

EXHIBIT E. SERVICE MODULE. CYBERSECURITY TRAINING

This Service Module sets out the special terms and conditions applicable to Kaspersky Cybersecurity Trainings and is to be read in conjunction with [Kaspersky Security Services General Terms and Conditions](#).

1. DESCRIPTION

Kaspersky Cybersecurity Training covers a broad range of cybersecurity topics, techniques and assessments from basic to expert level. Comprehensive training programs covering digital forensics, malware analysis and incident response topics. Trainings include both theory and hands-on 'labs', for maximum engagement. On completion of each training, Customers' trainees can complete an evaluation to validate their knowledge.

All trainings are available either as in-person classes on Customer premises or at Customer local/regional Kaspersky office.

Kaspersky Cybersecurity Training Program helps Customer and its employees to improve their cybersecurity knowledge in five main areas:

- Incident Response Training
- Digital Forensics Training (and Advanced level)
- Malware Analysis & Reverse Engineering Training (and Advanced level)
- YARA Training
- KATA Analyst Training
- Threat Intelligence Training

The detailed up-to-date description of the Cybersecurity Training is provided by Kaspersky in the Technical Commercial Proposal.

2. TRAININGS CURRICULUM AND REQUIREMENTS

2.1. Incident response

The course's curriculum is heavily focused on practicing. Kaspersky experts will take trainees through all the stages of responding to an incident based on a real-life targeted attack. Trainees will master incident detection, evidence acquisition, log file analysis, network analysis and creation of IoCs, and also get introduced to memory forensics. Trainees will be working in a simulated virtual environment with all the necessary tools to practice Incident Response. Trainees will get not only super-clear theoretical knowledge but also tap into their up-to-date experience, skills and tips. After completing the course, trainees will be able to verify and handle threats quicker in order to minimize the impact and contain the damage.

INCIDENT RESPONSE	
Topics covered*	
	• Identify a cyber incident and how to respond to it • Understand various attack techniques • Differentiate between APTs and other threats • Apply live analysis on victim machines • Acquire evidence in a forensically sound environment • Upgrade trainees forensics skills • Apply log file analysis with regular expressions and ELK • Create better network and host-based IoCs • Test Customer's network traffic forensics skills
Requirements	
<i>Level:</i>	Junior
<i>Prerequisites for students:</i>	Basic knowledge & general troubleshooting experience with Windows OS, familiarity with Linux OS commands.
<i>Hardware & Software</i>	• CPU: 64-bit Intel x64 2.0+ GHz processor or higher-based system is mandatory for this class • 16 GB (Gigabytes) of RAM or higher is mandatory for this class • USB 3.0 port • 150 Gigabytes of Free Space on the System Hard Drive - Free Space on Hard Drive is critical • Attendees should have the capability to have Local Administrator Access within their host operating system • 7Zip, http://www.7-zip.org/ • VMware Workstation 10, http://www.vmware.com/products/workstation/ or higher
<i>Duration</i>	Five Business days

2.2. Digital Forensics

This course emphasizes practical application, mirroring real-world scenarios to provide participants with a comprehensive understanding of incident response, allowing participants to gain invaluable insights and hands-on experience. By the end, participants will be proficient in incident scoping, evidence acquisition, Windows artifacts analysis, creation of Indicators of Compromise (IoCs), and browser and email activities analysis. Armed with this knowledge, participants will be better equipped to detect and mitigate threats swiftly, minimizing their impact and containing the damage effectively.

