kaspersky
expert training

Hunt APTs with Yara like a GReAT ninja

Course
program

№	Track	Lesson	Practice	Evaluation
1	Inception	Introduction and Yara overview	Lab: Hands-on with a Yara rule	Checkpoint quiz
		Virtual lab introduction		
		Yara rule design tips	—	
2	Strings-based rules	A rule to find rules	—	Knowledge check
		Strings and basic conditions	—	
		—	Lab: BlueTraveller Solution: BlueTraveller	Checkpoint quiz
		—	Lab: DiplomaticDuck Solution: DiplomaticDuck	
3	Designing efficient rules	Writing good rules	Lab: DoubleFantasy. Part 1 Solution: DoubleFantasy. Part 1	Checkpoint Quiz
			Lab: DoubleFantasy. Part 2 Solution: DoubleFantasy. Part 2	
			Lab: DoubleFantasy. Part 3 Solution: DoubleFantasy. Part 3	
		Performance tips	—	

№	Track	Lesson	Practice	Evaluation
4	Taking advantage of Yara modules	Yara’s PE library	Lab: TripleFantasy Solution: TripleFantasy	Checkpoint quiz
			Lab: WildNeutron Solution: WildNeutron	
			Lab: Polymorphic keylogger Solution: Polymorphic keylogger	
		Yara’s other libraries	Lab: Miniduke Solution: Miniduke	
			Lab: fake Chinese samples Solution: fake Chinese samples	
5	Hunting for new undetected samples on VTI	Hunting for new undetected samples on VTI	—	Checkpoint Quiz
6	Wildcards	—	Lab: Equation Solution: Equation	Checkpoint Quiz
			Lab: Sofacy Solution: Sofacy	
7	Digital certificates, imphashes and developers' footprints	—	Lab: case study EyePyramid Solution: EyePyramidSofacy	Checkpoint Quiz
			Lab: Volodimir’s Exploits Solution: Volodimir’s Exploits	

№	Track	Lesson	Practice	Evaluation
8	Malicious Office documents, OLE format	XLS Files	Lab: BlackEnergy XLS Files Solution: BlackEnergy XLS Files	Checkpoint quiz
			Lab: CERTUTIL Solution: CERTUTIL	
9	Expert Yara exercises	Hunting for new undetected samples on VTI	Lab: Freaky Shelly Solution: Freaky Shelly	Checkpoint Quiz
			Lab: case study Lazarus / Bluenoroff Solution: Lazarus / Bluenoroff	
			Lab: Mibsun Solution: Mibsun	
			Lab: case study Silverlight 0-day Solution: Silverlight 0-day	
			Lab: Lotus Panda Solution: Lotus Panda	
			Lab: Iced Turla Solution: Iced Turla	
10	YarGen, automation and a bit of magic	—	Lab: let's use YarGen	Checkpoint Quiz
		Setting up for yourself	—	
		Course summary	—	—

Thank you!

kaspersky.com

Discord server: kas.pr/g2j8

Help page: kas.pr/ii9f

kaspersky