

Syllabus: Malware Analysis to Detection Engineering: A Hands-On Masterclass

Learn how to turn malware analysis findings into detections that actually work. In this live, hands-on masterclass, Uriel Kosayev follows a Windows malware investigation from initial triage and behavioral analysis through telemetry investigation, detection writing, tuning, and validation. You work along in your own Flare-VM lab and Elastic Security environment, watch a detection miss a change in attacker behavior, and use that result to make it better. You leave with the recording and the detection rules you built during the session.

About TrainSec Academy

TrainSec is an online learning hub for current and aspiring cybersecurity pros who understand the need for excellence. Level up or change career using skill-expanding modular learning way. We turn beginners into experts and experts into masters. TrainSec is designed for those who are serious about being at the vanguard of the latest knowledge, skills and trends. We're already working with the best.

Instructor	Uriel Kosayev
Date	2026-11-12 (Thursday)
Time	15:00 UTC (10:00 New York, 16:00 Amsterdam, 17:00 Jerusalem, 20:30 Delhi)
Duration	4 hours, including Q&A
Format	Live online masterclass on Google Meet, hands-on, recording available in the student portal
Series	Tiny Masterclasses by TrainSec. A new live masterclass every month: trainsec.net/events
Language	English
Price	\$59 per seat (includes a \$59 TrainSec course voucher, usable on any course in the catalog)
Lab platform	Attendee-provided Windows VM with Flare-VM installed, plus an Elastic Security free trial account

Your instructor

Uriel Kosayev is a cybersecurity researcher and reverse engineer with over a decade of experience spanning offensive security, malware analysis, and incident response. He co-founded TrainSec Academy and authored two books: *Antivirus Bypass Techniques* (8,000+ copies sold) and *MAoS: Malware Analysis on Steroids* (2025). He has contributed vulnerability research to the MITRE ATT&CK framework and published academic white papers on malware detection and memory-based threats.

- **Instructor profile:** trainsec.net/uriel-kosayev

Target audience

SOC analysts, detection engineers, blue team and purple team practitioners, incident responders, threat hunters, and malware analysts who want to connect technical analysis to actionable detection logic.

Prerequisites

- An understanding of Windows processes, files, the registry, basic networking, and security logs.
- Familiarity with command-line tools and a SIEM or EDR console is helpful.
- Advanced reverse engineering experience is not required. Foundational concepts are explained as they come up.

Tools and software required

This is a hands-on masterclass. Please have both of the following ready before the session:

1. **A malware analysis VM with Flare-VM.** An isolated Windows virtual machine with the [Flare-VM](#) tools installed. Take a clean snapshot before the session, and never run workshop samples on your host computer.
2. **An Elastic Security account.** Register for the [Elastic Security](#) free trial. We use it to write and validate detection rules during the session. Free trials are time-limited, so register a few days before the masterclass so your account is still active on the day.

Learning outcomes

After this masterclass, attendees will be able to:

1. Apply a repeatable malware triage and behavioral investigation workflow.
 2. Connect observed behavior to the telemetry and fields needed for detection.
 3. Write, explain, and adapt detection logic in Elastic Security, including its data requirements and likely false positives.
 4. Validate a detection, recognize coverage gaps, and use controlled bypass testing to improve it.
-

Format and details

- **Core workflow:** ATTACK → TELEMETRY → INVESTIGATION → DETECTION → TUNING → VALIDATION → BYPASS → BETTER DETECTION.
- **Structure:** six modules that follow one investigation from first triage to a validated detection, combining technical explanation, live demonstration, and hands-on work in your own lab.
- **Duration:** 4 hours, including live Q&A. Questions are welcome throughout, with a dedicated block at the end.

- **Delivery:** live online on Google Meet. The recording is available afterwards in the TrainSec student portal.
 - **Series:** part of Tiny Masterclasses by TrainSec, with a new live masterclass every month. Browse upcoming events at trainsec.net/events.
 - **Language:** English.
 - **Price:** \$59 per seat. Every registrant also receives a \$59 TrainSec course voucher, usable on any course in the catalog.
 - **Certificate:** this masterclass does not include a certificate.
-

Modules

Module 1: Analysis workflow and lab foundations

Define the investigation question, confirm your analysis environment is safe and isolated, and distinguish static analysis, dynamic analysis, and telemetry-based investigation. Identify the evidence needed to explain what a suspicious program actually does.

Module 2: Malware triage and static analysis

Examine file type, hashes, executable metadata, strings, imports, and signs of packing or obfuscation. Use these findings to form testable hypotheses and prioritize deeper inspection. Discuss the limits of file reputation and isolated indicators.

Module 3: Dynamic analysis and behavioral investigation

Observe execution in the isolated Windows lab. Investigate process trees, command lines, file and registry changes, persistence, and network activity. Follow the execution chain and use targeted code inspection where it helps explain behavior.

Module 4: From behavior to useful telemetry

Map observed actions to the available Windows Event Logs and EDR telemetry. Identify relevant event fields, correlate activity across processes and timestamps, and distinguish a missing detection from missing data. Discuss how telemetry configuration affects visibility.

Module 5: Detection engineering and tuning

Translate the investigation into behavior-focused detection hypotheses. Write Elastic Security KQL queries, understand their required data fields, and distinguish a search query from a configured detection rule. Tune the logic against benign activity and document assumptions, exclusions, and coverage limits.

Module 6: Validation and bypass testing

Replay the behavior in the lab and check whether the detection triggers as expected. Test controlled variations such as changed filenames or execution context, investigate why coverage breaks, and

improve the rule. Re-test both malicious and benign cases before considering the detection ready for wider validation.

Discussion and Q&A

Review the complete investigation-to-detection workflow, common analysis mistakes, and practical next steps for applying the method in your own authorized environments.

Deliverables (included with registration)

1. **Your own detection rules.** The detection rules you write, tune, and validate during the masterclass stay with you in your Elastic Security environment.
2. **Practical, hands-on experience.** You work through the full investigation-to-detection workflow yourself, not just watch it.
3. **Masterclass recording.** Available after the event in the TrainSec student portal.
4. **\$59 TrainSec course voucher.** Per registrant, usable on any course in the catalog.

Before the session

- **Lab check:** boot your Flare-VM, confirm the tools launch, and take a clean snapshot. Log in to your Elastic Security trial and confirm you can reach the console.
- **Connection check:** use a laptop or desktop with a stable internet connection and working audio. Join the Google Meet a few minutes early to test audio and screen readability.
- **Bring your questions:** prepare questions about malware investigation or detection challenges. Anonymize any examples from your workplace.

About Tiny Masterclasses

This event is part of **Tiny Masterclasses by TrainSec**: a series of short, live, hands-on masterclasses from TrainSec instructors. Each one takes a single deep technical topic and delivers it in a few focused hours, with a recording you keep. A new masterclass runs every month. See what's coming next at trainsec.net/events.

Where this leads

This masterclass is a focused, hands-on taste of Uriel's full course, [Detection Engineering Professional: Attack Simulation & Defense](#), where you simulate attacks in a lab and write your own detection rules across many more techniques. Masterclass attendees receive an exclusive discount on the full course.

References and further reading

- [Flare-VM on GitHub](#): installation instructions for the analysis VM.

- [Elastic Security](#): free trial registration.
- [Detection Engineering: Blue, Purple and Red Team](#): Uriel's article on the TrainSec library.

Contact & support

Student support	info@trainsec.net
Discord community	discord.com/invite/qugcNyWdaU
LinkedIn	linkedin.com/company/trainsec
X (Twitter)	x.com/TrainSec
Website	trainsec.net