DIGITAL FORENSIC
Topics covered*

	• Acquire the fundamental expertise essential for digital forensics. • Comprehend the methods of obtaining diverse digital evidence and managing it within a forensically sound setting. • Demonstrate proficiency in utilizing the tools and resources of digital forensics. • Analyze browser and email histories effectively. • Be able to find traces of malicious actions related to incidents in MS Windows artifacts. • Learn how to use timestamps from various Windows artifacts to restore an incident scenario.
Requirements	
<i>Level:</i>	Junior (Built for Tier 2 Analysts)
<i>Prerequisites for students:</i>	• Basic knowledge and general troubleshooting experience with Windows OS. • Familiarity with initial Linux OS commands.
<i>Hardware & Software</i>	• CPU: 64-bit Intel x64 2.0+ GHz processor or higher-based system is mandatory for this class • 16 GB (Gigabytes) of RAM or higher is mandatory for this class • USB 3.0 port • 150 Gigabytes of Free Space on the System Hard Drive - Free Space on Hard Drive is critical • Attendees should have the capability to have Local Administrator Access within their host operating system • 7Zip, http://www.7-zip.org/ • VMware Workstation 10, http://www.vmware.com/products/workstation/ or higher
<i>Duration</i>	Five Business days

2.3. Advanced Digital Forensics

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. In this course, we dig deeper in File system structure, data and file recovery, memory forensics, and creation of Timeline of a complete image. Having completed the course, students will be able to successfully investigate computer incidents and improve the security level of the business.

ADVANCED DIGITAL FORENSICS	
Topics covered*	
	• 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
Requirements	
<i>Level:</i>	Senior
<i>Prerequisites for students:</i>	• Solid experience of using Windows and Linux operating environments and be able to troubleshoot general OS connectivity and setup issues • Be familiar with VMware and be able to import and configure virtual machines • Participation in Digital Forensic training (recommendation)
<i>Hardware & Software</i>	• CPU: 64-bit Intel x64 2.0+ GHz processor or higher-based system is mandatory • 8 GB (Gigabytes) of RAM or higher is mandatory • USB 2.0 or higher Port(s) • 100 Gigabytes of Free Space on trainees System Hard Drive - Free Space on Hard Drive is critical • Attendees should have the capability to have Local Administrator Access within their host operating system • Internet access in the training location • 7Zip, http://www.7-zip.org/ • VMware Workstation version 10 at least, http://www.vmware.com/products/workstation/ If they do not own a licensed copy of VMware Workstation, they can download a free 30-day trial copy from VMware.com
<i>Duration</i>	Five Business days

2.4. Malware Analysis & Reverse Engineering

This intermediate-level course is built around analysis of ten (10) targeted malware cases used in the wild by powerful APT actors recently. Cases including MontysThree, LuckyMouse & Lazarus have been researched personally by Kaspersky trainers as part of their work in the Kaspersky GReAT team – so trainees will get first-hand knowledge and best practices from their exclusive research.

By working in the dedicated virtual lab, using an array of tools like IDA Pro, Hex-Rays decompiler, Hiew, 010Editor and many others, trainees will gain practical experience



analyzing real-life targeted malware and will become a more efficient malware analyst and reverse engineer and prove trainees' skills are relevant to today's threat landscape.

MALWARE ANALYSIS & REVERSE ENGINEERING

Topics covered*

- Analyze real-life malware
- Reverse-engineer malicious documents and exploits
- Approach reverse engineering programs written in a number of languages and compiled for different architectures
- Become more familiar with assembly
- Master advanced features of reverse-engineering tools, understand steganography
- Handle obfuscated or encrypted content
- Understand the roundabout ways attackers launch their programs
- Analyze shellcodes

Requirements

<i>Level:</i>	Senior
<i>Prerequisites for students:</i>	Proficiency in at least one scripting/programming language (ideally Python) and a basic understanding of Intel assembly language, alongside a basic understanding of reverse engineering and targeted malware, are paramount for anyone taking the course. More specifically trainees will need: • Basic knowledge of networking, programming concepts, OS internals etc. • Familiarity with x86 assembly language • Basic usage of disassemblers and debuggers • Proficiency with at least one scripting language – ideally Python. • Experience with C programming is especially helpful.
<i>Hardware & Software</i>	• CPU: 64-bit Intel x64 2.0+ GHz processor or higher-based system is mandatory • 8 GB (Gigabytes) of RAM or higher is mandatory • USB 2.0 or higher Port(s) • 100 Gigabytes of Free Space on trainees System Hard Drive - Free Space on Hard Drive is critical • Attendees should have the capability to have Local Administrator Access within their host operating system • Internet access in the training location • 7Zip, http://www.7-zip.org/ • VMware Workstation version 10 at least, http://www.vmware.com/products/workstation/ If they do not own a licensed copy of VMware Workstation, they can download a free 30-day trial copy from VMware.com
<i>Duration</i>	Five Business days

