First-line Incident Response training for general IT specialists

Cybersecurity for IT Online

Free trial
cito.kaspersky.com

kaspersky bring on the future

Kaspersky Cybersecurity for IT Online

Cybersecurity for IT Online (CITO)

Interactive training that builds strong cybersecurity and first-level incident response skills for general IT specialists

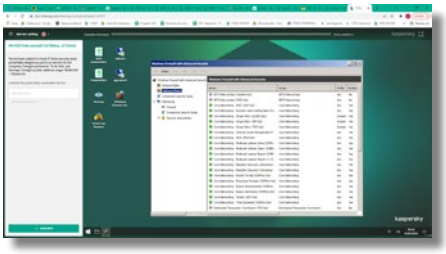
Creating a strong corporate cybersecurity posture is impossible without the systematic education of all relevant employees. Most enterprises provide cybersecurity education and training on two levels – expert training for IT security teams and security awareness for non-IT employees. Kaspersky offers a comprehensive set of products for both. But what's missing? For IT teams, service desks, and other technically advanced staff, standard awareness programs are not enough. However, they don't need to become cybersecurity experts – it's too expensive and too time-consuming.

Training format

Training is completely online. Trainees only need Internet access and the Chrome browser on their PC. Each of 6 modules consists of a short theoretical overview, practical tips and between 4 and 10 exercises covering specific skills teaching students how to use IT security tools and software in everyday work.

Study is intended to be spread over the course of a year. The recommended rate of progress is 1 exercise per week – each exercise takes between 5 and 45 minutes to complete.

The current edition of the training is targeted at the Windows corporate environment.



Training delivery method:
Cloud or SCORM format

First-line incident response

Kaspersky is launching first-on-the-market online skills training for generalist enterprise IT professionals. It consists of 6 modules*:

- Malicious software
- Potentially unwanted programs and files
- Investigation basics
- Phishing incident response
- Server security
- Active Directory Security

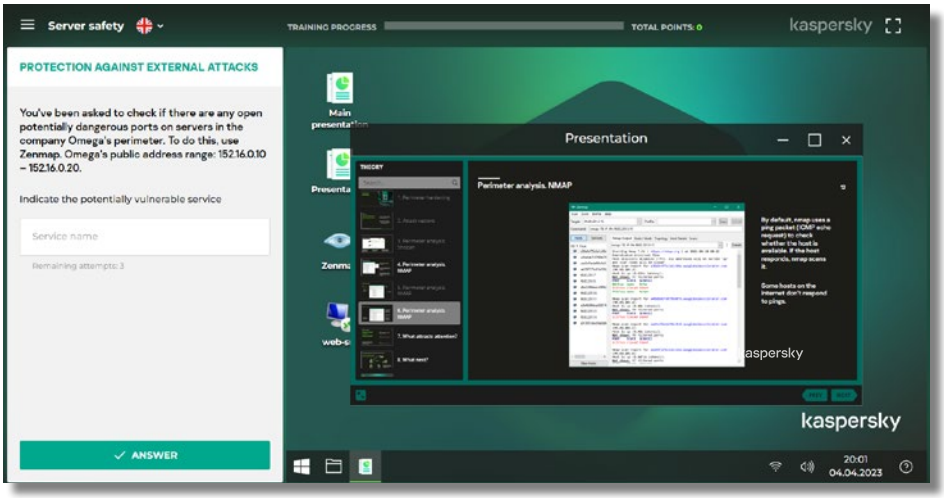
The program equips IT professionals with practical skills to recognize a possible attack scenario in a seemingly benign incident, and how to collect incident data for handover to IT security. It also creates a passion for hunting out signs of malicious activity, cementing the role of all IT team members as the first line of security defense.

Why is CITO training effective?

