Kaspersky Cybersecurity Training

kaspersky

Kaspersky Cybersecurity Training

Cybersecurity education is the critical tool for enterprises faced with an increasing volume of constantly evolving threats. IT Security staff need to be skilled in the advanced techniques that form a key component of effective enterprise threat management and mitigation strategies.

These courses offer a broad curriculum in cybersecurity topics and techniques and assessment ranging from basic to expert. All are available either in-class on customer premises or at a local or regional Kaspersky office, if applicable.

Courses are designed to include both theoretical classes and hands-on 'labs'. On completion of each course, attendees will be invited to complete an evaluation to validate their knowledge.

Kaspersky Cybersecurity Services

- **Kaspersky Threat Intelligence**
- **Kaspersky Threat Hunting**
- **Kaspersky Cybersecurity Training**
  - Windows Digital Forensics
  - Malware Analysis and Reverse Engineering
  - Advanced Windows Digital Forensics
  - Advanced Malware Analysis and Reverse Engineering
  - Windows Incident Response
  - Efficient Threat Detection with Yara
- **Kaspersky Incident Response**
- **Kaspersky Security Assessment**

Service Benefits

Windows Digital Forensics and Advanced Windows Digital Forensics

Improve the expertise of your in-house digital forensics and incident response team. Courses are designed to fill experience gaps – developing and enhancing practical skills in searching for digital cybercrime tracks and in analyzing different types of data for restoring attack timelines and sources. Having completed the course, students will be able to successfully investigate computer incidents and improve the security level of the business.

Malware Analysis and Reverse Engineering and Advanced Malware Analysis and Reverse Engineering

These courses are intended for 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, common techniques used by malware authors to maintain persistence, avoid detection, inject into system processes memory etc. The advanced course will cover 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 with IOCs.

Windows Incident Response

Course will guide your in-house team through all of the stages of the incident response process and equip them with the comprehensive knowledge needed for successful incident remediation.

Efficient Threat Detection with Yara

Will help to learn how to write the most effective Yara rules, how to test them and improve them to the point where they find threats that nothing else does.

Hands-On Experience

From a leading security vendor, working and learning alongside our global experts who inspire participants through their own experience at the 'sharp end' of cybercrime detection and prevention.

Program Description

Topics	Duration	Skills gained
Windows Digital Forensics		
Through a real-life simulated cyber targeted attack incident, the course will cover the following topics: · Introducing digital forensics · Live response and evidence acquisition · Post-mortem analysis of Windows machines · Windows OS registry internals · Windows OS events · Windows OS artifacts analysis · Browsers artifacts forensics · Email analysis · Forensics challenges with SSD disks · Recommendations when building a digital forensics lab · Testing the newly gained skills with a practical challenge using different Windows artifacts	5 days	· Acquiring various digital evidence and dealing with it in forensically sound environment · Find traces of incident-related malicious activities from the Windows OS artifacts · Utilizing time stamps from different Windows artifacts to reconstruct an incident scenario · Finding and analyzing browser and email history · Be able be apply the tools and instruments of digital forensics · Understating the process of creating a digital forensics lab
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 · Reversing tips and tricks	5 days	· Get preliminary knowledge about OS and assembly language · Conduct static and dynamic malware analysis obtaining full understanding of 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 · Be able to analyze PDF exploits from scratch
Advanced Windows Digital Forensics		
Through a real-life simulated cyber targeted attack incident, the course will cover the following topics: · Numerical systems · FAT file system · NTFS file system · Deep Windows forensics · 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	5 days	· Conducting deep file system analysis · Identifying and recovering deleted files using different techniques · Analyzing network traffic with different tools · Identifying and tracking malicious activities in memory dump · Identifying and dumping interesting parts from memory for further analysis · Reconstructing the incident timeline using file system timestamps · Creating one timeline for all Windows OS artifacts for a better understating of the incident scenario
Advanced Malware Analyisis & 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)	5 days	· 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 · Producing static decryptors for real-life scenarios and then continuing with in-depth analysis of the malicious code · Be able to analyze malicious documents that are typically used to deliver initial payloads and know how to extract them · Ensuring damage assessment and incident response efforts are accurate and effective
Windows Incident Response		
· In a real-life simulated environment, an incident will take place and the course will cover the following topics on that 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 SNORT · 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	5 days	· Understanding the phases of incident response · What to consider while responding to a cyber incident · Understanding various attack techniques and targeted attack anatomy through the Cyber Kill Chain · Responding to different incidents with appropriate actions · The ability to differentiate APTs from other threats · Confirming cyber incidents using live analysis tools · Understanding the difference between live analysis and post-mortem - and when to apply each of them · Identifying digital evidence; HDD, memory and network traffic with an introduction on their forensics analysis · Writing YARA and SNORT IOCs for the detected attack · Log file analysis · Understanding the process involved in building an IR team
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 · A set of exercises for improving your Yara skills	2 days	· Create effective Yara rules · Test Yara rules · Improve them to the point where they find threats that nobody else does

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.

Know more at kaspersky.com/transparency

Proven.
Transparent.
Independent.