First Line Incident Response Training for General IT Specialists

2019

Cybersecurity for IT Online

kaspersky

Learn more on kaspersky.com

Cybersecurity for IT Online (CITO)

Interactive training to build strong cybersecurity and first-level incident response skills for general IT specialists

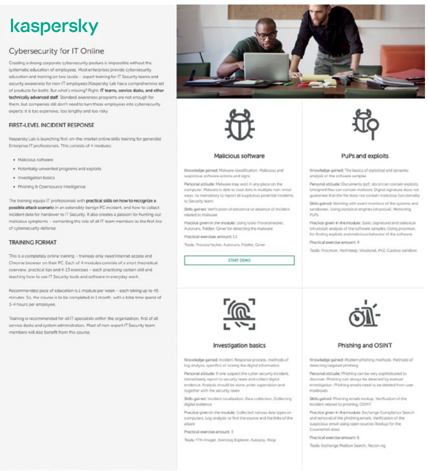
Creating a strong corporate cybersecurity posture is impossible without the systematic education of all relevant employees. Most enterprises provide cybersecurity education and training on two levels – expert training for IT Security teams and security awareness for non-IT employees (Kaspersky has a comprehensive set of products for both). But what's missing? Right: IT teams, service desks, and other technically advanced staff. Standard awareness programs are not enough for them, but companies still don't need to turn these employees into cybersecurity experts: it is too expensive, too lengthy and too risky.

Training format

This is a completely online training – trainees only need Internet access and Chrome browser on their PC. Each of 4 modules consists of a short theoretical overview, practical tips and 4 to 10 exercises – each practicing certain skill and teaching how to use IT Security tools and software in everyday work.

Study is intended take be spread over the course of a year. The recommended rate of progress is 1 exercise per week – each exercise taking from 5 up to 45 minutes to complete.

Current edition of training is targeted to Windows corporate environment.



kaspersky

Cybersecurity for IT Online

Creating a strong corporate cybersecurity posture is impossible without the systematic education of 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 Lab has a comprehensive set of products for both). But what's missing? Right: **IT teams, service desks, and other technically advanced staff**. Standard awareness programs are not enough for them, but companies still don't need to turn these employees into cybersecurity experts: it is too expensive, too lengthy and too risky.

FIRST-LEVEL INCIDENT RESPONSE

Kaspersky Lab is launching first-on-the-market online skills training for generalist Enterprise IT professionals. This consists of 4 modules:

- Malicious software
- Potentially unwanted programs and exploits
- Investigation basics
- Phishing & Opensource Intelligence

The training equips IT professionals with **practical skills on how to recognize a possible attack scenario** in an ostensibly benign PC incident, and how to collect incident data for handover to IT Security. It also creates a passion for hunting out malicious symptoms – cementing the role of all IT team members as the first line of cybersecurity defense.

TRAINING FORMAT

This is a completely online training – trainees only need Internet access and Chrome browser on their PC. Each of 4 modules consists of a short theoretical overview, practical tips and 4-13 exercises – each practicing certain skill and teaching how to use IT Security tools and software in everyday work.

Recommended pace of education is 1 module per week – each taking up to 45 minutes. So, the course is to be completed in 1 month, with a total time spend of 3-4 hours per employee.

Training is recommended for all IT specialists within the organization, first of all service desks and system administrators. Most of non-expert IT Security team members will also benefit from this course.

Malicious software

Knowledge gained: Malware classification. Malicious and suspicious software actions and signs

Personal attitude: Malware may exist in any place on the computer. Malware is able to steal data in multiple non-trivial ways. Its mandatory to report all suspicious potential incidents to Security team

Skills gained: Verification of existence or absence of incident related to malware

Practice given in the module: Using tools ProcessHacker, Autoruns, Fiddler, Gmer for detecting the malware

Practical exercises amount: 13

Tools: ProcessHacker, Autoruns, Fiddler, Gmer

START DEMO

PuPs and exploits

Knowledge gained: The basics of statistical and dynamic analysis of the software samples

Personal attitude: Documents (pdf, docx) can contain exploits. Unsigned files can contain malware. Digital signature does not guarantee that the file does not contain malicious functionality

Skills gained: Working with event monitors of the systems and sandboxes. Using statistical engines (virustotal). Removing PUPs

