

First-line Incident Response training for general IT specialists

2022

Cybersecurity for IT **Online**



Free trial: cito-training.com

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.

Serverselay 😑 -				
	Control for a first sector to a secto	Eve Endersteine E	Falls Falls W W	

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.



If you didn't manage to execute the task correctly, you will be prompted to attempt and pass the educational part again.



If you did well, you will be directed to the next exercise block.

Certificates

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

kaspersky Certificate	
This certificate of successful comparison of the module Maldous Bofurent confirm that: Definition of the Configuration of the Configuration collect data to analyze a socurity moder.	
Nom20	

🗮 Malicious Software 🛛 🛟 -	TRAINING PROGRESS						TOTAL	scon: • kaspersky	
				Process Hacker 2				– 🗖 ×	
	n Find Window all Find Handles and DLLs								
	Browners Society Netwo	nik Diek							
	Name	Local address	Local port	Remote address	Remote port	Protocol	State	Ouner	
	El System (de Process(1)	192 168 152 2	42108			TCP	Time wait	N/A	
	System (de Process(1)	192.168.152.2	49188			TCP	Time welt	N/A	
	System(4)	192 168 152 2	139			TOP	Listen	N/A	
	System(4)	0.0.0.0	445			TCP	Listen	N/A	
	System(4)		445			TCP6	Listen	N/A	
	E System(4)	192.168.152.2	137			UDP	Unknown	N/A	
	System(4)	192.168.152.2	138			UDP	Unknown	N/A	
	C uTorrent exe(1976)	127.0.0.1	10000			TOP	Listen	N/A	
	C uTorrent.exe(1976)	0.0.0	51723			TCP	Listen	N/A	
	(uTorrent exe(1976)		51723			TCP6	Listen	N/A	
	(uToment, exe(1976)	0.0.0.0	1900			UDP	Unknown	N/A	
	C uTorrent.exe(1976)	0.0.0	51723			UDP	Unknown	N/A	
	(uTorrent exe(1976)	192.168.166.129	62971			UDP	Unknown	N/A	
	(S) uTorrent.exe(1976)	127.0.0.1	62972			UDP	Unknown	N/A	
	(uTorrent exe(1976)		51723			UDP6	Unknown	N/A	
	(S uToment.exe(1976)	192,168,166,129	51732	11.83.102.6	6781	TOP	Unknown	N/A	
111-1-1-1	(S) uTorrent.exe(1976)	192.168.166.129	51733	72.192.87.90	9230	TCP	Unknown	N/A	
wrong	(uTorrent exe(1976)	192,168,166,129	51734	88.201.72.1	7288	TCP	Unknown	N/A	
	utorrentie.exe(2676)	127.0.0.1	63616			UDP	Unknown	N/A	
	 Telegram.eve(2028) 	192.168.202.128	60694	149.154.167.51	443	TCP	SYN sent	N/A	
	Chrome.exe(2204)	WIN-658C3R5L7TN	60997	kaspersky.com	443	TOP	Established	N/A	
	Chrome.exe(2204)	WIN-658C3R5L7TN	60297	facebook.com	443	TCP	Established	N/A	
	chrome.exe(2204)	WIN-6S8C3R5L7TN	60092	github.com	80	TCP	Established	N/A	
	chrome.exe(2204)	WIN-658C3R5L7TN	58200	google.com	80	TCP	Established	N/A	
	😨 firefax.exe(2732)	WIN-6S8C3R5L7TN	7809	mail.google.com	443	TOP	Established	N/A	
	😨 firefax.exe(2732)	WIN-6S8C3R5L7TN	60297	vik.com	443	TCP	Established	N/A	
	😻 firefax.exe(2732)	WIN-6S8C3R5L7TN	48029	bitbucket.org	80	TCP	Established	N/A	
CONTINUE	😻 firefax.exe(2732)	WIN-6S8C3R5L7TN	49030	pastebin.com	80	TCP	Established	N/A	
	willogon.exe(1650)	127.0.0.1	12750	k97mq6mqob412xzpxalfq.dynchs.org	8080	TCP	Established	N/A	
	🛋 🔝 🐨 👀) 🔹 🖀 🗉 🛋 I	a (A)					17:56 03/11/2017	
								17:56	
		S (2 🛛				∧ ⊡ // d0	ENG 03.11.2017	

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.



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
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

Module	Target	Knowledge	Personal	Skills	Practice given
name	audience	gained	attitude	gained	in module
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

Contact us

To arrange a demo, price inquiries and delivery information please contact your Kaspersky manager, or email awareness@kaspersky.com

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

Key program differentiators



Substantial cybersecurity expertise 20+ 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. Kaspersky Security Awareness offers a diverse range of solutions covering all the cybersafety-specific needs of enterprises, and teaches the skills everyone needs using the latest learning techniques and technologies.

One flexible training solution for all

Choose a single solution that addresses a specific security need, or let us provide packages that make it easy for you to launch and target training according to all your needs and priorities. You can find more information about packages here: kaspersky.com/awareness





www.kaspersky.com