Number of students	Max 15 participants
--------------------	---------------------

2.5. Advanced Malware Analysis & Reverse Engineering

The focus of the course is advanced static analysis because for cybersecurity incidents involving previously unseen malicious code, this is the most reliable way to determine functionality of the code and find actionable artefacts. It allows organizations affected by APTs to define adequate damage assessment and incident response.

The course also heavily features Kaspersky's exclusive know-hows on the automation of decryption, decoding and other processing of the samples which helps not only optimize routine tasks, but preserves trainees work in the code. Trainees will be introduced to a custom static analysis framework (available for download), proven to be very efficient during decades of Kaspersky APT research.

ADVANCED MALWARE ANALYSIS & REVERSE ENGINEERING	
Topics covered*	
	- 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
Requirements	
Level:	Senior
Prerequisites for students:	2+ years of malware analysis as a daily job / in professional capacity 2+ years of experience analyzing code in IDA Pro - General knowledge of the Intel x86/x86_64 architecture - Understanding of the x86/x86_64 assembly language - Knowledge or programming experience with the Windows API - Basic knowledge of Python 3 - Basic knowledge of C/C++
Hardware & Software	- CPU: 64-bit Intel x64 2.0+ GHz processor or higher-based system is mandatory 8 GB (Gigabytes) of RAM or higher is mandatory - USB 2.0 or higher Port(s) 100 Gigabytes of Free Space on trainees System Hard Drive - Free Space on Hard Drive is critical

	- Attendees should have the capability to have Local Administrator Access within their host operating system - Internet access in the training location 7Zip, http://www.7-zip.org/ - VMware Workstation version 10 at least, http://www.vmware.com/products/workstation/ If they do not own a licensed copy of VMware Workstation, they can download a free 30-day trial copy from VMware.com
<i>Duration</i>	Five Business days
<i>Room</i>	Max 15 participants

2.6. Threat Detection with YARA

This training will lead through one of the essential tools for the APT hunter: the YARA detection engine. During this training students 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 students will gain access to some of Kaspersky internal tools and learn how to maximize the knowledge for building effective APT detection strategies with YARA.

THREAT DETECTION WITH YARA	
Topics covered*	
	- Write cleaner, more efficient, Yara rules - Tips & tricks to create fast, efficient rules - Yara generators to save time and effort - Test Yara rules for false positives - Hunt new undetected samples in Customer's infrastructure - Use external Yara modules for efficient hunting - Discover secrets of anomaly search - Test trainees new skills on real life cases
Requirements	
<i>Level:</i>	Senior
<i>Prerequisites for students:</i>	Knowledge of the Yara language & its basic rules and experience handling malware samples
<i>Hardware & Software</i>	- CPU: 64-bit Intel x64 2.0+ GHz processor or higher-based system is mandatory for this class 16 GB (Gigabytes) of RAM or higher is mandatory for this class - USB 3.0 port
<i>Duration</i>	Two Business days

2.7. KATA Analyst training

This course will help Customer's in-house cyber security/SOC analyst team to understand the KATA/KEDR platform architecture and fundamentals including usage for proper security threat analysis, and will equip them with the knowledge needed to customize the platform detection capabilities. Lessons are delivered using real case examples and through hands-on exercises.

