kaspersky

Hunt APTs with Yara like a GReAT Ninja

Our New Cybersecurity Training for Experts

Have you ever wondered how Kaspersky discovered some of the world's most famous APT attacks? Now, you can enhance your threat hunting career, improve incident response strategies for your business and get the inside track - from the comfort of your home. In our brand new online training, Kaspersky experts will lead you through an essential tool for every threat hunter: the Yara detection engine.

This self-paced training includes a hands-on virtual lab with lots of exclusive exercises from real world cases worked on by Kaspersky researchers.

Hands-on training
Use our virtual lab to complete 20+ practical exercises, all based on Kaspersky's exclusive APT research.

Become more efficient
Take your cybersecurity skills to the next level by learning how to identify threats quicker and with less effort.

Learn with the best
Kaspersky experts are threat hunting pioneers. Now you can discover how YARA helps them uncover APTs that nobody else can find.

Course overview

Hunt APTs with Yara Like a GReAT Ninja is suitable for both beginners and experienced Yara users - no hardcore reverse engineering skills are needed.

Why Yara?

For InfoSec professionals

- ✔ Advance your career as a threat hunter
- ✔ Hunt threats more efficiently
- ✔ Find APT samples on VirusTotal
- ✔ Build effective threat detection strategies

For enterprises

- ✔ Train your team to find new malware samples, new exploits and zero-days
- ✔ Speed up incident response
- ✔ Increase your defences with custom rules

Practical outcomes

During this training you will learn how to write the most effective Yara rules, how to test them and improve them to the point where they find threats that nobody else does.

What you'll learn

- ✓ Write cleaner, more efficient, Yara rules
- ✓ Utilise tips & tricks to create fast and efficient rules
- ✓ Use Yara generators to save time and effort when writing codes
- ✓ Test Yara rules for false positives that could skew your results

- ✓ Hunt new undetected samples in your infrastructure and cloud platforms
- ✓ Use external modules within Yara for even more efficient hunting
- ✓ Discover secrets of anomaly search
- ✓ Test your new skills on real life cases like BlueTraveller and DiplomaticDuck

Training highlights

🔒	Access	6 months to complete your course from activation of your access code
🕑	Language	Courses delivered in English with subtitles
📝	Pace	Self-guided learning that fits around your life
🕐	Course duration	It will take you approximately 15 hours to finish the course
☁	Downloads	PDF downloads of training materials & tips
📱	Learning environment	Browser-based via desktop, mobile & tablet (excludes virtual lab which requires an RDP client)
👤	Course author	Costin Raiu, Director of GReAT, Kaspersky
▶	Guided videos	Over 50 videos to guide you through the course
⚙	Access to virtual lab	200 hours of virtual lab time for hands-on learning
🔍	Platform support	Available by email 0900 - 1730 UK time on standard business days via help.kasperskyxtraining.com

Learn with the best

Your course leader
Costin Raiu,
Director of GReAT

Costin is Director of Kaspersky's industry leading Global Research and Analysis Team (GReAT), the team that researched the inner workings of Stuxnet, Duqu, Flame, Carbanak, Turla, Lazarus, the Equation Group and many more.

Costin has over 25 years' experience in cybersecurity and specialises in analysing Advanced Persistent Threats and high-level malware attacks.

He is a member of the Virus Bulletin Technical Advisory Board and the Computer AntiVirus Researchers' Organization (CARO) as well as a reporter for the Wildlist Organization International.

Our team of cybersecurity experts is the one of best in the industry, with first hand experience, skills and secret sauces to bring to your online training.

Working globally - in Europe, Russia, the Americas, Asia & the Middle East - the Kaspersky Global Research and Analysis Team is well-known for the discovery and dissection of some of the world's most sophisticated threats, including cyber-espionage and cyber-sabotage activities.

These talented cybersecurity professionals provide leading threat intelligence and research and are frequently sought out by international media for their expert commentary on IT security due to their research into 400+ malicious & advanced cyber-campaigns.

Their expertise, passion and curiosity for the discovery and analysis of cyberthreats is unmatched.

Kaspersky Threat Intelligence Portal: **https://opentip.kaspersky.com/**
Securelist: **https://securelist.com/**