

Hunt APTs with Yara

Course
program

No	Track	What you will learn/practice	Lesson	Practice
1	Inception	<ul style="list-style-type: none">What Yara is and what you can do with this toolYara syntaxYara 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	<ul style="list-style-type: none">A rule to find rulesInteresting stringsPE structure fields	The rules of Yara club	Knowledge check
				Lab: BlueTraveller
			Strings and basic conditions	Lab: DiplomaticDuck
				Checkpoint quiz
3	Designing efficient rules	<ul style="list-style-type: none">Designing efficient rulesPerformance tips	Writing good rules	Checkpoint Quiz
			Performance tips	Lab: DoubleFantasy
4	Taking advantage of Yara modules	<ul style="list-style-type: none">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	<ul style="list-style-type: none">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

No	Track	What you will learn/practice	Lesson	Practice
7	Digital certificates, imphashes and developers' footprints	<ul style="list-style-type: none">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	<ul style="list-style-type: none">Dumping OLE files	XLS files	Lab: BlackEnergy XLS files
				Lab: Certutil
				Checkpoint Quiz
9	Expert Yara exercises	<ul style="list-style-type: none">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 of magic	<ul style="list-style-type: none">Use of automatic Yara generatorsSetting up Yara environment within your organizationHunting threats	Setting up for yourself	Lab: let's use YarGen
			Course summary	Checkpoint Quiz

Own the knowledge, outsmart the threat.

[Buy now](#)

[Find a partner](#)

[Contact us](#)

kaspersky