- Interactive: the stimulation of real processes without any risk to the computer
- Creates skills as well as knowledge: learning by doing
- Intuitive learning process: convenient navigation and hints
- Covers all the main IT security topics and problems that general IT staff face in their work

Learning process

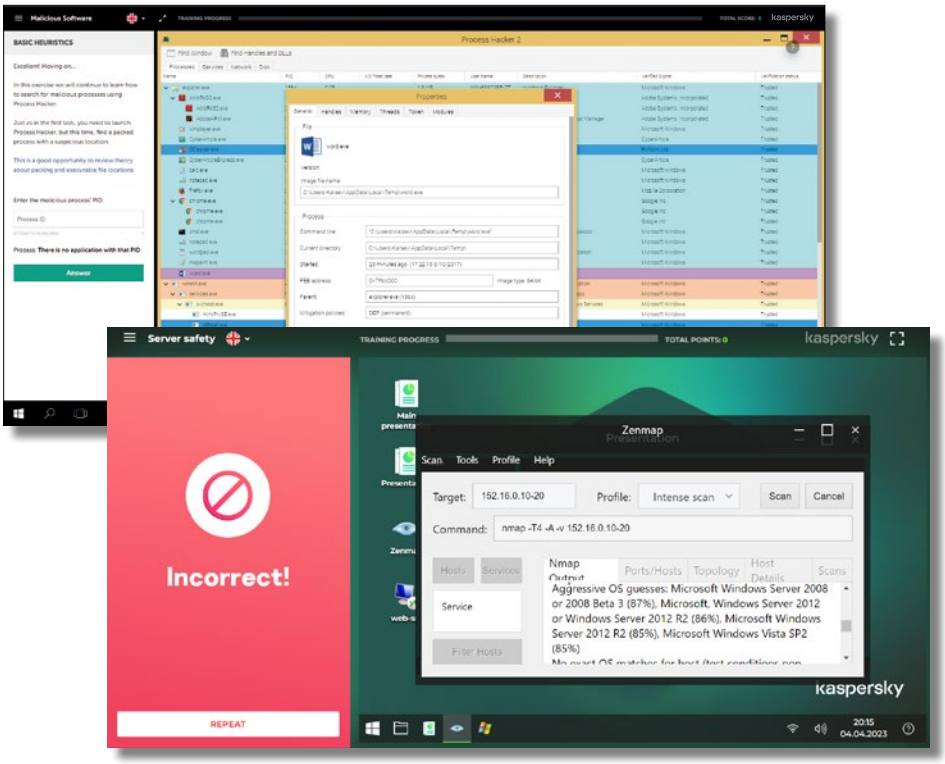
Each learning exercise block consists of two parts: education and practice, with tasks simulating real processes related to previous explanations.



* for the latest list of topics please check cito.kaspersky.com

When you've finished working through the lesson, please complete the task

If you did well, you will be directed to the next exercise block and if you didn't do too well, you can use the hints or re-read the lesson material to refresh your knowledge

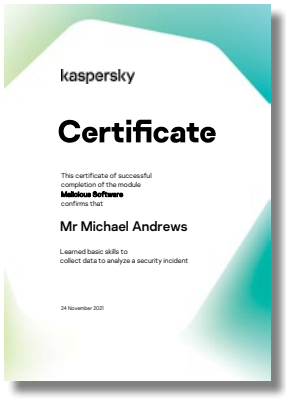


Who is this training for?

This training is recommended for all IT specialists within the organization, especially service desks and system administrators. But most non-expert IT security team members will benefit from this course too.

Certificates

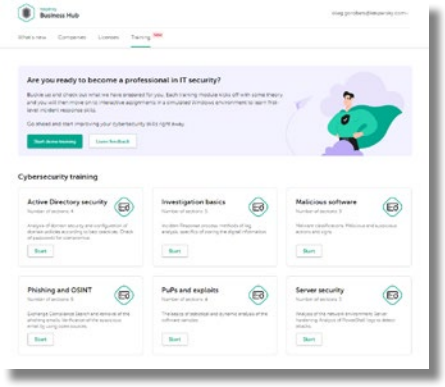
Personal certificates are available for employees after the completion of each module



