analyze algorithms and structures by compiling and disassembling code fragments
Malware analysis and reverse engineering	• Learn the basics of malware analysis and reverse engineering tools to successfully investigate malware attacks • Get acquainted with reverse engineering tools written in different programming languages, including scripting and compiled for different operating system architectures • Master the translation of high-level code structures using compilers • Learn to analyze algorithms and structures by compiling and disassembling code fragments
Advanced malware analysis and reverse engineering	• Learn how to create static decryptors to solve real-world problems and analyze malicious code in depth • Conduct in-depth analysis of modern malicious code samples, from obtaining the initial artifact to creating technical descriptions of TTP with IoC • Keep damage assessment and incident response measures accurate and effective
Advanced reverse engineering with Ghidra	• Learn how to configure Ghidra and build its latest version from source code • Learn the typical malware analysis workflow using Ghidra • Get a clear understanding of how to work with data types and structures in Ghidra and how to identify runtime library code using Ghidra • Learn how to use Ghidra's disassembler and decompiler scripting capabilities to automate reverse engineering tasks • Get more out of Ghidra with Eclipse IDE™ (Eclipse IDE is a trademark of Eclipse Foundation, Inc.)

Training programs	Knowledge and skills acquired

Malware Analysis training

Mobile malware reverse engineering

- Learn how to analyze mobile malware, including Android/iOS samples
- Master advanced static analysis (shallow analysis): permissions, strings, signatures, resource files, decompilation of Dalvik bytecode
- Learn static analysis of native libraries for Android and iOS with Ghidra
- Train your advanced dynamic analysis skills with the Frida dynamic toolset

Threat Hunting training

Security operations and threat hunting

- Understand the structure of SOC as part of security services as a whole
- Learn how to plan and organize security monitoring
- Master how to use multiple threat intelligence sources to find emerging modern threats
- Learn to detect and investigate malicious activity in Windows and Linux infrastructures based on attacker tactics, techniques and procedures
- Get experience using ELK-based threat hunting infrastructure (Elasticsearch, Logstash, Kibana)

Suricata for incident response and threat hunting

- Understand NIDS and how to use it
- Write Suricata rules for different protocols
- Learn to use tips and recommendations to create quick and effective rules
- Learn about typical network attacks
- Review regulations: basic knowledge of network protocols and using regular expressions
- Learn to use Suricata to find threats
- Analyze suspicious traffic and recognize traffic anomalies
- Learn how to identify and eliminate false alarms

Hunting for APT threats with YARA

- Learn to write clear and effective YARA rules
- Master exclusive techniques for creating fast and effective rules
- Figure out how to test YARA rules for false positives that skew results
- Learn to identify new undetected malware samples in your infrastructure and cloud platforms
- Learn how to use external YARA modules to hunt threats even more effectively
- Explore the world of finding anomalies
- Practice with real-life examples (BlueTraveller, DiplomaticDuck)

Training programs	Knowledge and skills acquired

Incident Response training

Incident response

- Learn how to identify and respond to cyber incidents
- Study the sequence and content of incident response phases
- Learn how to look for signs of intrusion
- Differentiate APT threats from other types of threats
- Learn different attack methods and the anatomy of targeted attacks based on the kill chain
- Analyze affected machines in real time
- Analyze log files using regular expressions and ELK
- Improve the quality of the IoCs you create
- Master the skills of forensic analysis of network traffic and memory
- Learn how to collect digital evidence and work with it effectively

Digital forensics in Windows

- Learn how to detect and manage a variety of digital evidence in forensic investigations
- Master the basic tools and techniques of digital forensics
- Learn to find traces of malicious activity related to incidents
- Improve your skills with forensic analysis of memory, browser history, and email
- Reconstruct the incident scenario using time metrics from various Windows artifacts

Advanced Digital Forensics

- Conduct in-depth forensic analysis of FAT & NTFS file systems, including deleted file recovery
- Perform memory & network forensic to detect and trace malicious activity
- Analyze & reconstruct attack timelines and sources
- Recover data using file carving, shadow copies, and advanced Windows artifacts

Industrial CyberSecurity (ICS) training

Cybersecurity of modern industrial systems

Basic level

- Learn about industrial system security, industrial network architecture, and classification of the main threats to ICS: vulnerabilities, exploits and attacks
- Learn about the types of attackers and social engineering methods
- Improve your knowledge about security policies and procedures and master the basics of incident response methods
- Learn how to stay safe in your everyday work

Cybersecurity of modern industrial systems

Advanced level

- Learn the main measures and recommendations for security mechanisms in industrial systems
- Study how to identify security incidents
- Learn the basics of how to conduct incident investigations
- Get recommendations on how to structure your cybersecurity team
- Explore real-life examples of incident investigations in ICS
- Master the skills to develop and implement an effective cybersecurity incident response plan
- Learn about countermeasures: network segmentation, using firewalls, protecting isolated networks
- Go in depth into attacks on industrial organizations

Training for executives on industrial cybersecurity

Express course

- Master cybersecurity basics about attacks, intruders, threats, vulnerabilities and more
- Learn about the modern cyberthreat landscape, incident prevention and investigation
- Explore the differences between IT and ICS security
- Learn the basics of legal regulation in cybersecurity

Training programs	Knowledge and skills acquired

Industrial CyberSecurity (ICS) training

Digital forensics and incident response in ICS

- Learn to detect cybersecurity incidents in industrial systems
- Create a plan for investigating incidents in an ICS
- Learn how to collect and process evidence (physical and digital)
- Understand how to use specialized digital forensics tools and techniques for software (e.g., SCADA) and hardware (e.g., PLC) in industrial systems
- Search for traces of intrusion based on evidence
- Recover incident images and use timestamps in ICS software and hardware
- Prepare investigation reports and make practical recommendations to resolve consequences and prevent similar incidents in the future

Vulnerability discovery through fuzzing

- Learn the basic concepts and methods of fuzzing, including corpus mutation
- Master building feedback, instrumentation and code coverage
- Learn how to use fuzzing to find vulnerabilities with and without access to source code

IoT vulnerability research and exploitation

- Learn how to check the hardware and software of IoT devices for vulnerabilities
- Analyze vulnerabilities
- Make recommendations for resolving detected issues
- Choose compensation measures the smart way to protect IoT devices

For more about Industrial cybersecurity training programs and other related services, check out the Kaspersky ICS CERT page.

Kaspersky Cybersecurity Training

www.kaspersky.com

#kaspersky
#bringonthefuture