KASPERSKY lab

Cybersecurity for IT Online

First line incident response training for general IT specialists

kaspersky.com/awareness
#truecybersecurity

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 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.

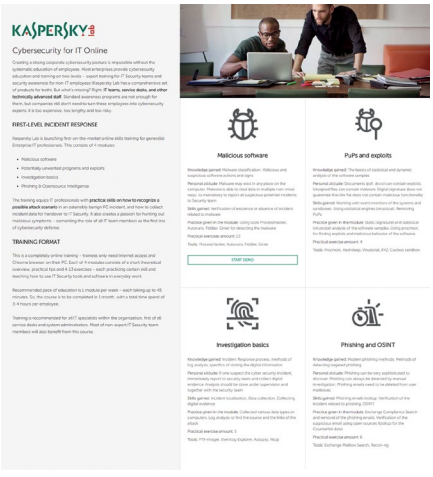
Training format

This is a completely online training – trainees only need Internet access and Chrome browser on their PC. Each of 5 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.

The course is targeted for 1 year. Recommended pace of education is 1 module per week – each taking up to 45 minutes.

Current edition of training is targeted to Windows corporate environment.

Current edition of training is targeted to Windows corporate environment.



First-line incident response

Kaspersky Lab is launching first-on-the-market online skills training for generalist Enterprise IT professionals. It consists of 5 modules:

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

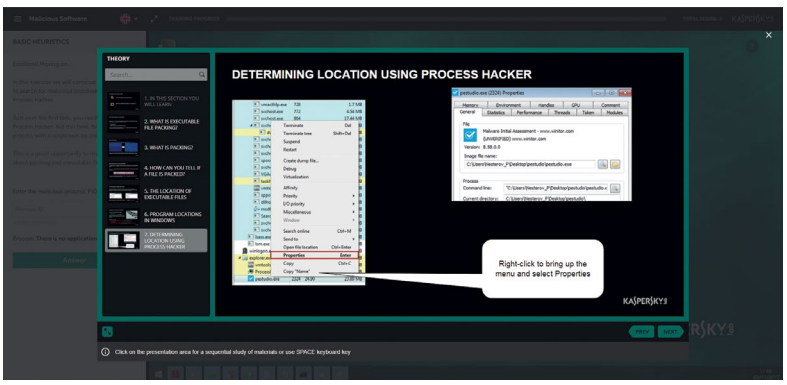
Training program equips IT professionals with practical skills on how to recognize a possible attack scenario in an ostensibly benign PC incident, and how to collect incident data for handover to IT Security. It also creates a passion for hunting out malicious symptoms – cementing the role of all IT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

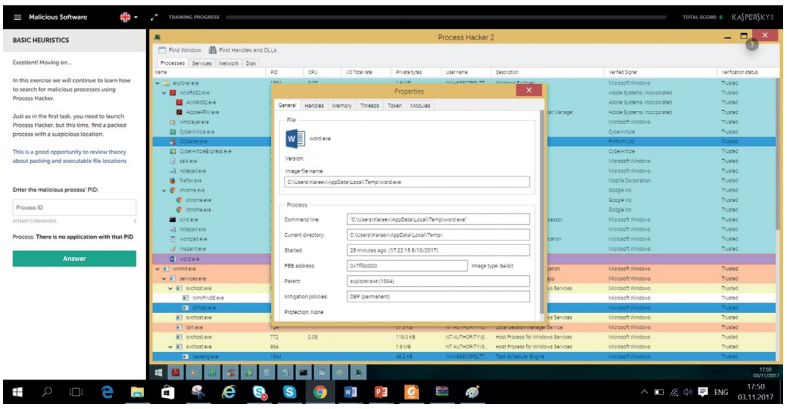
Why CITO training is effective?

- **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

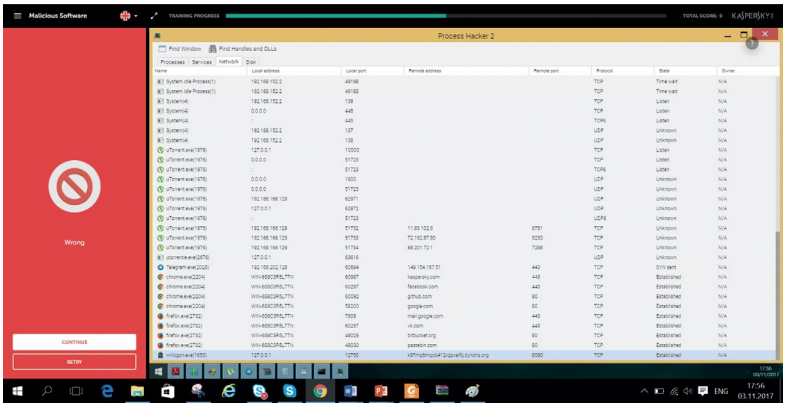
Learning process

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





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

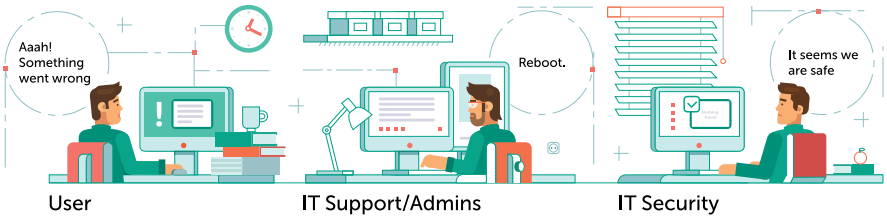


If you did the task well you will be directed to the next exercise block.

