KASPERSKY lab

Kaspersky Security Training Program

Breakdown and Description of Courses
Training for Security Professionals

www.kaspersky.com
#truecybersecurity

Contents

Kaspersky Security Training Program

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.

Executive Summary

The Kaspersky Security Training Program has been developed specifically for organizations looking to better protect their infrastructure and intellectual property through promoting the role of cybersecurity. The program offers a broad curriculum in cybersecurity topics and techniques, with assessment levels ranging from basic to expert, integrating a full range of specialist security skills, functionalities and competencies into a single body of knowledge.

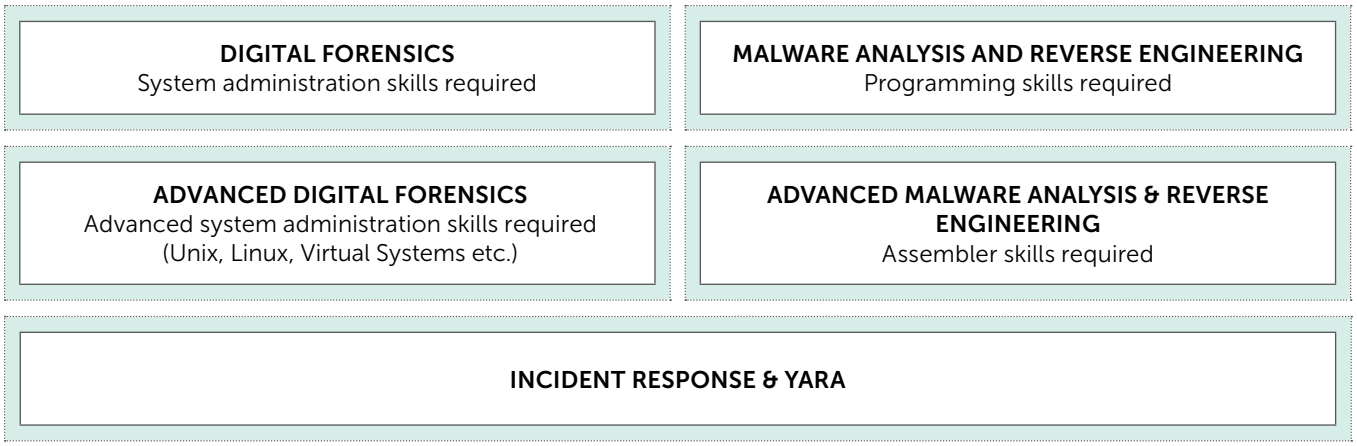
For more than 17 years, Kaspersky Lab's cybersecurity expertise – including threat detection, malware research, reverse engineering and digital forensics – has been continuously evolving and advancing. Our experts understand how best to handle the threats posed by the 350,000 malware samples encountered by us every day, and how to impart that knowledge to organizations confronted with the new dangers of contemporary cyber-reality.

The Security Training Program has been designed and developed by the security authorities who helped build the Kaspersky antivirus labs, and who now inspire and mentor the next generation of global experts.

A Comprehensive Offering

All training courses can be delivered either at customer premises or at Kaspersky Lab local or regional offices, as applicable. Courses are designed to include both theoretical classes and practical 'labs'. On completion of each course, students are invited to validate their knowledge through a test and evaluation.

Security Training Program



Training for Security Professionals

Organizations who may particularly expect to benefit from Kaspersky Lab's Security Training Program include:

- Large enterprises (banks, telcos, airlines, hotel chains, etc.)
- MSSPs (Managed Security Services Providers)
- Law enforcement agencies (LEA)

Beginner or Expert?

The program covers everything from fundamentals to advanced techniques and tools used for digital forensics, malware analysis and incident response, allowing organizations to improve their cybersecurity knowledge pool in these areas.