KATA ANALYST TRAINING	
Topics covered*	
	• KATA/KEDR Fundamentals (Alerts, Events, Engine, Ruleset, Tasks) • KATA/KEDR Exercises – Real cases investigated through deep alert analysis, EDR telemetry analysis, and EDR usage for investigation/remediation. • KATA/KEDR Task usage for investigation & remediation (pre-configured & custom) • Custom Detection Rulesets: ○ Targeted Attack Analyzer (EDR Telemetry based) custom ruleset ▪ Indicator of Attack (IO) rules analysis & writing ▪ A Custom Rule for Threat Hunting – A “LOL” bin ▪ A Custom Rule for Threat Checking - Exchange 03/21 in-the-wild vulnerabilities ○ YARA engine custom ruleset ▪ YARA engine and rule logic ▪ YARA basic rule writing & usage in KATA/KEDR ○ IDS and OpenIOC ruleset introduction
Requirements	
<i>Level:</i>	Junior
<i>Prerequisites for students:</i>	• Basic knowledge of cyber security threats. Experience in incident response or SOC monitoring activities will be a plus. • Prior access to the KATA/KEDR Web UI is helpful but not required.
<i>Hardware & Software</i>	• CPU: 64-bit Intel x64 2.0+ GHz processor or higher-based system is mandatory for this class (demo labs will be done on cloud.skytap.com) • 16 GB (Gigabytes) of RAM or higher is mandatory for this class • USB 3.0 port
<i>Duration</i>	One Business day (total eight (8) hours: best delivery in two sessions 4h+4h)

2.8. Threat Intelligence training

Having completed the training, students will be familiar with what Threat Intelligence is, what its role is in CSIRT, and how it helps to detect and analyze external threats and enables the effective operation and interaction of different teams.

The training covers cyber threat intelligence domains and principles that are designed to build up comprehensive protection - from strategic plans to operational procedures.

Students will not only learn the core threat intelligence concepts, but also gain practical skills in applying tailored threat intelligence in company, analysis of multiple data sources (including Surface Web and Darknet), and creating SIGMA rules for malware detection.

THREAT INTELLIGENCE TRAINING	
Topics covered*	
	• Cyber Threat Intelligence • Intelligence-Driven Defense • Levels of Threat Intelligence • Cyber Kill Chain • Threat Intelligence and CSIRT • Maturity models • Threat Hunting: Collection/Processing/Analysis stage • Operational Cyber Threat Intelligence: SIGMA, YARA • Threat Landscape • OSINT methodology, tools and utilities • Network Perimeter Reconnaissance and understanding attack surface • Usage of special search engines • Prioritization of threats • Vulnerabilities monitoring • Getting information from Darknet • Cognitive Biases
Requirements	
<i>Level:</i>	Middle and Senior-level CTI analysts, SOC analysts, IS specialists
<i>Prerequisites for students:</i>	• Be familiar with MITRE ATT&CK and Cyber Kill Chain • Experience in Incident Response / Security Operation Center processes / Threat Hunting / Threat Intelligence will an advantage.

<i>Hardware & Software</i>	• CPU: 64-bit Intel x64 2.0+ GHz processor or higher-based system is mandatory. • 8 GB (Gigabytes) of RAM or higher is mandatory. • Attendees should have the capability to have Local Administrator Access within their host operating system. • Internet access in the training location. • 7Zip, http://www.7-zip.org/
<i>Duration</i>	Two Business days

***Covered topics may be adjusted by Kaspersky as part of the trainings improvement.**

Requirements for the room

- ✓ Limited to max 15 participants
- ✓ Enough space to come to every student if needed.
- ✓ Marker board (preferred) or flip chart to write at, markers. Board big enough to leave comments from previous days as a reminder for the students
- ✓ Big screen or projector to show the materials to the students. If projecting on the writable surface is possible - it would be nice. Materials have to be visible to everyone in the room. HDMI interface from the screen/projector to trainer's laptop
- ✓ SMB share or 3-4 USB sticks to spread the virtual machine among the students. It's about 10 GB large.

