









Kaspersky Cybersecurity Training

Kaspersky Cybersecurity Training

Kaspersky Cybersecurity Services:

-  Kaspersky Managed Detection and Response
-  Kaspersky Cybersecurity Training
-  Kaspersky Incident Response
-  Kaspersky Targeted Attack Discovery
-  Kaspersky Security Assessment
-  Kaspersky SOC Consulting

Turn good professionals into cybersecurity wizards

Kaspersky Cybersecurity Training covers a broad range of cybersecurity topics, techniques and assessments from basic to expert level. All our courses are available either as in-person classes on customer premises or at your local/regional Kaspersky office.

The courses include both theory and hands-on 'labs', for maximum engagement. On completion of each course, students can complete an evaluation to validate their knowledge.

Choose your training course

Windows Digital Forensics: basic and advanced

Improve your in-house digital forensics and incident response teams' expertise with courses specially designed to fill gaps in knowledge and experience. Students will develop and enhance their practical skills in searching for traces of digital cybercrime and analyzing different types of data for restoring attack timelines and sources. After they've completed the course, students will be able to investigate computer incidents successfully, raising the overall security level of your business.

Malware Analysis and Reverse: basic and advanced

These courses are aimed at security researchers and incident response personnel, malware analysts, security engineers, network security analysts, APT hunters and IT security staff. Students will become familiar with the scope of reverse engineering applications, assembly language, corresponding tools and common techniques used by malware authors to maintain persistence, avoid detection, inject into system process memory, and more.

The advanced course covers most of the steps required to analyze a modern APT toolkit, from receiving the initial sample all the way to producing a deep technical description using IOCs.

Windows Incident Response

The Windows Incident Response course will guide your in-house team through every stage of the incident response process and equip them with the comprehensive knowledge needed to successfully verify, contain, analyze and remediate incidents.

Efficient Threat Detection with Yara

This course will teach students how to write effective Yara rules, how to test them and improve them to the point where they find threats that nobody else does.

Program descriptions

Topics

Key skills gained

All-levels

5 days

Windows Digital Forensics

Through a simulated real-life targeted cyberattack, the course covers the following topics:

- Introduction to digital forensics
- Live response and evidence acquisition
- Post-mortem analysis of Windows machines
- MS Windows registry internals
- MS Windows events
- MS Windows artifacts analysis
- Browsers artifacts forensics
- Email analysis
- Forensics challenges with SSD disks
- Recommendations for building a digital forensics lab
- Testing the newly gained skills with a practical challenge using different Windows artifacts

- How to acquire various digital evidence and deal with it in a forensically sound environment
- Find traces of incident-related malicious activities from
- MS Windows artifacts
- Utilize time stamps from different Windows artifacts to reconstruct an incident scenario
- Find and analyze browser and email history
- Be able to apply the tools and instruments of digital forensics
- Understand the process of creating a digital forensics lab

Mid-level

5 days

Malware Analysis & Reverse Engineering

- Basic analysis using IDA Pro
- Dynamic analysis using popular virtualization solutions and debuggers
- Malicious documents analysis
- Unpacking
- Decryption
- Shellcodes analysis
- Exploit analysis
- Reverse tips and tricks

- A grounding in OS and assembly language
- Be able to conduct static and dynamic malware analysis to fully understand its behavior and functionality
- Deal with malware anti-analysis tricks, self-protective techniques and protection software bypasses
- Identify and reverse engineer standalone and embedded shellcodes
- Analyze PDF exploits from scratch

Advanced-level

5 days

Advanced Windows Digital Forensics

Through a simulated real-life targeted cyberattack, the course covers the following topics:

- Numerical systems
- FAT file system
- NTFS file system
- Data and file recovery from file system, shadow copies and using file carving
- Forensics challenges in Cloud computing
- Memory forensics
- Network forensics
- Timeline vs SuperTimeline analysis
- Testing the newly gained skills with a practical challenge with acquired digital evidence

- Conduct deep file system analysis
- Identify and recover deleted files using different techniques
- Analyze network traffic with different tools
- Identify and track malicious activities in memory dump
- Identify and dump interesting parts from memory for further analysis
- Reconstruct the incident timeline using file system timestamps
- Create a single timeline for all Windows OS artifacts to gain a better understanding of the incident scenario

Topics

Key skills gained

Advanced-level

5 days

Advanced Malware Analysis & Reverse Engineering

- Unpacking
- Decryption
- Developing own decryptors for common scenarios
- Byte code decompilation
- Code decomposition
- Disassembly
- Reconstruction of modern APT architectures
- Recognizing typical code constructs
- Identification of cryptographic and compression algorithms
- Classification and attribution based on code and data
- Class and structure reconstruction
- APT plugin architectures (based on recent APT samples)

- Be able to analyze a modern APT toolkit, from receiving the initial sample, all the way to producing a technical description of the attacker's TTPs with IOCs
- Produce static decryptors for real-life scenarios and then continuing with in-depth analysis of the malicious code
- Analyze malicious documents that are typically used to deliver initial payloads and know how to extract them
- Ensure that damage assessment and incident response efforts are accurate and effective

Mid-level

5 days

Windows Incident Response

In a simulated real-life environment, an incident will take place and the course will cover the following topics on that specific scenario:

- Introducing the incident response process and its workflow
- Explaining the difference between normal threats and APTs
- Explaining APT Cyber Kill Chain
- Applying the incident response process to different incident scenarios
- Applying Cyber Kill Chain on the simulated environment
- Applying live analysis on victim machines for first responders
- Forensically sound evidence-acquisition techniques
- Introducing post-mortem analysis and digital forensics
- Introducing memory forensics
- Log file analysis with regular expressions and ELK
- Introducing cyber threat intelligence
- Creating IoCs (Indicators of Compromise), with YARA and Suricata
- Introducing malware analysis and sandboxing
- Introducing network traffic forensics
- Discussing incident analysis reporting and recommendations on building CSIRT
- Testing the newly gained skills with a practical challenge in another simulated scenario

- Understand the phases of incident response
- What to consider while responding to a cyber incident
- Understand various attack techniques and targeted attack anatomy through the Cyber Kill Chain
- Respond to different incidents with the appropriate actions
- The ability to differentiate APTs from other threats
- Confirm cyber incidents using live analysis tools
- Understand the difference between live analysis and post-mortem - and when to apply each of them
- Identify digital evidence; HDD, memory and network traffic with an introduction on their forensics analysis
- Write YARA and Suricata rules to detect IOCs for the investigated attack
- Log file analysis
- Understand the process involved in building an IR team

All-levels

2 days

Efficient Threat Detection with Yara

- Brief intro into Yara syntax
- Tips & tricks to create fast and effective rules
- Yara-generators
- Testing Yara rules for false positives
- Hunting new undetected samples on VT
- Using external modules within Yara for effective hunting
- Anomaly search
- Lots (!) of real-life examples
- Exercises for improving your Yara skills

- Create effective Yara rules
- Test Yara rules
- Hunt for new undetected samples in your infrastructure and in cloud platforms



Kaspersky Cybersecurity Training

[Learn more](#)

www.kaspersky.com

© 2022 AO Kaspersky Lab.
Registered trademarks and service marks
are the property of their respective owners.