General and Advanced: Digital Forensics	Developed to meet the requirements of enterprises that grow their in-house expertise in this area and/or have their own SOC (Security Operation Center) and/or deploy CERTs. Geared to employees who may find themselves working on incident response and digital forensics.
General and Advanced: Malware Analysis & Reverse Engineering	Developed to meet the needs of enterprises that maintain a skilled team of malware analysts and researchers. They may also have own their SOC and/or CERTs deployed. Geared to employees who may expect to conduct malware analyses and reverse engineering as part of their duties.
Incident Response	Incident Response course is designed for employees from enterprises who are directly involved in responding to the information security incidents.
Yara Training	Yara Training course is designed for professionals whose work routinely involves incident response and threat hunting.

Program Benefits

Educating staff in cybersecurity helps your organization to equip your security team to deal with ever-changing security technologies and a continuously evolving threat environment.

General 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.
General and Advanced: Malware Analysis & 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 Training	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.

Schedule and Components

Digital Forensics

- Basic Digital Forensics takes place over five 8-hour days.
- This training is for participants working in information security related roles who already have advanced system administration skills. Due the many practical tasks, technical prerequisites for this training include a PC for each student with the appropriate tools installed, including Live Response Tools (Sysinternals), Forensics Live CDs (Helix, DEFT) and Forensics Disk Imaging (FTK, dd, HDD). All are free tools we actively used in the workplace.
- It is impossible to study digital forensics (DF) without understanding its **main principles**.

Tools change with time, but basics and methods of work remain consistent. Participants will receive not just a set of tools and instructions, but knowledge of fundamental principles and functionality. All practical tasks are based on real cases wherever possible without breaching customer confidentiality.

Day 1

Topics

Introduction to Digital Forensics
- Common terms and principles
- Procedures and processes
- Building the Forensics Lab (HW and SW)
- Virtualization

Live Response and Evidence Acquisition
- Fundamentals of incident response
- Case study scenario
- Memory acquisition
- Live response Tools (Sysinternals)
- Forensics live CDs (Helix, DEFT)
- Remote acquisition
- Forensics disk imaging (FTK, dd, HDD)
- SSD VS digital forensics
- Image mounting in Windows and Linux OS (FTK, mount)

Overview

Because a successful digital forensics process depends on successful incident response, the steps involved in efficient incident response will be covered along with some tools widely used in incident response for the acquisition of evidence from the system memory or hard drive on a live or shot down target system to what is called forensically sound image and techniques for mount and reading the acquired image on Windows and Linux operating systems.

Due to the constantly improving techniques, live analysis or response is a highly recommended practice in situations, where analysis of the target machine/s needs to be conducted immediately at the scene. On Day 1 we will demonstrate some live response techniques using different set of tools.

We will also provide students with essential knowledge about the digital forensics field, including definition, process and procedures. Building a workspace for digital forensics is no easy task when you consider the risk of data loss, hardware failure or even infection caused by the evidence under investigation. This section will deliver some guidelines about configuring the digital forensics workstation and will also explore the benefits of virtualization techniques in creating a multi-platform environment for running different tools.

Major differences in HDD and SSD or Solid State Drive operations makes it very difficult to follow the same procedures or use same tools for acquisition or analysis. In this module we will demonstrate why SSD are different and which challenges are present during the analysis of SSDs.

Day 2

Topics

Windows Registry Internals
- Registry structure
- Extraction of users' registry hives (FTK)
- User profile data
- Evidential information in registry (time zone, network address, OS version, autostart executables, browsing history, etc.)
- Windows registry recovery (MiTec WRR)
- Analysis of users and system activities (RegRipper)

Overview

The registry is one of the most important evidence-gathering components of the Windows operating system and a 'mandatory for analysis' element of the digital forensics process. Using the registry, the investigator will be able to retrieve important information about the operating system such as time zone, network address, browsed websites, security policy and startup executables. User activities such as login and opened files can also be extracted from the registry hives. Malware executables usually acquire a registry location to guarantee survival during system reboot or user logoff, and this can provide the investigator with clues about malicious activity in the machine under investigation.