Practice given in the module: Static (signature) and statistical (virustotal) analysis of the software samples. Using procmon, for finding exploits and malicious behavior of the software

Practical exercise amount: 4

Tools: Procmon, Hashdeep, Virustotal, AYZ, Cuckoo sandbox

Investigation basics

Knowledge gained: Incident Response process, methods of log analysis, specifics of storing the digital information

Personal attitude: If one suspect the cyber security incident, immediately report to security team and collect digital evidence. Analysis should be done under supervision and together with the security team

Skills gained: Incident localization, Data collection, Collecting digital evidence

Practice given in the module: Collected various data types on computers. Log analysis to find the source and the links of the attack

Practical exercise amount: 5

Tools: FTK-imeger, Eventlog Explorer, Autopsy, Ntop

Phishing and OSINT

Knowledge gained: Modern phishing methods. Methods of detecting targeted phishing

Personal attitude: Phishing can be very sophisticated to discover. Phishing can always be detected by manual investigation. Phishing emails need to be deleted from user mailboxes

Skills gained: Phishing emails lookup. Verification of the incident related to phishing. OSINT

Practice given in the module: Exchange Compliance Search and removal of the phishing emails. Verification of the suspicious email using open sources (lookup for the Counterfeit data)

Practical exercise amount: 6

Tools: Exchange Mailbox Search, Recon-ng

First-line incident response

Kaspersky is launching first-on-the-market online skills training for generalist Enterprise IT professionals. It consists of 4 modules:

- Malicious software
- Potentially unwanted programs and files
- Investigation basics
- Phishing incident response

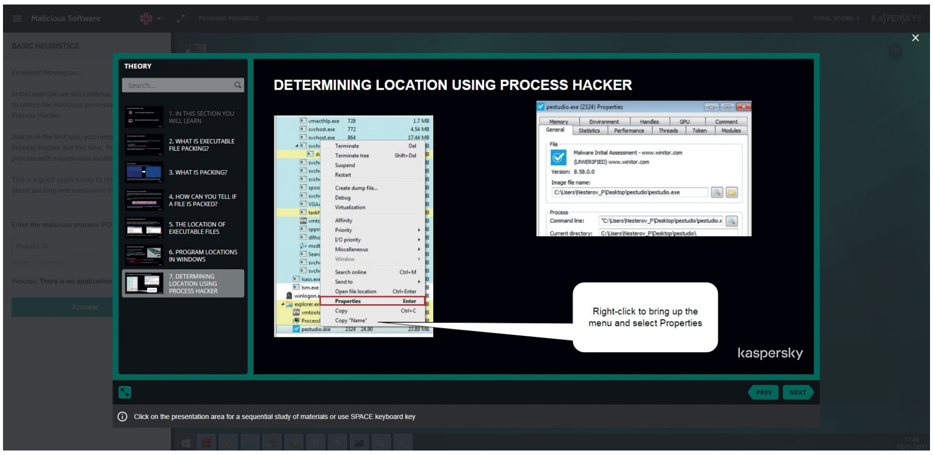
Training program equips IT professionals with practical skills on how to recognize a possible attack scenario in an ostensibly benign PC incident, and how to collect incident data for handover to IT Security. It also creates a passion for hunting out malicious symptoms – cementing the role of all IT team members as the first line of security defense.

Why CITO training is effective?

- Interactive: stimulation of real process but without risk for the computer
- Create skills not only knowledge: learning by doing
- Intuitive learning process: convenient navigation and hints:
- Covered main IT security topics and problems general IT is facing in his job
- Online: only internet connection/ access to corporate LMS and Chrome browser needed

Learning process

Each learning exercise block consists of educational part and practice – real process simulation with the task related to the previous explanations.



Excellent! Moving on...

In this exercise we will continue to search for malicious processe... Process Hacker.

Just as in the first task, you need... Process Hacker, but this time, fi... process with a suspicious locati...

This is a good opportunity to re... about packing and executable fi...