Trainings order recommendations

- ✓ Start with Junior level trainings
- ✓ Make a 2-4 weeks pause between Junior level to process all the information and practice new skills
- ✓ Participate in Middle/Senior level after Junior level trainings
- ✓ Make a 6-12 month pause between Senior level trainings

Schedule of the Cybersecurity Trainings provision

- ✓ Service Delivery Date shall be agreed by Parties in written including via email within three (3) months before its start

3. OBLIGATIONS OF THE PARTIES

3.1. Accordingly, the Customer shall:

- 3.1.1.** nominate times for the performance of the Service;
- 3.1.2.** release Kaspersky from any liability for any loss of production, loss of availability, loss of data, loss of connectivity, degradation of network bandwidth, loss of access to systems or loss of use suffered or incurred directly or indirectly by the Customer;
- 3.1.3.** co-operate with Kaspersky in all matters relating to the Service and provide in a prompt manner, any information, documents, or materials which may reasonably be required by Kaspersky in the delivery of the Service and, in relation to any information so provided, ensure that such information is complete and accurate in all material respects.

3.2. Accordingly, Kaspersky will:

- 3.2.1.** perform the Service remotely and/or onsite, as agreed in writing via email;

- 3.2.2.** deliver the Service or, if applicable, each part of the Service on the Service Delivery Date as agreed by Parties in writing including via email;
- 3.2.3.** use its reasonable endeavors to meet any agreed deadlines for completion of the Service;
- 3.2.4.** use reasonable efforts and take reasonable precautions when performing the Service.

4. LIABILITY LIMIT

- 4.1.** Customer acknowledges that Kaspersky ability to provide the Service and to meet any timeframe agreed for the provision of the Service is dependent on the Customer providing that information and facilities and equipment providing decisions and instructions at the times required by Kaspersky.
- 4.2.** Customer agrees that the Service can be provided by Kaspersky group of companies.
- 4.3.** In the event that performance of the Service is delayed or otherwise adversely affected by the failure of Customer to meet its obligations, Kaspersky shall bear no responsibility for such delay or other consequence arising from the Customer's failure to act.
- 4.4.** If the Service at Customer's premises is delayed due to circumstances which are not the liability of Kaspersky, the Client must bear the reasonable cost of waiting time and any additional traveling expenses incurred by Kaspersky personnel.
- 4.5.** Customer understands and acknowledges that no use of or connection to the Internet is absolutely secure and Kaspersky is not liable for any loss, damage or adverse consequences suffered by Customer whatsoever resulting from use of or connection to the Internet, including unauthorized access to, damage or loss of information or other materials to be transmitted between the Parties.

5. CANCELLATION FEES

- 5.1.** Kaspersky is entitled to an extension of time to perform its obligations under this T&C, which is equal to the delay caused by the Customer, without prejudice to any other right or remedy it may have, in cases if Kaspersky performance of its obligations under this T&C is prevented or delayed by any act or omission of the Customer (including but not limited to failure to provide access/access prolongation to the Customer's premises or facilities where required, failure to provide required data and information within reasonable time to commence the Service, not scheduling or participating in required events, etc.). In such circumstances Kaspersky has no liability in respect of such delay in the provision of the Service and may invoice Customer directly or through the Partner for any additional charges incurred in relation of the said extensions.
- 5.2.** In the event that the Customer cancels the Service prior to the agreed Service Delivery Date or requires the Service Delivery Date to be changed at short

notice then the Customer shall make such cancellation or change to the Service Delivery Date in writing to Kaspersky.

- 5.3.** In the event that the Customer reschedules or cancels the Service prior to the Service Delivery Date, Kaspersky may, at its discretion charge the Customer a late cancellation fee and recover any out-of-pocket expenses incurred as a result of the cancellation or rescheduling of the Service.

6. APPLICABLE LEGISLATION

- 6.1.** Customer confirms the carrying out of the Service does not contravene any law or regulation, in particular as it relates to individuals, users, third party information stakeholders, third party information service providers or other parties likely to be affected by the Service on the Customer's information systems.
- 6.2.** For the purposes of the Computer Misuse Act 1990 (or any statutory modification or reenactment or foreign equivalent thereof) Customer consents to Kaspersky accessing and assessing its IT systems and networks (including without limitation any programs or data held on such systems and networks) to enable Kaspersky to provide the Service.
- 6.3.** For the purposes of applicable copyright legislation, Customer grants rights to evaluate, alter, and/or circumvent technical and/or security measures of the Customer's resources, IT infrastructure, and data, where necessary for the performance the Service.