In this module, we examine the structure of the Windows registry and the location and contents of different registry hives in the file system. Students will learn how to navigate through the registry hives either online in a live system or offline by extracting the hives files from a backup of the forensic image.

Day 3

Topics

- Windows artifacts analysis
- Prefetch (WinPrefetchView)
- Event logs
- LNK
- Jobs
- Recycle bin
- Metadata of compound files (EXIF, Thumbnails, Office files)

Overview

The Windows operating system uses different file structures and formats to store data about its operations. As with the Windows registry, some files are of particular interest to the investigator. Information extracted from these files can provide an added value to the investigation process, so understanding these files structures is critical. In this module, the investigators will be able to locate and parse Event log files, .lnk files, Windows tasks, prefetch files and recycle bin contents. The module also covers the extraction of evidential information from compound files such as images with exif data, thumbnail files and Microsoft office files.

Day 4

Topics

Browser Forensics (Nirsoft browsing tools)
- Data location for different browsers
- IE analysis
- Chrome analysis
- Firefox analysis

Email analysis
- Server-client structure
- Outlook forensics (pff-tools)
- Lotus Notes
- Web based email clients

Overview

During the normal web browsing, important information stored in the file system, the location and structure of data differing between browsers. In this section, the investigator will learn how to find and analyze the browsing history, internet cache files, bookmarks, cookies, etc. Leading browsers Chrome, Firefox and IE will be covered in this Module.

Email is a standard method of communication nowadays for official and non-official purposes. Email files can store considerable evidential information. Different implementations of the email service, by private mail server or web mail, and the existence of different clients such as Outlook and Lotus. The investigator needs to understand the behavior and workings of the email client in the user machine and to have the skills necessary to investigate these files in order to extract related data. In this module, we will discuss the remnants after usage web based e-mail services and Outlook and Lotus mail clients.

Day 5

Overview

On the final day, students undertake a number of exercises, covering different elements of the training and involving different types of files. Students must apply forensic analysis to these files in order to answer questions correctly. At the end of the day, the correct answers will be discussed with the students to obtain the maximum benefit from the exercise.

Skills gained

- Under our guidance students will learn how to collect digital evidence and deal with it properly
- During this training students will reconstruct an incident, use time stamps and find traces of intrusion on investigated components of the Windows OS
- The OS itself isn't the only source of knowledge. Students will also learn how find and analyze browser and email history and how to use this software to collect evidence

Malware Analysis & Reverse Engineering

- General Malware Analysis takes place over five 8-hour days.
- Training is suitable for IT-related professionals looking to acquire practical skills in malware analysis. Some programming experience is critical. Due to the many real life practical tasks, technical prerequisites for this training include a PC for each student. Virtual machines will be provided with the following free tools installed: IDA, Immunity debugger, OllyDdg, WireShark, Sysinternals tools, Fiddler proxy, dumpers, PE analyzers and other utilities for static and dynamic analysis. We will assume that there is no LAN and internet in the training room, but the company should provide some means of distributing disk images to participants.
- This course provides all the necessary information about the modern malware and anti-malware landscape. Participants will learn about current malware functioning and how it infects companies' IT infrastructures through their weakest points, exploiting these weaknesses after infection. Students will also learn all the main methods and malware analysts' routines.
- Strong anti-malware theory is combined with surface analysis. To operate effectively as analysts, students need to understand what lies behind the tools and techniques. All our trainers are practitioners, not theorists. Their experience is based on daily routines.

Day 1

Topics

Introduction to malware analysis
- Malware types
- Goals of malware analysis
- Reverse engineering basics

Windows internals
- Core Windows system files
- Portable executable (PE) file format, export and import sections
- Windows API functions, useful for analysis
- Intel architecture, 32-bit (IA-32)

Overview

In order to reverse malicious code, it is necessary to understand the **basics of modern OSs and processors instructions**. The course starts with a Windows architecture overview, exploring the Application Programming Interface (API), kernel and user OS modes, kernel mode components (Hardware Abstraction Layer or HAL, device drivers, Windows PE launcher) and core Windows system files. Popular system libraries (.DLLs) and WinAPI functions will be briefly addressed, with supporting materials. Web access to MSDN is advisable, but not essential.