Training topics and outcomes

Module name	Target audience	Knowledge gained	Personal attitude	Skills gained	Practice given in module
Malicious Software	Users with administrated rights on servers and/or workstations	Malware techniques and classification Malicious and suspicious software actions and signs Heuristic analysis basics	Malware can exist anywhere on the computer Malware can steal data in multiple non-trivial ways It is mandatory to report all suspicious potential incidents to the security team	Verification of the existence or absence of a malware-related incident	Using ProcessHacker, Autoruns, Fiddler, Gmer tools for detecting malware

Module name	Target audience	Knowledge gained	Personal attitude	Skills gained	Practice given in module
Potentially unwanted programs and files (PuPs)	Users with the rights to install additional software, and users who actively evaluate/ open files received from the outside	The basics of statistical and dynamic analysis of software samples and suspicious documents	Documents (pdf, docx) can contain exploits Unsigned files can contain malware or riskware All unsigned executables should be checked for possible infection A digital signature does not guarantee that the file doesn't contain malicious functionality	Working with system and sandbox event monitors Using statistical engines Removing PuPs	Static (signature) and statistical (virustotal) analysis of the software samples Using procmon, to search for exploits and malicious behavior of software File analysis with Cuckoo sandbox Creating scripts for malware removal using AVZ
Investigation basics	IT employees involved in the forensic or incident response activities led by the security team	The Incident Response process Methods of log analysis Specifics of storing digital information	If you suspect a cybersecurity incident, immediately report it to the security team and collect digital evidence Analysis should be done under the supervision of and in co-operation with the security team	Collecting digital evidence NetFlow traffic analysis Timeline analysis Event log analysis	Collecting volatile and non-volatile data (FTK-imager) Log analysis to find the source and the links of the attack (eventlogexplorer) Lateral movement investigation by NetFlow analysis (ntop) Disk analysis using Autopsy
Phishing and Open source intelligence (OSINT)	IT employees involved in forensic or incident response activities	Modern phishing methods Methods of analysis for email headers	Phishing can be very sophisticated, making it hard to discover, but it can always be detected by manual investigation Phishing emails need to be deleted from user' mailboxes	Phishing email analysis and deleting obfuscated phishing emails from users' mailboxes Open source intelligence for understanding what hackers know about your company	Search and removal of the phishing emails in Exchange Mailbox Using Recon-ng for web reconnaissance
Server security	Server administrators	Analyze the network environment Server hardening Analyze PowerShell logs to detect attacks	Network perimeter compromise is one of the major attack vectors. It's impossible to close all vulnerabilities - you need to reduce the attack surface to make it as hard as possible for an attack to succeed. Even if it doesn't stop an intruder, it will buy you time for detection.	Search for vulnerable and non-standard network services Configure systems according to the 'default deny' principle Search for signs of an attack in PowerShell logs	Use Nmap to find vulnerable network services Configure Software Restriction Policies for program control and Windows Firewall for network control Analyze events using Event Log Explorer
Active Directory Security	Active Directory administrators	Use an API to check passwords in a database of compromised passwords Configure domain policies according to recommendations Methods for analyzing Active Directory domain security	Default Active Directory configuration is not optimal from security point of view. Attacker can elevate their privileges in many ways. Study security recommendations, use tools which provide better visibility for Active Directory	Safely check for password hashes in a database Search for inconsistencies between recommended and actual domain policies Assess the security of Active Directory settings	Use the Have I Been Pwned? API to search the database of compromised passwords Use Policy Analyzer to compare current domain policies with best practices Use Ping Castle reports



Integration with Kaspersky Endpoint Security Cloud

Boost your cybersecurity skills and get the most out of specialized cybersecurity products with CITO training, available for KES Cloud Pro users directly from the Business Hub.

