Enterprise / MSSP / Law-enforcement

▶ INTELLIGENCE SERVICE: CYBERSECURITY EDUCATION

Leverage Kaspersky Lab’s cybersecurity knowledge, experience and intelligence through this innovative education program.

Cybersecurity awareness and education are now critical requirements for enterprises faced with an increasing volume of constantly evolving threats. Security employees need to be skilled in the advanced security techniques that form a key component of effective enterprise threat management and mitigation strategies.

Kaspersky Lab’s Cybersecurity Education program has been developed specifically for any organization looking to promote the role of cybersecurity in order to better protect its infrastructure and intellectual property. The program offers a broad curriculum in cybersecurity topics and techniques and assessment ranging from basic to expert.

IMPROVE YOUR IT SECURITY SKILLS TODAY

A COMPREHENSIVE OFFERING

All training courses are offered in English, and 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 practical ‘labs’. On completion of each course, attendees will be able to complete an evaluation to validate their knowledge.

BEGINNER, INTERMEDIATE OR EXPERT?

The program covers everything from security fundamentals to advanced digital forensics and malware analysis, helping customers to improve their cybersecurity knowledge in three main domains:

- Fundamental knowledge of the topic
- Digital Forensics and Incident Response
- Malware Analysis & Reverse Engineering

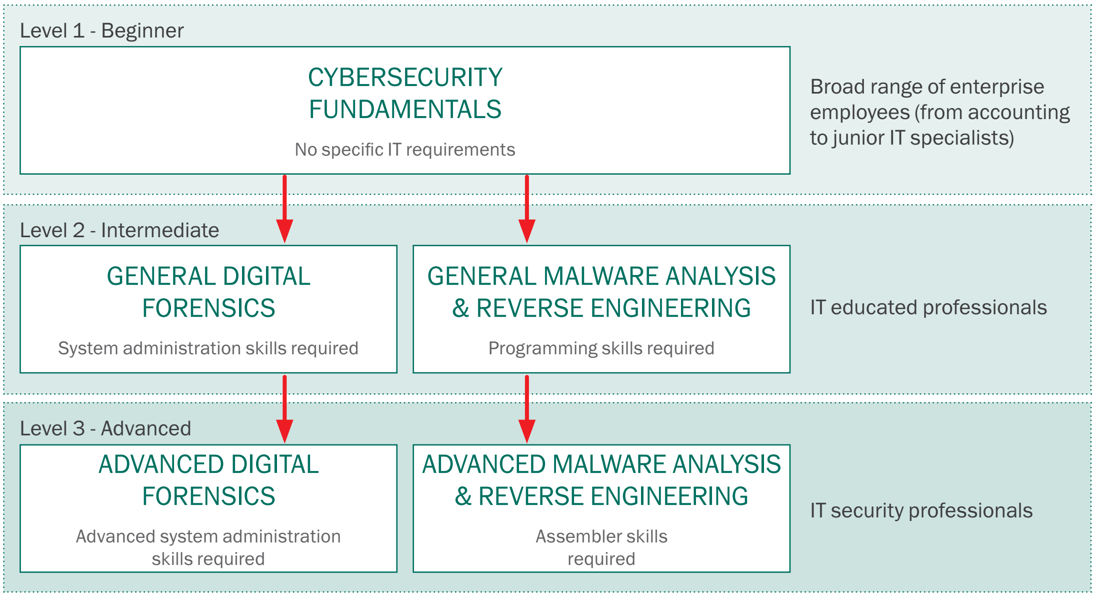
SERVICE BENEFITS

Educating staff in cybersecurity helps organizations to:

- **LEVEL 1 – Cybersecurity Fundamentals**
  Reduce expenditure / mitigate reputational risks / mitigate the leakage of confidential information related to generic security mistakes and unawareness of the functionality of major threats.
- **LEVELS 2-3 – Digital Forensics**
  Improve the expertise of the in-house digital forensics and incident response team.
- **LEVELS 2-3 – Malware Analysis & Reverse Engineering**
  Improve the expertise of the in-house Malware Analysis & Reverse Engineering team.

HANDS-ON EXPERIENCE

From a leading security vendor.



Level 1 - Beginner

CYBERSECURITY FUNDAMENTALS

No specific IT requirements

Broad range of enterprise employees (from accounting to junior IT specialists)

Level 2 - Intermediate

GENERAL DIGITAL FORENSICS

System administration skills required

GENERAL MALWARE ANALYSIS & REVERSE ENGINEERING

Programming skills required

IT educated professionals

Level 3 - Advanced

ADVANCED DIGITAL FORENSICS

Advanced system administration skills required

ADVANCED MALWARE ANALYSIS & REVERSE ENGINEERING

Assembler skills required

IT security professionals

PROGRAM DESCRIPTION

TOPICS	Duration	Skills gained
LEVEL 1 – Cybersecurity Fundamentals		
• Cyberthreats & Underground market overview • Spam & Phishing, Email security • Cyber threat types & protection technologies • Advanced persistent threats • Investigation basics using public web tools • Securing your workplace	2 days	• Understand the threat landscape • Be able to use your PC more safely • Recognize different types of attacks • Classify cyber weapons and malware and understand their goals and working principles • Analyze phishing mails • Recognize infected or faked websites
LEVEL 2 – GENERAL DIGITAL FORENSICS		
• Introduction to Digital Forensics • Live Response and Evidence Acquisition • Windows Registry Internals • Windows artifacts analysis • Browsers Forensics • Email analysis	5 days	• Build the Digital Forensics lab • Collect digital evidence and deal with it properly • Reconstruct an incident and use time stamps • Find traces of intrusion on investigation artifacts in Windows OS • Find and analyze browser and email history • Be able be apply with the tools and instruments of digital forensics
LEVEL 2 – GENERAL MALWARE ANALYSIS & REVERSE ENGINEERING		
• Malware Analysis & Reverse Engineering goals and techniques • Windows internals, executable files, x86 assembler • Basic Static analysis techniques (strings extracting, import analysis, 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 needed 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
LEVEL 3 – 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 Memory dumps • Reconstruct the incident timeline
LEVEL 3 – ADVANCED MALWARE ANALYISIS & REVERSE ENGINEERING		
• Malware Analysis & Reverse Engineering goals and technics • Advanced Static & dynamic analysis techniques (manual unpacking) • Deobfuscation techniques • Rootkit & Bootkit analysis • Exploits analysis (.pdf, .doc, .swf, etc.) • Non-Windows Malware Analysis (Android, Linux, Mac OS)	5 days	• Use the world best practices in reverse engineering • Recognize anti-reverse engineering technics (obfuscation, anti-debugging) • Apply advanced malware analysis for Rootkits/Bootkits • Analyze exploit shellcode, embedded in different file types • Analyze non-Windows malware

WHY KASPERSKY LAB?

- Founded and led by the world's foremost security expert, Eugene Kaspersky
- Partnerships with global law enforcement agencies such as Interpol and CERTS
- Cloud-based tools monitoring millions of cyberthreats across the globe in real time
- Global teams analyzing and understanding Internet threats of all kinds
- World's largest independent security software company — focused on threat intelligence and technology leadership
- Undisputed leader in more independent malware detection tests than any other vendor
- Identified as a Leader by Gartner, Forrester and IDC

For more information on Kaspersky Intelligence Services, please contact us via intelligence@kaspersky.com.
TO LEARN MORE VISIT www.kaspersky.com.