Students will learn in detail about the main OS entities: processes, threads and process and thread environment blocks (PEB and TEB). We'll describe multitasking, context switching, scheduling and other OS mechanisms.

After OS internals, the course moves to reverse engineering basics, starting with the Portable Executable (PE) file format: its headers, sections and directories. Assembler instructions for modern x86 processors are also in scope here. Students will gain an understanding of compilation, linking and decompilation processes, including real-world practical exercises on these topics, in course of the first day.

Day 2

Topics

Static analysis of applications
- When it's necessary: preliminary, quick or in the field
- Method advantages and disadvantages

Static analysis techniques
- String extraction and web search
- Hashing and signature checking
- Metadata extraction and abnormalities detection
- Imports, exports and resources analysis
- Code analysis
- Automatic unpacking

Overview

There are two types of analysis – static and dynamic. Static analysis is performed without actually executing programs and provides a quick preliminary analysis. Students will practice surface analysis: looking for anomalies in PE headers, analyzing suspicious strings, resources and imported functions. They will learn to use different hashing algorithms for file integrity checking, validate digital signatures, and search for information about suspicious objects on the internet. Using real life samples, they will detect simple malware protections deployed by packers, and remove them with automatic tools. Students will also study methods of increasing the clarity of disassembled malware code and fast navigation through such code. They will learn how to understand and recover the whole malware algorithm and find the malicious code inside the programs.

Day 3

Topics

Dynamic analysis of a local data
- Process activity including memory dumps
- Monitor APIs
- Monitor events
- Execution in sandbox
- Debugging
- Registry activity

Dynamic analysis of a network data
- Create a virtual network
- Traffic inspection
- Offline traffic analysis
- Network simulation

Overview

Dynamic analysis helps to observe a program's behavior directly, including aspects like network traffic, which APIs are used, how the application interacts with the registry and so on. Students will learn how to debug the applications, take memory dumps, monitor Windows API function calls, monitor registry activity, create a virtual network, imitate the real network functionality in the laboratory environment and inspect network traffic. All these tasks are learned through lab exercises. After trainers have demonstrated how each tool is used, students will themselves carry out the analysis of real samples.

Day 4

Topics

Non-Win32 analysis
- .NET
- Visual basic
- Java
- Win64

Overview

Windows API is not the only programming interface for malware, so participants will also work with NET, Java and other popular languages during training. Students will learn all necessary tools for analysis acceleration due to p-code and intermediate languages decompilation.

Day 5

Topics

Script analysis
- Batch files
- AutoIt
- Python
- JavaScript and VBS scripts
- Visual Basic Script
- Real life hands-on exercises on wrappers analysis

Overview

Of course, malware goes far beyond the portable executable files. Even legitimate websites may be compromised by drive-by infections created by malefactors. To investigate these threats malware analysts use the script languages. The analysis of automation scripts (compiled beforehand into executable files), installers and other wrappers is all covered.

Skills gained

- With the help of our experts, students will detect malicious sites through script malware analysis and conduct express malware analysis themselves.
- Students will build a secure environment for malware analysis on their own: deploying a sandbox and all necessary tools
- Students will understand the principles of Windows programs execution, unpacking real life samples, debugging and analyzing malicious objects to identify their functions

Advanced Digital Forensics

- Advanced Digital Forensics takes place over five 8-hour days.
- Training is suitable for IT-related professionals possessing advanced system administration skills. Due to the many practical tasks, technical prerequisites for this training include a PC for each student with tools installed including the following: Recover deleted file (TSK), File carving (foremost, bulk extractor), Restore Point and Volume Shadow Copy (libvshadow), Network traffic analysis (Wireshark, Bro, Network Miner).
- **The File system** contains data of particular forensic value. But there are many other significant sources of such data, including **random access memory and network traffic** snapshots. By bringing everything together into the **super timeline**, a complete picture of the incident is revealed – this is what advanced forensic training is all about.