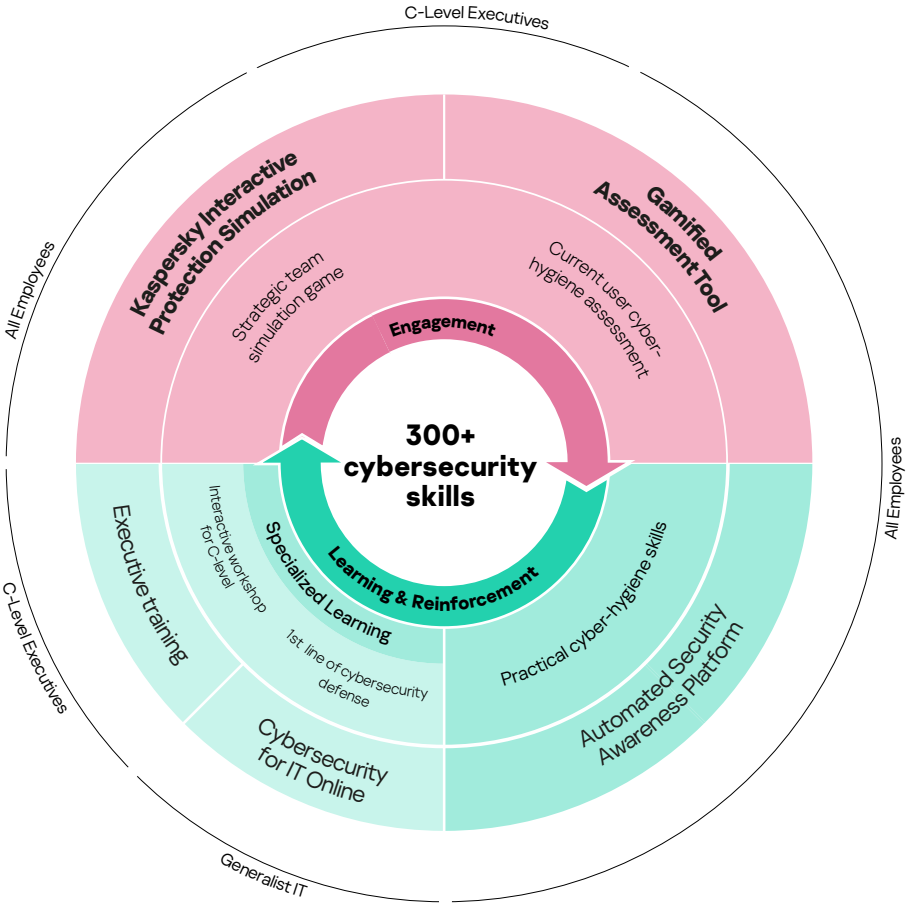
Kaspersky Security Awareness – a new approach to mastering IT security skills

One flexible training solution for all

Kaspersky Security Awareness has a longstanding international track record of success. Used by businesses of every size to **train over a million employees across more than 75 countries**, it brings together over 25 years of Kaspersky's cybersecurity expertise with extensive experience in adult education.

The portfolio offers a range of engaging training options that increase the cybersecurity awareness of your employees at every level, empowering them to play their part in the overall cybersecurity of your organization.

Because sustainable changes in behavior take time, our approach involves building a continuous learning cycle with multiple components. Game-based learning engages senior management, turning them into advocates of cybersecurity initiatives and supporters of building a culture of cybersafe behavior. Gamified assessment helps to define gaps in employee knowledge and motivate them for further learning, while online platforms and simulations equip them with the right skills, reinforced.



Key program differentiators

Substantial cybersecurity expertise
25+ years' experience in cybersecurity transformed into a cybersafety skillset that lies at the heart of our products

Training that changes employees' behavior at every level of your organization
Our gamified training provides engagement and motivation through edutainment, while the learning platforms help to internalize the cybersecurity skillset to ensure that learnt skills don't get lost along the way.

Enterprise Cybersecurity: www.kaspersky.com/enterprise
Kaspersky Security Awareness: www.kaspersky.com/awareness
Kaspersky Cybersecurity for IT Online: cito.kaspersky.com

www.kaspersky.com

kaspersky bring on the future