Kaspersky Security Training

www.kaspersky.com
#truecybersecurity

Kaspersky Security 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 Lab 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.

Service Benefits

Digital Forensics and Advanced 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

Reverse engineering training is designed to help incident responding groups in the investigation of malicious attacks. This course is intended for IT department employees and system administrators. Students will learn to analyze malicious software, to collect IoCs (Indicators of Compromise), to write signatures for detecting malware on infected machines, and to restore infected/encrypted files and documents.

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.

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.

KATA Administration

KATA Administration Training provides all the know-how required to plan, install and configure the solution in order to optimize its threat detection efficiency.

KATA Security Analyst

The training course includes a number of practical exercises based on the real threat detection scenarios providing the knowledge needed to confidently monitor, interpret and respond to KATA alerts.

Hands-On Experience

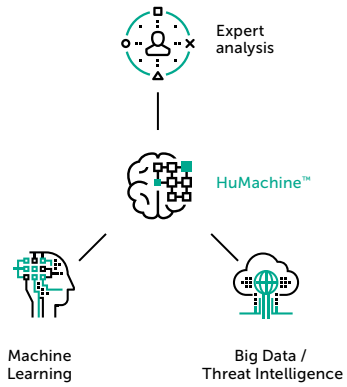
From a leading security vendor, working and learning alongside our global experts who inspire participants through their own experience at the 'sharp end' of cybercrime detection and prevention.

Program Description

Topics	Duration	Skills gained
Digital Forensics		
• Introduction to Digital Forensics • Live response and evidence acquisition • Windows registry internals • Windows artifacts analysis • Browsers forensics • Email analysis	5 days	• Build a Digital Forensics lab • Collect digital evidence and deal with it properly • Reconstruct an incident and use time stamps • Find traces of intrusion based on artifacts in Windows OS • Find and analyze browser and email history • Be able be apply with the tools and instruments of digital forensics
Malware Analysis & Reverse Engineering		
• Malware Analysis & Reverse Engineering goals and techniques • Windows internals, executable files, x86 assembler • Basic static analysis techniques (strings extracting, importanalysis, • PE entry points at a glance, automatic unpacking, etc.) • Basic dynamic analysis techniques (debugging, monitoring tools, traffic interception, etc.) • .NET, Visual Basic, Win64 files analysis • Script and non-PE analysis techniques (Batch files; Autoit; Python; Jscript; JavaScript; VBS)	5 days	• Build a secure environment for malware analysis: deploy sandbox and all necessary tools • Understand principles of Windows program execution • Unpack, debug and analyze malicious object, identify its functions • Detect malicious sites through script malware analysis • Conduct express malware analysis
Advanced Digital Forensics		
• Deep Windows Forensics • Data recovery • Network and cloud forensics • Memory forensics • Timeline analysis • Real world targeted attack forensics practice	5 days	• Be able to perform deep file system analysis • Be able to recover deleted files • Be able to analyze network traffic • Reveal malicious activities from dumps • Reconstruct the incident timeline
Advanced Malware Analyisis & Reverse Engineering		
• Malware Analysis & Reverse Engineering goals and techniques • Advanced static analysis techniques (Analysing shellcode statically, parsing PE header, TEB, PEB, loading functions by different hash algorithms) • Advanced dynamic analysis techniques (PE structure, manual and advanced unpacking, unpacking malicious packers that store the full executable in an encrypted form) • APT reverse engineering (cover an APT attack scenario, starting from phishing email and going as in-depth as possible) • Protocol analysis (analyse encrypted C2 communication protocol, how to decrypt traffic) • Rootkits and Bootkits analysis (debugging the boot sector using Ida and VMWare, Kernel debugging using 2 virtual machines, analysing Rootkit samples)	5 days	• Be able to follow best practices in reverse engineering while recognizing anti-reverse engineering tricks(obfuscation, antidebugging) • Be able to apply advanced malware analysis for Rootkits/Bootkits dissection • Be able to analyze exploit shellcode embedded in the different file types and non-Windows malware
Incident Response		
• Introduction to Incident Response • Detection and primary analysis • Digital analysis • Creating of detection rules (YARA, Snort, Bro)	5 days	• Differentiate APTs from other threats • Understand various attackers' techniques and targeted attack anatomy • Apply specific methods of monitoring and detection • Follow incident response workflow • Reconstruct incident chronology and logic • Create detection rules and reporting

Program Description

Topics	Duration	Skills gained
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
KATA Administration		
• Common Solution Deployment Scenarios and Server Locations • Sizing Considerations • Licensing Model • Sandbox Server • Central Node • Sensor • Integration with Infrastructure • Installation of Endpoint Sensor • Adding a License and Updating Databases • Solution Operation Algorithm	1 day	• Design the implementation plan fitted to a customer's environment • Install and setup all the KATA components • Maintain and monitor the solution
KATA Security Analyst		
• KATA alerts interpretation • Detection and analysis technologies explanation • Scoring and risk engines explanation	1 day	• Understand how scoring works and how it's used by risk engines • Be able to confidently monitor, interpret and respond to KATA alerts



Kaspersky Lab
Enterprise Cybersecurity: www.kaspersky.com/enterprise
Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com

#truecybersecurity
#HuMachine

www.kaspersky.com