Enter the malicious process' PID

Process ID

Process: There is no application

1. IN THIS SECTION YOU WILL LEARN
2. WHAT IS EXECUTABLE FILE PACKING?
3. WHAT IS PACKING?
4. HOW CAN YOU TELL IF A FILE IS PACKED?
5. THE LOCATION OF EXECUTABLE FILES
6. PROGRAM LOCATIONS IN WINDOWS
7. DETERMINING LOCATION USING PROCESS HACKER

DETERMINING LOCATION USING PROCESS HACKER

```
vmacthlp.exe   728        1.7 MB
svchost.exe    772       4.54 MB
svchost.exe    864      17.44 MB
pestudio.exe   2324 24.90  23.89 MB
```

File: Malware Initial Assessment - www.winitor.com (UNVERIFIED) www.winitor.com

Version: 8.58.0.0

Image file name: C:\Users\Nesterov_P\Desktop\pestudio\pestudio.exe

Process

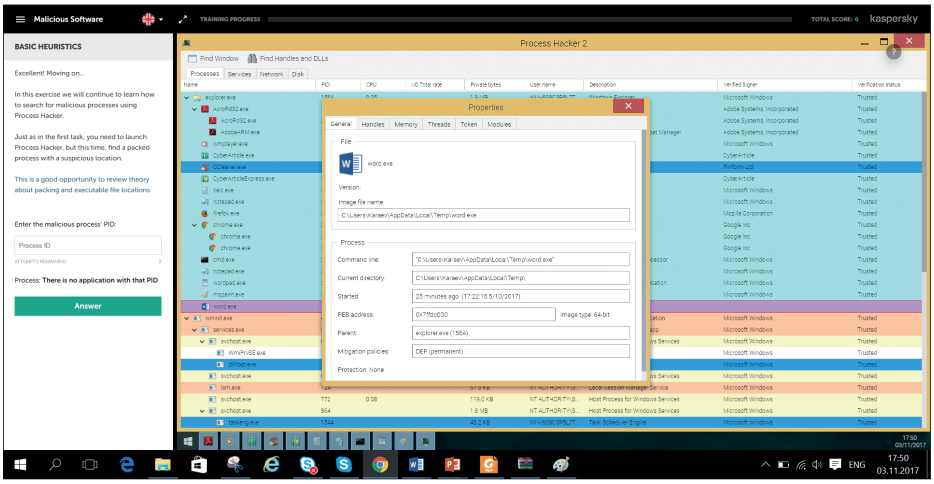
Command line: "C:\Users\Nesterov_P\Desktop\pestudio\pestudio.exe

Current directory: C:\Users\Nesterov_P\Desktop\pestudio\

Right-click to bring up the menu and select Properties

Click on the presentation area for a sequential study of materials or use SPACE keyboard key

In case you didn't manage to execute the task correctly you will be proposed to pass an educational part once again.



BASIC HEURISTICS

Excellent! Moving on...

In this exercise we will continue to learn how to search for malicious processes using Process Hacker.

Just as in the first task, you need to launch Process Hacker, but this time, find a packed process with a suspicious location.

This is a good opportunity to review theory about packing and executable file locations

Enter the malicious process' PID:

Process ID

ATTEMPTS REMAINING: 3

Process: **There is no application with that PID**

Answer

Name	PID	CPU	I/O Total rate	Private bytes	User name	Description	Verified Signer	Verification status
explorer.exe	1564	0.05		1.9 MB	WIN-6S8C3R5L7T	Windows Explorer	Microsoft Windows	Trusted
AcroRd32.exe							Adobe Systems, Incorporated	Trusted
AcroRd32.exe							Adobe Systems, Incorporated	Trusted
AdobeARM.exe						at Manager	Adobe Systems, Incorporated	Trusted
wmplayer.exe							Microsoft Windows	Trusted
CyberArticle.exe							CyberArticle	Trusted
CCleaner.exe							Piriform Ltd	Trusted
CyberArticleExpress.exe							CyberArticle	Trusted
calc.exe							Microsoft Windows	Trusted
notepad.exe							Microsoft Windows	Trusted
firefox.exe							Mozilla Corporation	Trusted
chrome.exe							Google Inc	Trusted
chrome.exe							Google Inc	Trusted
chrome.exe							Google Inc	Trusted
cmd.exe						ocessor	Microsoft Windows	Trusted
notepad.exe							Microsoft Windows	Trusted
wordpad.exe						ication	Microsoft Windows	Trusted
mspaint.exe							Microsoft Windows	Trusted
word.exe								
wininit.exe						ation	Microsoft Windows	Trusted
services.exe						app	Microsoft Windows	Trusted
svchost.exe						ws Services	Microsoft Windows	Trusted
WmiPrvSE.exe							Microsoft Windows	Trusted
dllhost.exe							Microsoft Windows	Trusted
svchost.exe						ws Services	Microsoft Windows	Trusted
lsm.exe	724			57.5 KB	NT AUTHORITY\S...	Local Session Manager Service	Microsoft Windows	Trusted
svchost.exe	772	0.08		119.0 KB	NT AUTHORITY\S...	Host Process for Windows Services	Microsoft Windows	Trusted
svchost.exe	864			1.8 MB	NT AUTHORITY\S...	Host Process for Windows Services	Microsoft Windows	Trusted
taskeng.exe	1544			48.2 KB	WIN-6S8C3R5L7T...	Task Scheduler Engine	Microsoft Windows	Trusted

