Kaspersky xTraining

Embrace your security team's potential with Kaspersky’s global expertise

kaspersky BRING ON THE FUTURE

Online self-learning format

Learn at your own pace from anywhere with browser-based access on your desktop/tablet/ mobile

Highly practical

Safely practice your cyber security skills in a virtual environment, revealing the specifics of real- world cyber attack cases

Learn from best

Acquire unique hints, strategies and insights from global leading InfoSec professionals

Support & feedback

Take a chance to ask course experts questions during monthly online live sessions

Certificate of completion

Receive a Kaspersky letterhead PDF document signed by course leader(s) for you to present and impress your employer

Time to take your cyber security team to a new level

Kaspersky xTraining is a response to a constantly evolving cyber threat landscape. We deliver up-to-date knowledge on effective threat detection and mitigation strategies from comprehensive and well-known experiences of the Kaspersky Global Research & Analysis Team (GReAT).

Who will benefit with xTraining?

Security operations professionals

SOC teams manager

Cybersecurity consulties

Threat hunters

Malware reversers

Governmental organizations & CERT's

Academies & research institutions

Kaspersky xTraining in faces

Costin Raiu,
Security Researcher

Ayman Shaaban,
Digital Forensics and Incident Response Group Manager

Igor Kuznetsov,
Director of Global Research and Analysis team (GReAT)

Tatyana Shishkova,
Lead Security Researcher at Global Research and Analysis Team (GReAT)

Reverse engineering

Reverse engineering 101 All levels

- Gain the initial knowledge needed for malware analysis
- Understand the main Intel assembly instructions
- Understand different calling conventions (stdcall, fastcall) and memory types (automatic, dynamic, static)
- Analyze executables generated by different compilers so you are more familiar with more esoteric ones
- Prepare yourself for the next level RE course

Mobile malware reverse engineering Intermediate

- Understand how to analyze mobile malware including Android/iOS samples
- Learn advanced static analysis or so-called surface analysis: permissions, strings, signature, resource files, decompilation of Dalvik bytecode
- Learn how to analyze native libraries for Android and iOS statically using Ghidra
- Learn advanced dynamic analysis using dynamic instrumentation with Frida

Targeted malware reverse engineering Intermediate

- Analyze real-life malware used in the wild by APT groups
- Reverse-engineer malicious documents and exploits
- Approach reverse engineering programs written in a number of programming or scripting languages (C, .NET, Delphi, Powershell, JavaScript, C++) and compiled for different architectures (x86, x64) with different compilers or operating systems (Windows, Linux)
- Master advanced features of reverse-engineering tools including IDA Pro's scripting capabilities

Advanced malware analysis techniques Advanced

- Analyze modern complicated code samples, from receiving the initial artefact, 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 damage assessment and incident response efforts are accurate and effective

Advanced malware analysis with Ghidra* Advanced

- Get familiarized with the process of setting up Ghidra and building its latest version from source code
- Understand how to perform a typical malware analysis workflow with Ghidra
- Gain a firm understanding of how to work with data types and structures in Ghidra
- Determine to identify runtime library code with Ghidra
- Learn how to use Ghidra's scripting capabilities to automate reverse engineering tasks
- Understand how to extend Ghidra's capabilities using the Eclipse IDE

*Ghidra is an open-source reverse engineering framework created and maintained by the National Security Agency Research Directorate

Threat hunting

Hunt APTs with Yara like a GReAT ninja All levels

- Write cleaner, more efficient, Yara rules
- Utilize tips & tricks to create fast and efficient rules
- Use Yara generators to save time and effort when writing codes
- Test Yara rules for false positives that could skew your results
- Hunt new undetected samples in your infrastructure and cloud platforms
- Use external modules within Yara for even more efficient hunting
- Discover secrets of anomaly search
- Test your new skills on real life cases like BlueTraveller and DiplomaticDuck

Security operations and threat hunting Intermediate

- Understand the structure of any Security Operations Center as a part of security defense services
- Be able to plan and organize security monitoring in the enterprise
- Use different threat intelligence sources to find new advanced threats
- Detect and investigate malicious activity in Windows and Linux infrastructures based on attacker's tactics, techniques and procedures
- Learn threat hunting infrastructure based on ELK (Elasticsearch, Logstash, Kibana)

Suricata for incident response and threat hunting All levels

- Understand what is a NIDS and how to use it
- Write Suricata rules for different protocols
- Utilize tips and tricks to create fast and efficient rules
- Learn about typical network attacks
- Analyze suspicious traffic and recognizing traffic anomalies
- Learn how to identify and fix a false alarm
- Learn how to use Suricata for threat hunting
- Gain new skills through a practical challenge in virtual environment

