First Line Incident Response Training for General IT Specialists

Cybersecurity for IT Online

2019

kaspersky

Learn more on kaspersky.com
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.

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.

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.
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**

- **User**: Aaah! Something went wrong.
- **IT Support/Admins**: Reboot.
- **IT Security**: It seems we are safe.

**Should be**

- **User**: Aaah! Something went wrong.
- **IT Support/Admins**: Let’s check...
- **IT Security**: We are really safe now!
## Training outcomes and topics covered

<table>
<thead>
<tr>
<th>Module name</th>
<th>Target audience</th>
<th>Knowledge gained</th>
<th>Personal attitude</th>
<th>Skills gained</th>
<th>Practice given in module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious Software</td>
<td>Users with administrator rights on servers and/or workstations</td>
<td>Malware techniques and classification</td>
<td>Malware may exist in any place on the computer</td>
<td>Verification of existence or absence of incident related to malware</td>
<td>Using tools ProcessHacker, Autoruns, Fiddler, Gmer for detecting malware</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Malicious and suspicious software actions and signs</td>
<td>Malware is able to steal data in multiple non-trivial ways</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Heuristic analysis basics</td>
<td>It is mandatory to report all suspicious potential incidents to Security team</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Potentially Unwanted programs and files (PuPs)</td>
<td>Users with the rights to install additional software, and users who actively evaluate/ open files received from the outside</td>
<td>The basics of statistical and dynamic analysis of the software samples and suspicious documents</td>
<td>Documents (pdf, docx) can contain exploits</td>
<td>Working with event monitors of systems and sandboxes</td>
<td>Static (signature) and statistical (virustotal) analysis of the software samples</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Unsigned files can contain malware or riskware</td>
<td>Using statistical engines</td>
<td>Using procmem, to search for exploits and malicious behavior of software</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>All unsigned executables should be checked for possible infection</td>
<td>Removing PuPs</td>
<td>File analysis with Cuckoo sandbox</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Digital signature does not guarantee that the file does not contain malicious functionality</td>
<td></td>
<td>Creating scripts malware removal scripts using AVZ</td>
</tr>
<tr>
<td>Investigation basics</td>
<td>IT employees involved in the forensic or incident response activities led by Security team</td>
<td>Incident Response process, methods of log analysis, specifics of storing digital information</td>
<td>If you suspect a cyber security incident, immediately report to security team and collect digital evidence</td>
<td>Collecting digital evidence</td>
<td>Collecting volatile and non-volatile data (FTK-imager)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Analysis should be done under supervision of the security team and in-co-operation with them</td>
<td>Netflow traffic analysis</td>
<td>Log analysis to find the source and the links of the attack (eventlogexplorer)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Timeline analysis</td>
<td>Lateral movement investigation by netflow analysis (ntop)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Event log analysis</td>
<td>Disk analysis using Autopsy</td>
</tr>
<tr>
<td>Phishing and Open source intelligence (OSINT)</td>
<td>IT employees involved in forensic or incident response activities</td>
<td>Modern phishing methods</td>
<td>Phishing can be very sophisticated to discover. Phishing can always be detected by manual investigation</td>
<td>Phishing email analysis and deleting obfuscated phishing emails from users mailboxes</td>
<td>Exchange Mailbox Search and removal of the phishing emails</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Methods of email headers analysis</td>
<td>Phishing emails need to be deleted from user mailboxes</td>
<td></td>
<td>Using Recon-ng for web reconnaissance</td>
</tr>
</tbody>
</table>

## Contact us

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

**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