kaspersky
expert training

Hunt APTs with Yara like a GReAT ninja

Course
program

№	Track	What you will learn/practice	Lesson	Practice
1	Inception	• What Yara is and what you can do with this tool • Yara syntax • Yara design tips	Introduction and Yara overview	Hands-on with a Yara rule
			Virtual lab introduction	
			Yara rule design tips	Checkpoint quiz
2	Strings-based rules	• A rule to find rules • Interesting strings • PE structure fields	The rules of Yara club	Knowledge check
				Lab: BlueTraveller
			Strings and basic conditions	Lab: DiplomaticDuck
				Checkpoint quiz
3	Designing efficient rules	• Designing efficient rules • Performance tips	Writing good rules	Checkpoint Quiz
			Performance tips	Lab: DoubleFantasy
4	Taking advantage of Yara modules	• Additional Yara modules	Yara's PE library	Lab: TripleFantasy
				Lab: WildNeutron
				Lab: Polymorphic keylogger
			Yara's other libraries	Lab: Miniduke
				Lab: fake Chinese samples
				Checkpoint quiz
5	Hunting for new undetected samples on VTI	• Work with VirusTotal Intelligence	Hunting for new undetected samples on VTI	Checkpoint quiz
6	Wildcards	Wildcards through exercises featuring the Equation group and Sofacy	—	Lab: Equation
				Lab: Sofacy
				Checkpoint Quiz

№	Track	What you will learn/practice	Lesson	Practice
7	Digital certificates, imphashes and developers' footprints	• Exercises based on WildNeutron, Eye-Pyramid and other famous cases	–	Lab: WildNeutron. Part 2 Lab: case study EyePyramid Lab: Volodimir's exploits Checkpoint Quiz
8	Malicious office documents OLE format	• Dumping OLE files	XLS files	Lab: BlackEnergy XLS files Lab: Certutil Checkpoint Quiz
9	Expert Yara exercises	• Hunting for samples based on real cases	–	Lab: Freaky Shelly Lab: case study Lazarus / Bluenoroff Lab: Mibsun Lab: case study Silverlight 0-day Lab: Lotus Panda Lab: Iced Turla Checkpoint Quiz
10	YarGen, automation and a bit ofmagic	• Use of automatic Yara generators • Setting up Yara environment within your organization • Hunting threats	Setting up for yourself	Lab: let's use YarGen
			Course summary	Checkpoint Quiz

Thank you!

kaspersky.com

Discord server: kas.pr/g2j8

Help page: kas.pr/ii9f

kaspersky