Day 1

Topics

Deep Windows forensics
- Binary and hex
- Partitioned hard drive and MBR analysis
- File system structure
- Different Windows file systems (FAT, NTFS)
- NTFS Internals
- MFT analysis and file system timestamps

Overview

We start at advanced level by digging deep into Windows forensics. The knowledge in Binary and Hex systems needed by the investigator to be able to read and interpret such systems is provided, then the structure of a partitioned hard drive and the skills necessary to interpret the MBR of the hard drive with only a hex-editor are explained. The structure of the file system in general is explored, together with the different file systems used by the Windows operating system, digging deep in NTFS file system internals and using a hex editor to start interpreting the NTFS and to understand the meaning of the timestamps stored by the NTFS file system in MFT entries. At the end of this exercise students will be able to understand how the file system stores and deletes files and will be ready to start work on data recovery.

Day 2

Topics

Data recovery
- Recover deleted file (TSK)
- File carving (foremost, bulk_extractor)
- Restore Point and Volume Shadow Copy (libvshadow)

Network and Cloud forensics
- Network traffic collection
- Network traffic analysis (Wireshark, Bro, Network miner)
- Cloud forensics – SaaS, PaaS, IaaS

Overview

Data recovery is widely used in digital forensics. Today, we will discuss the difference between deleted and wiped files from a file system perspective, and how to recover deleted files. This will include how file signature and the concept of file carving can be used where deleted files are no longer linked to the file system, as well as the importance and the use of Windows restore points and volume shadow copies, learning how to recover user's data and files from both.

Most malicious activity in a computer system includes some network involvement. Stealing sensitive financial information or disseminating malware, for example, usually involves network traffic. So analyzing network traffic can increase understanding of the malicious activities under investigation. This module addresses how to collect and analyze network traffic using different hardware and software tools.

The challenges that face digital forensics continue to grow in line with new technologies. Cloud computing is one of the fastest growing technologies of recent years, and its structure makes it an anti-forensic technique by almost by definition. In this module, we will discuss the different deployments of cloud computing and how to conduct what's known as 'cloud forensics' under each.

Day 3

Topics

Memory forensics
- Windows memory foundation
- Memory in virtualization
- Volatility framework
- Rekall framework

Overview

RAM often contains important system data. Although the system memory is the crucial point in live analysis, advanced tools can acquire the memory to a single file for later analysis. This module covers how the memory works and some of the techniques used to conceal malicious activities in the memory. Students are taught the skills needed to analyze memory files offline and to extract important information about running processes, network connections, malicious activities, registry files opened in memory and dump executables from memory files.

Topics

Timeline analysis
- Timeline basics
- Building a timeline based on file system activity (TSK)
- Super Timeline (log2timeline and Plaso Framework)

Day 4

Overview

Timestamps are highly important in tracking the activity of a specific system or user during analysis. From a chosen start point, the investigator creates a timeline of all user, program or systems activity. Today module, students will gain the knowledge required to understand different timestamps and to extract specific relevant evidential information from the timeline.

Day 5

Overview

On the final day of training, students will apply their newly gained skills to a previously provided case scenario with evidence files, including forensic images of the hard drive, memory and network traffic, related to a real world targeted attack. Having analyzed the evidence files to solve the case, students then present their findings, at the end of which a model answer will be given.