Incident response

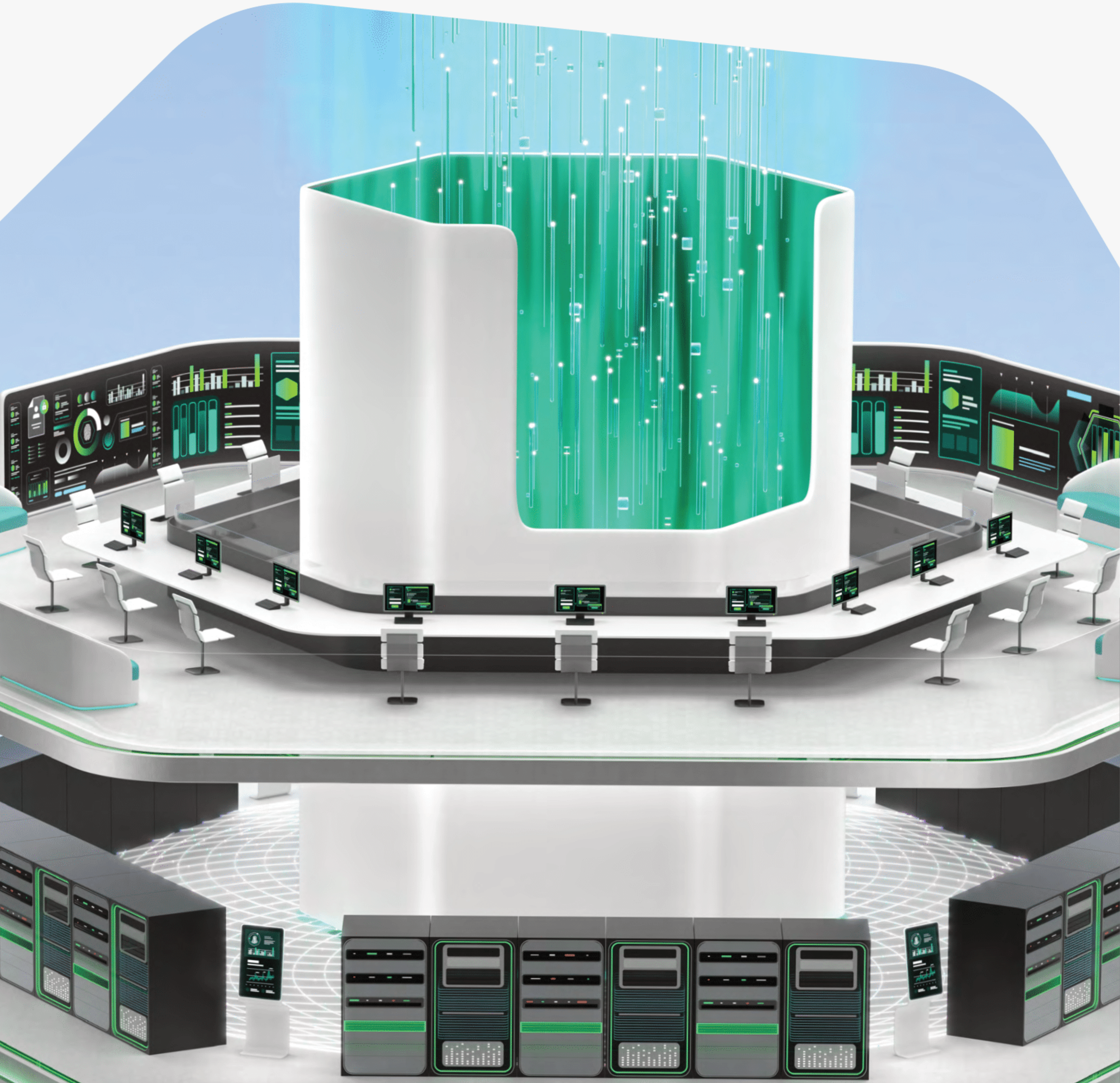
Windows Incident Response Intermediate

- Gain new skills through a practical challenge in virtual environment
- Understand the phases of incident response
- Know how to identify and respond to a cyber incident
- Understand various attack techniques and targeted attack anatomy through the Cyber Kill Chain
- Differentiate APTs from other threats
- Apply live analysis on victim machines
- Acquire evidence in a forensically sound environment
- Upgrade your memory forensics skills
- Apply log file analysis with regular expressions and ELK
- Enhance cyber threat intelligence knowledge
- Be able to create better network and host-based IoCs (Indicators of Compromise)
- Test your network traffic forensics skills

Product security assessment

Cyber capacity building program All levels

- Building capacity to identify, evaluate and estimate risks related to external applications in ICT infrastructure
- Managing identified risks and assessing the integrity and security of external applications
- Forming a list of requirements for external applications to minimize cybersecurity risks related to them
- Developing an understanding of industry best practices for building a secure ICT ecosystem with regard to external applications



Learn more about xTraining

Learn more

Contact us

www.kaspersky.com