

kaspersky
expert training

Windows incident response

**Course
program**

No	Track	What you will learn	What you will practice	Lesson	Practice	Evaluation
1	Introduction	<ul style="list-style-type: none">• About your trainer• Course roadmap• The CIA Triad• The cyberthreats landscape• APT attacks and Cyber Kill Chain• Key terms and definitions	—	Course introduction	—	—
				Foundation of information security		
				Overview of cyber threat landscape		
				Cyber Kill Chain		
				Open-source intelligence (OSINT)		
2	Incident response process	The 6 stages of the incident response process: <ul style="list-style-type: none">• Preparation• Identification• Containment• Eradication• Recovery• Post-incident activity	<ul style="list-style-type: none">• Creating an incident response plan	Incident response process	Applied Session: IR plan for industrial case Solution: IR plan for industrial case	Quiz
				Stage 1: preparation		
				Stage 2: identification		
				Stage 3: containment		
				Stage 4 and 5:		
				Stage 6: post incident		
				Incident response summary	—	—

No	Track	What you will learn	What you will practice	Lesson	Practice	Evaluation
3	Incident detection: network- and system-based	<ul style="list-style-type: none">• How an incident can be detected• How to verify a detected incident	<ul style="list-style-type: none">• Live incident verification and analysis on victim machines (using different approaches: IRCD and PowerShell)	How to work in the virtual lab	—	—
				Introduction to the practical case	Applied session: run-through attack scenario	—
				Incident detection: system-based	Applied session: live analysis on the victim machines Solution: live analysis with IRCD Solution: live analysis with PowerShell	Quiz
4	Evidence acquisition	<ul style="list-style-type: none">• How to acquire digital evidence in a forensically sound environment, while considering evidence integrity• The difference between full forensic image and triage collection	<ul style="list-style-type: none">• Triage data acquisition using the FTK-Imager• Triage data acquisition using Velociraptor	Evidence acquisition	—	—
				Triage approach	Applied session: memory acquisition with Dumpit and FTK-Imager, and triage data collection with FTK-manager Solution: Triage data acquisition with FTK-Imager	Quiz

No	Track	What you will learn	What you will practice	Lesson	Practice	Evaluation
				Triage data acquisition with KAPE	Applied session: Triage data acquisition with Velociraptor	Quiz
				Solution: triage collection with FTK imager and Velociraptor		
				Evidence acquisition with Paladin, and acquisition over visualization	—	—
5	Memory analysis	<ul style="list-style-type: none"> Memory analysis with Volatility framework 	<ul style="list-style-type: none"> Memory forensic analysis on the acquired memory in order to extract relevant information for the case under investigation 	Memory forensics	Applied session: memory forensic analysis on the acquired memory Solution: memory forensic analysis	Quiz
6	Log file analysis	<ul style="list-style-type: none"> ELK Stack for log file analysis 	<ul style="list-style-type: none"> Log file analysis using the Linux command line, Log Parser and Windows PowerShell 	Log file analysis	Applied session: M S IIS log file analysis using the ELK Stack Solution: log file analysis	Quiz
7	Network analysis	<ul style="list-style-type: none"> How to dump network traffic for analysis 	<ul style="list-style-type: none"> Creating Suricata rules for network intrusion detection Network analysis with Wireshark 	Network IOCs: dumping network traffic	—	—
				Network analysis tools	Applied session: network forensic analysis tools Solution: Network forensic analysis tools	Quiz

No	Track	What you will learn	What you will practice	Lesson	Practice	Evaluation
				Network intrusion detection with Suricata	Applied session: network intrusion detection with Suricata Solution: Network intrusion detection with Suricata	Quiz
8	Cyber Threat Intelligence (CTI)	<ul style="list-style-type: none">• What is an Indicator of Compromise (IOC)• The need for IOC scanning in the IR process• The IOC scanning cycle• An example of an IOC sharing platform• YARA and how to write YARA rules• How to create YARA rules to detect malicious files in a case study	<ul style="list-style-type: none">• Creating YARA rules for the detection of malicious files	Scanning for indicators of compromise (IOCs)	Applied session: Creating YARA rules for the detection of malicious files Solution: Scanning for Indicators of compromise	Quiz
				HOST-based IOC scanning with YARA		
				Course summary	—	—

Own the knowledge, outsmart the threat.

[Buy now](#)

[Find a partner](#)

[Contact us](#)

kaspersky