kaspersky
expert training

Security operations and threat hunting

Course
program

№	Track	What you will learn	What you will practice	Section	Lesson	Evaluation
0	Course overview	• About your trainers • Course roadmap • Course structure	–		Course introduction	–
					Introduction to virtual lab	–
1	Introduction to SOC	• General Cybersecurity Concepts: the nature of targeted attacks and SOC's role in responding to them • SOC people: structure of and roles in the SOC team • SOC service model • SOC use cases and playbooks • SOC process tree • Security monitoring and incident handling • Threat intelligence and threat hunting	• TTP hunting • WMI consumer hunting • Linux service hunting • Domain anomaly hunting		Introduction to SOC	–
					SOC people	–
				SOC services	Introduction to SOC services	–
					Security monitoring	Knowledge check: security monitoring
					SOC use cases	Knowledge check: SOC use cases
					Threat intelligence	Knowledge check: threat intelligence
					Threat hunting	Knowledge check: threat intelligence
				SOC technologies	SOC technologies	–
					In detail: ELK Stack	–
					SOC tools	–
				SOC development	SOC development and maturity levels	–

№	Track	What you will learn	What you will practice	Section	Lesson	Evaluation
				Labs	Lab: threat hunting walkthrough	
					Lab: Windows WMI consumer hunting	Quiz
					Lab: Linux service hunting	Quiz
					Lab: domain name hunting	Checkpoint quiz
2	Windows environment threat hunting	• Windows OS main cybersecurity features • Processes, places and sensitive information storage • Kerberos attacks and exploitation • Windows active directory audit management • Preventing account manipulation, privilege escalation and lateral movement • Mapping offensive activities onto logs	• Searching for the actions of adversaries from the logs • Matching attacking techniques with the MITRE ATT&CK matrix • Using Windows audit for investigations	Windows credentials and authentication	SAM and NTDS DIT. Part 1	Knowledge check: SAM and NTDS DIT. Part 1
					Lab: Password credentials in SAM and NTDS	Quiz
					SAM and NTDS DIT. Part 2	Knowledge check: SAM and NTDS DIT. Part 2
					Lab: Password credentials in memory	Quiz
					SAM and NTDS DIT. Part 3	Knowledge check: SAM and NTDS DIT. Part 3
					Lab: Security support providers	Quiz
					Lab: User rights	Quiz
					Lab: Windows services exploitation	Quiz

№	Track	What you will learn	What you will practice	Section	Lesson	Evaluation
				Windows privileges	Privileges and access control Lab: Windows privileges	Knowledge check: privileges and access control
					UAC Lab: UAC	Knowledge check: UAC
					Pass the token Lab: Pass the token and Impersonation	Knowledge check: pass the token
				Kerberos	Kerberos principles	Knowledge check: Kerberos
					Kerberoasting Lab: Kerberoasting	Knowledge check: Kerberoasting Quiz
					AS-REP roasting Lab: AS-REP roasting	Knowledge check: AS-REP roasting
					Silver ticket Lab: Silver ticket	Knowledge check: Silver ticket Quiz
					Golden ticket Lab: Golden ticket	Knowledge check: Golden ticket Checkpoint quiz

№	Track	What you will learn	What you will practice	Section	Lesson	Evaluation
				Windows security auditing	Windows security auditing Lab: Windows Security Auditing	Knowledge check: Windows security auditing Quiz
3	Linux security, attack vectors and hunting	• Linux general info: distros, package management, important features, etc. • Linux security components • Linux monitoring • Linux capabilities and auditing system	• System tool privilege abuse hunting and investigation (openssl) • Auditd telemetry for hunting and investigation • Sudo misconfiguration abuse hunting and investigation	Linux security	–	–
				Mandatory access control	–	–
				Labs	Lab: openssl	Quiz
					Lab: sudo privelage escalation	Checkpoint quiz
4	Network threat hunting	• Basics of network technologies • Common approaches to the network security • Network security monitoring • Specialized network devices	• Investigation spoofing and replying attacks • Investigation server-side attacks	Introduction to networks	–	–
				Typical network attack	–	–
				Network security monitoring tools	–	–
				Labs	Lab: Spoofing and replying. Investigation with Wireshark and Zeek	Checkpoint quiz
					Lab: client-side attack	–
				Course summary	–	–

Thank you!

kaspersky.com

Discord server: kas.pr/g2j8

Help page: kas.pr/ii9f

kaspersky