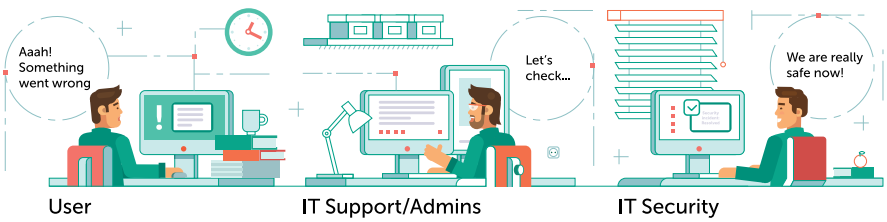
Whom to train

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



Should be



Training Outcomes And Topics Covered

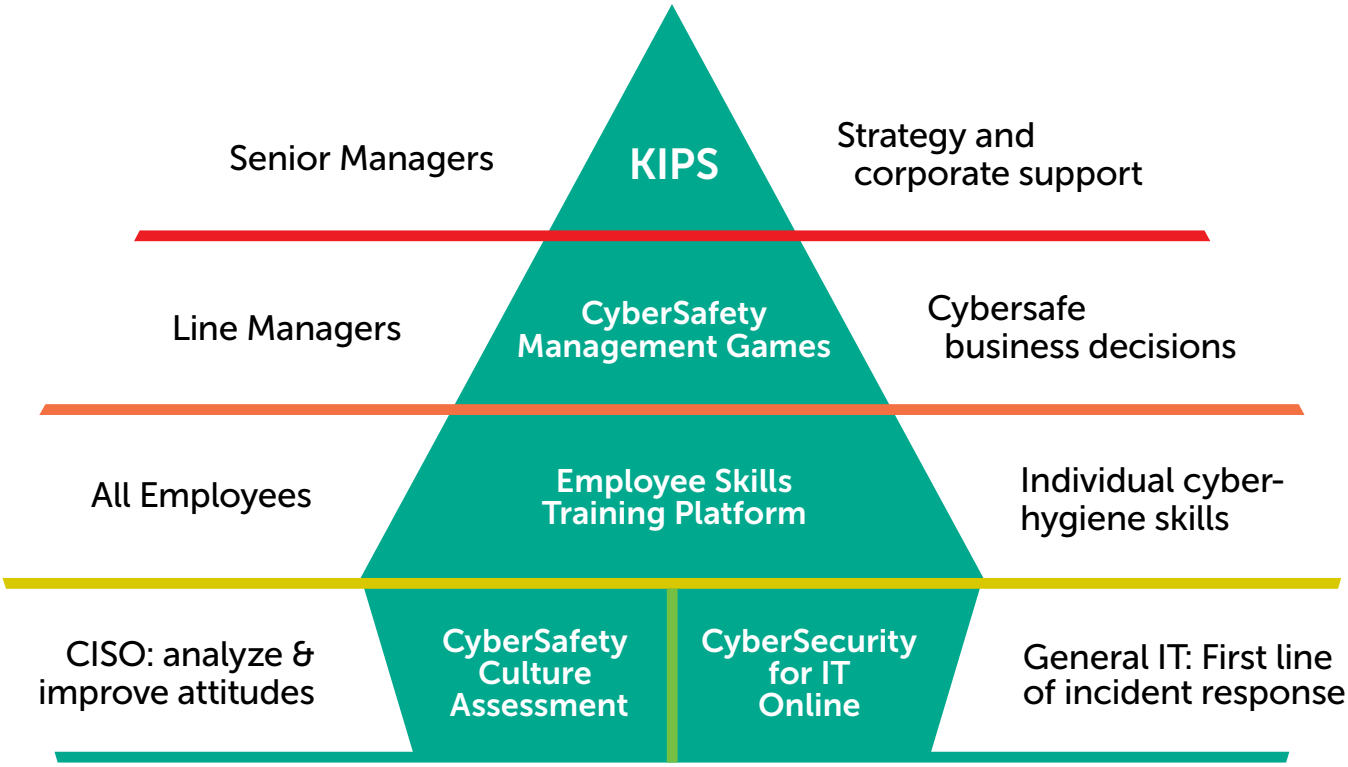
Module name	Target audience	Knowledge gained	Personal attitude	Skills gained	Practice given in module
Malicious Software	Users with administrator rights on servers and/or workstations	Malware techniques and classification Malicious and suspicious software actions and signs Heuristic analysis basics	Malware 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
Enterprise Security	IT specialists involved in setup, configuration and administration of internal or external servers and systems	Methods of assessment of the security of individual systems Layered security Various Security Software	If you don't have security setup instructions, follow the layered security approach. Antivirus is always a must Principle of making attack successful more expensive that the gain from the attack	Verifying server security settings when nesting the system/ server from colleagues or suppliers Testing password strength Secure server setup Vulnerability lookup and patching	Windows server security assessment and setup

Contact us

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

Kaspersky® Security Awareness

Kaspersky Lab has launched a family of computer-based training products that utilize modern learning techniques and address all levels of organizational structure. This approach helps create collaborative CyberSafety Culture which ensures a self-sustained state of cybersecurity throughout the organization.



Setting objectives & choosing a program

Setting goals based on KL global data

Comparison with world/ industry average

Learning management

Learning automation

Self-adjusting learning path

Calculation of time spends

Reporting & analytics

Actionable reports anytime

On-the-fly analysis of what can be improved

Program efficiency & appreciation

True gamification

Competition & challenge

Preventing overload

up to
90%
A decrease in a total number of incidents

not less than
50%
A decrease in a monetary volume of incidents

up to
93%
Probability of using the knowledge in the daily work

more than
30x
ROI from spending to the security awareness products

amazing
86
Willingness to recommend the program

www.kaspersky.com

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