File

word.exe

Version:

Image file name: C:\Users\Karaev\AppData\Local\Temp\word.exe

Process

Command line: "C:\Users\Karaev\AppData\Local\Temp\word.exe"

Current directory: C:\Users\Karaev\AppData\Local\Temp\

Started: 25 minutes ago (17:22:15 5/10/2017)

PEB address: 0x7ffdc000 Image type: 64-bit

Parent: explorer.exe (1564)

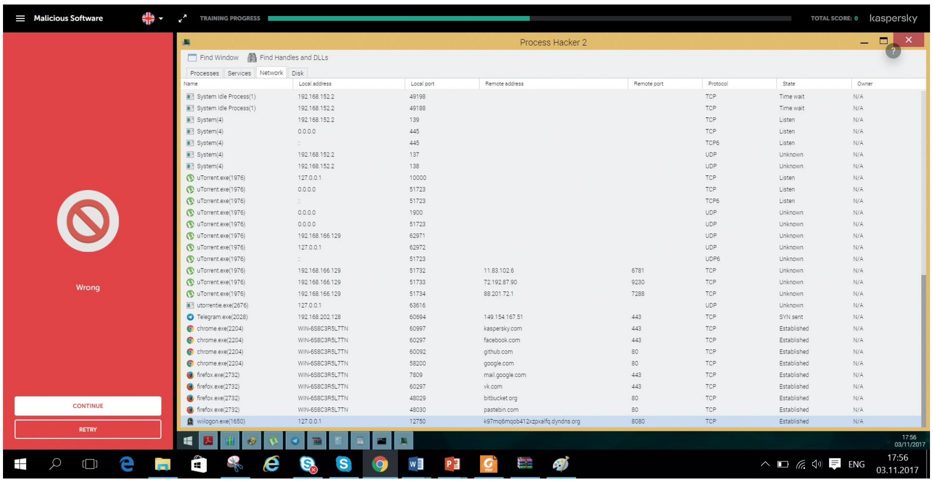
Mitigation policies: DEP (permanent)