Skills gained

- After this advanced training, students will be able to perform deep file system analysis to recover deleted files
- Participants will be able also to analyze other sources of data such as network traffic or to reveal malicious activities from memory dumps
- As a result, participants will be able to reconstruct a complete incident timeline

Advanced Malware Analysis & Reverse Engineering

- Advanced Malware Analysis takes place over five 8-hour days.
- This course is suitable for IT-related professionals whose work routinely involves malware analysis. Due to the many practical tasks, technical prerequisites for this training is PC for each student with required tools installed. Disk images for deployment are provided.
- Participants will study **anti-analysis techniques** favored by cybercriminals. After this in-depth course, technical employees will be able to **unpack**, **deobfuscate** and remove **anti-debugging** techniques, and even to dissect **root-** and **boot-kits**.

Day 1

Dynamic Analysis

Topics

- Skills test
- PE structure
- Manual unpacking: learning how to unpack files correctly and rebuild import table
- Advanced unpacking
- Unpacking malicious packers that store the full executable in an encrypted form

Day 2

Static shellcode analysis

Topics

- Analysing shellcode statically from malware samples, exploits and off-the-shelf exploitation frameworks
- Parsing PE header, TEB, PEB.
- Loading functions by different hash algorithms – and how to automate import resolution with scripts

Day 3

APT reverse engineering

Topics

- Cover an APT attack scenario, starting from phishing email and going as in-depth as possible

Day 4

Protocol analysis

Topics

- Analyse encrypted C2 communication protocol
- How to decrypt traffic

Day 5

Rootkits and bootkits analysis

Topics

- Debugging the boot sector using Ida and VMWare
- Kernel debugging using 2 virtual machines
- Analysing Rootkit samples

Skills gained

- This advanced training leads to students following best practices in reverse engineering while recognizing anti-reverse engineering tricks (obfuscation, anti-debugging).
- Supported by Kaspersky Lab's working experts, students will apply advanced malware analysis for Rootkits/Bootkits dissection.
- Participants will analyze exploit shellcode in real life samples, embedded in the different file types and non-Windows malware that are currently gaining popularity.

Kaspersky Incident Response Training

- Incident Response training takes place over 5 8-hour days
- The course is suitable for employees who take part in response to the occurring information security incidents
- Participants will learn the principles of building the correct response framework and will gain knowledge on the most efficient mitigation strategies leading to faster resolution of the incidents. The course will provide guidance for each step of the comprehensive incident response and will help to build strong in-house expertise.

Day 1

Topics

Introduction to incident Response:
- Terms and definitions
- Types of incidents
- Kill Chain ... Stages of targeted attacks
- Stages of incident handling
- Differences between APT and other threats

DEMOs:
- Demonstrations about some known malware campaigns
- Kaspersky Anti-APT product

Overview

The need to security experts rises when an incident take place, they know what to do. They understand that the first response to any incident will guide them through the whole analysis process, so it must be accomplished as flawless as possible. Besides keeping calm, some important steps must be followed during the incident time in order to ensure appropriate response to any incident. This must be considered while implementing the security architecture and during building the response plan.

In the first day, we will explain the importance of Incident response plan to be present in any entity nowadays and how it is not about "if we got attacked" any more, but it is about "When we got attacked". We will learn about the different steps in the incident handling process and what is essential to be present before the incident take place, what we must do during the incident and what we have to do after the incident.

Advanced Persistent Threat or APT is a trend that kept and continue rising during the last few years. We will understand what does it mean and how can you be targeted with an attack that can deceive your normal security implementations while demonstrating some famous malware campaigns that were discovered recently then demonstrate the new Kaspersky Anti-APT product and explain how can it be useful in detecting such attacks.

Day 2

Topics

Detection and primary analysis:
- Scenarios for incidents (How the attackers do it)
- Indicators of security incidents
- Methods of monitoring and detection
- First response
- •Live Response. IRCDs
- Information gathering (Whois, domain tools, Maltego ...)
- Online tools (Sandboxs, reputation check, Phishing DB)
- Remote Response in corporate network Evidence collection (memory, network traffic, images, logs)

Overview

So, before understanding how such attacks were detected, we need to understand how the attackers do it. In the second day, we will discuss some scenarios of targeted attacks that can happen within any entity and determine some general incidents' indicators that will help us in setting detection rules for different incidents and learn more about environment monitoring techniques.