Protection: None

17:50
03/11/2017

ENG 17:50
03.11.2017

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



Wrong

CONTINUE

RETRY

Name	Local address	Local port	Remote address	Remote port	Protocol	State	Owner
System Idle Process(1)	192.168.152.2	49198			TCP	Time wait	N/A
System Idle Process(1)	192.168.152.2	49188			TCP	Time wait	N/A
System(4)	192.168.152.2	139			TCP	Listen	N/A
System(4)	0.0.0.0	445			TCP	Listen	N/A
System(4)	::	445			TCP6	Listen	N/A
System(4)	192.168.152.2	137			UDP	Unknown	N/A
System(4)	192.168.152.2	138			UDP	Unknown	N/A
uTorrent.exe(1976)	127.0.0.1	10000			TCP	Listen	N/A
uTorrent.exe(1976)	0.0.0.0	51723			TCP	Listen	N/A
uTorrent.exe(1976)	::	51723			TCP6	Listen	N/A
uTorrent.exe(1976)	0.0.0.0	1900			UDP	Unknown	N/A
uTorrent.exe(1976)	0.0.0.0	51723			UDP	Unknown	N/A
uTorrent.exe(1976)	192.168.166.129	62971			UDP	Unknown	N/A
uTorrent.exe(1976)	127.0.0.1	62972			UDP	Unknown	N/A
uTorrent.exe(1976)	::	51723			UDP6	Unknown	N/A
uTorrent.exe(1976)	192.168.166.129	51732	11.83.102.6	6781	TCP	Unknown	N/A
uTorrent.exe(1976)	192.168.166.129	51733	72.192.87.90	9230	TCP	Unknown	N/A
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.exe(2028)	192.168.202.128	60694	149.154.167.51	443	TCP	SYN sent	N/A
chrome.exe(2204)	WIN-6S8C3R5L7TN	60997	kaspersky.com	443	TCP	Established	N/A
chrome.exe(2204)	WIN-6S8C3R5L7TN	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-6S8C3R5L7TN	58200	google.com	80	TCP	Established	N/A
firefox.exe(2732)	WIN-6S8C3R5L7TN	7809	mail.google.com	443	TCP	Established	N/A
firefox.exe(2732)	WIN-6S8C3R5L7TN	60297	vk.com	443	TCP	Established	N/A
firefox.exe(2732)	WIN-6S8C3R5L7TN	48029	bitbucket.org	80	TCP	Established	N/A
firefox.exe(2732)	WIN-6S8C3R5L7TN	48030	pastebin.com	80	TCP	Established	N/A
wiilogon.exe(1650)	127.0.0.1	12750	k97mq6mqob412xzpxalfq.dyndns.org	8080	TCP	Established	N/A

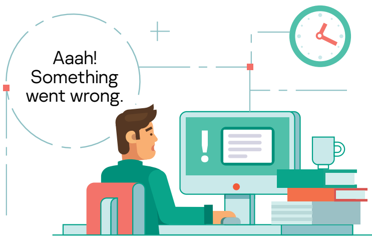
17:56
03/11/2017

ENG 17:56
03.11.2017

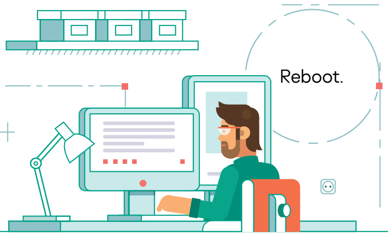
Whom to train

Training is recommended for all IT specialists within the organization, first of all service desks and system administrators. Most of non-expert IT Security team members will also benefit from this course.

Now



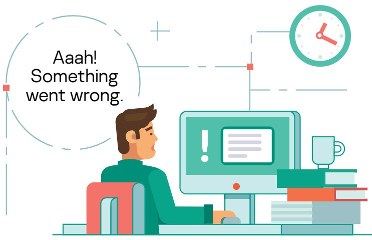
User



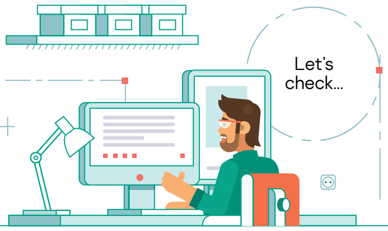
IT Support/Admins

IT Security

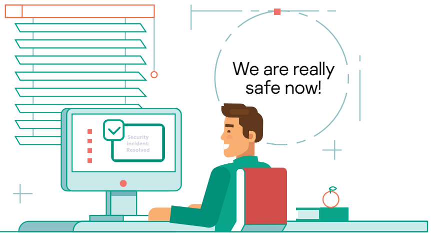
Should be



User



IT Support/Admins



IT Security

Training outcomes and topics covered

Module name	Target audience	Knowledge gained	Personal attitude	Skills gained	Practice given in module
Malicious Software	Users with administrator rights on servers and/or workstations	Malware techniques and classification Malicious and suspicious software actions and signs Heuristic analysis basics	Malware may exist in any place on the computer Malware is able to steal data in multiple non-trivial ways It is mandatory to report all suspicious potential incidents to Security team	Verification of existence or absence of incident related to malware	Using tools ProcessHacker, Autoruns, Fiddler, Gmer 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 the 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 Digital signature does not guarantee that the file does not contain malicious functionality	Working with event monitors of systems and sandboxes 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 malware removal scripts using AVZ
Investigation basics	IT employees involved in the forensic or incident response activities led by Security team	Incident Response process, methods of log analysis, specifics of storing digital information	If you suspect a cyber security incident, immediately report to security team and collect digital evidence Analysis should be done under supervision of the security team and in co-operation with them	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 email headers analysis	Phishing can be very sophisticated to discover. Phishing 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	Exchange Mailbox Search and removal of the phishing emails Using Recon-ng for web reconnaissance

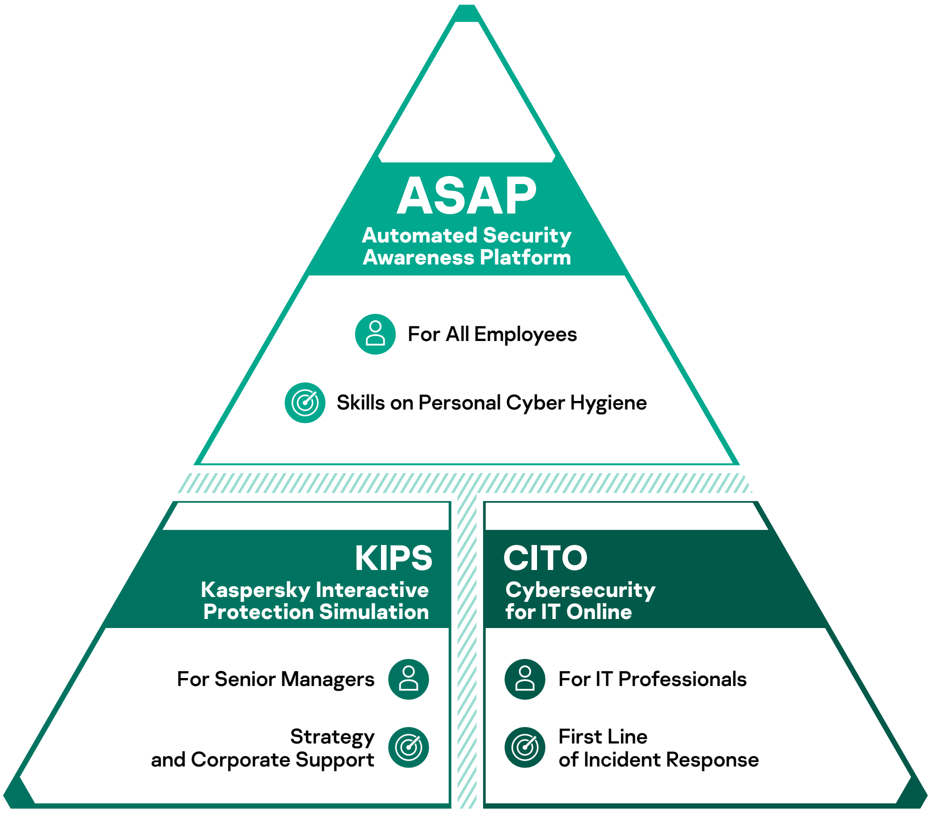
Contact us

For demo, price and delivery information please address your Kaspersky Lab manager, or email awareness@kaspersky.com

Kaspersky®
Security
Awareness

Kaspersky offers computer-based training products that combine more than 20 years expertise in cybersecurity and the best known educational technologies and practices.

This approach ensures training effectiveness: changes users behavior and helps create cybersafe environment throughout an organization.


ASAP
Automated Security Awareness Platform
For All Employees
Skills on Personal Cyber Hygiene
KIPS
Kaspersky Interactive Protection Simulation
For Senior Managers
Strategy and Corporate Support
CITO
Cybersecurity for IT Online
For IT Professionals
First Line of Incident Response

Kaspersky Security Awareness comprises of 3 elements which intermesh, but which are also fully effective if used separately.

- **Skills** instead of just knowledge
- **Computer-based –** easy delivery, management & measurement
- **Real life examples & practical exercises –** students engagement and motivation
- **Clear training structure and latest L&D technologies** – easy for administrators, efficient for students

Enterprise Cybersecurity: www.kaspersky.com/enterprise
Kaspersky Security Awareness: www.kaspersky.com/awareness

www.kaspersky.com

kaspersky

**BRING ON
THE FUTURE**