Although dealing with detected incident differs based on the type of the incident itself. But, in general you will find yourself in deep need to do some specific actions each time. In this part, we will discuss some primary analysis actions that will help in identifying false positives from the alerts launched by the monitoring techniques and assist to collect more information about the incident under investigation such as getting information about specific domain or malicious URL accessed from your internal network.

After excluding any false-positive and distinguish incident from normal events and after collecting primary information about the incident, you will need to acquire digital evidences for further deep analysis. We will explain what evidences are important for us and the right way to collect these evidences.

The physical location is no more limiting incident response process as it did in the past, now you can monitor, detect and even perform analysis on an infected network or machine remotely. We will explain how to acquire evidences remotely.

Day 3

Topics

Digital analysis
- Digital forensics introduction
- Push-button forensics (pros and cons)
- Analysis of Disk Images
- Analysis of host-based artifacts
- Timeline
- Memory analysis
- Log application analysis
- Network traffic analysis

Overview

After acquiring all different types of digital evidences, performing deep analysis on the acquired evidences will reveal more findings that makes us realize what exactly happened, the amount of data loss and how to avoid such incidents in the future.

In the third day, we will be introduced to the digital forensics analysis and the difference between, what is called, push-button forensics and the deep forensic analysis that depends on the investigator knowledge. We will go through the analysis of different types on evidences such as System artifacts, system hard disks and network logs and will learn how to create one timeline from different activities to deeply understand all the actions that done by the attacker or the malware within the victim machine.

Day 4

Topics

Creating of detection rules
- YARA
- SNORT
- Bro
- Reporting
- Building of CSIRT

Overview

After complete analysis of the incident. There is very important step, that must NOT be skipped, which is the lessons learned. In this phase you may need to implement specific policies or set new rules. But in most cases you will need to go technical and implement new security controls or set new firewall rules. Also, after the incident you will have some IOCs or indicators of compromise. Using these IOCs you will be able to avoid this attack to take place within your environment once again. In the fourth day of the training we will learn how to build the IOCs and how to use it in creating new rules in different formats such as YARA and Snort and update these rules to the implemented monitoring solution such as Kaspersky Anti-APT product.

After that we will discuss why we should document each incident and build technical report and what we should include in our case report. By the end of the day, we will explain the steps of building Cyber Security Incident Response Team or CSIRT, and why it is mandatory for any big entity to have one.

Day 5

Overview

To maximize the benefit from the course, in the last day of the training the attendees will provided with an exam about the different parts of the training by which they can test their newly gained skills and knowledge. The instructors will be there for any help or guidance. After finishing the exam, the instructor will solve the exam with the attendees and discuss any question that needs more clarification.

Skills gained

- Participants will get a comprehensive understanding of the incident response techniques from the leading experts who provide incident response worldwide
- Knowledge gained on this training course will ensure correct incident response framework implementation and will help to avoid possible mistakes resulting in faster resolution of the information security incidents

Topics

- 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

Yara Training

- Yara Training takes place over two 8-hour days.
- This course is suitable for IT-related professionals whose work routinely involves incident response and threat hunting. Intendent audience are security researchers, malware analysts, security engineers, network security analysts, APT researchers. The training is suitable for both beginners and experienced Yara users, with or without reverse engineering experience.
- Participants will learn how to write the most effective Yara rules, how to test them and improve them to the point where they find threats that nobody else does. During the training they will gain access to some of our internal tools and learn how to maximize your knowledge for building effective APT detection strategies with Yara.

Skills gained

- After this training participants will gain the knowledge to create effective Yara rules
- As a result, participants will be able to increase threat detection levels in the organization leading to early remediation of the occurring incidents

Kaspersky Lab, Moscow, Russia **www.kaspersky.com**
All about Internet security: **www.securelist.com**
Find a partner near you: **www.kaspersky.com/buyoffline**

www.kaspersky.com