



SOC TIER 3 : ADVANCED THREAT HUNTING & SECURITY ENGINEERING

250 HOURS TOTAL | ADVANCED PRACTICAL MASTERCLASS

Interested?

info@trivian.nl | 085 - 760 81 85 | Boeing Avenue 254, 1119 PZ Schiphol-Rijk

COURSE DESCRIPTION

The **SOC Tier 3: Advanced Threat Hunting & Security Engineering** course is a professional masterclass intended for experienced analysts and high-level graduates wishing to transition from reactive monitoring to proactive defense architecture.

Students in this course will be exposed to the highest level of defensive cyber operations, moving beyond standard alert triage into the world of Detection Engineering, Advanced Malware Reverse Engineering, and deep-dive Digital Forensics (DFIR). The program focuses on "The Invisible Attacker" - teaching students how to hunt for Advanced Persistent Threats (APTs) and "Living off the Land" techniques that bypass traditional security controls. By practicing with advanced tools like IDA/Ghidra, Volatility, and automated SOAR orchestration, students gain the skills required to lead technical response teams and architect security logic from scratch.

This unique training course is developed by leading cyber experts to meet the standards of top global institutes. It places a significant emphasis on technical leadership and the mastery of complex security ecosystems, including containerized environments and automated threat intelligence pipelines.

THE COURSE FOCUSES ON THREE CORE PILLARS:

- **Detection Engineering:** Moving from "consuming" alerts to "creating" high-fidelity detection logic (Sigma/Yara).
- **Advanced DFIR:** Performing root-cause analysis at the memory and kernel level to deconstruct sophisticated breaches.
- **Proactive Hunting:** Utilizing Python, advanced KQL, and AI-driven behavior analysis to find threats before they trigger an alarm.

TARGET AUDIENCE:

This course is intended for SOC Tier 2 Analysts, Incident Responders, or graduates of the SOC T1+T2 program who wish to reach the rank of Senior Analyst or Security Engineer.

PREREQUISITES:

- Completion of SOC Tier 1+2 program OR 1-2 years of experience in a SOC environment.
- Strong technical background in Networking and OS Internals.
- Proficiency in at least one querying or scripting language (KQL/SPL/Python).



PROGRAM STRUCTURE OVERVIEW

MODULE	TOPIC	TOTAL HOURS	THEORY	PRACTICAL
1	Detection Engineering & Content Creation	50	15	35
2	Advanced Malware Analysis & Reverse Engineering	60	20	40
3	Proactive Threat Hunting (Advanced KQL/Python)	50	10	40
4	Advanced DFIR: Memory & Network Forensics	50	15	35
5	Security Architecture, SOAR & Leadership	40	20	20
Total hours		250	80	170

DETAILED SYLLABUS

MODULE 1: DETECTION ENGINEERING & CONTENT CREATION (50 HOURS)

FOCUS: MASTERING THE "BLUE TEAM" VERSION OF EXPLOIT DEVELOPMENT—CREATING LOGIC THAT CATCHES ZERO-DAYS AND STEALTHY MOVEMENT.

SUBJECT	TOTAL HOURS	HOURS
The Detection Lifecycle	Designing a pipeline from Log Ingestion to Alert Triage.	5
Sigma & Yara Mastery	Writing vendor-agnostic rules for SIEMs and EDR scanners.	10
Advanced SIEM Logic	Multi-stage correlation, behavior-based logic, and statistical outliers.	15
Purple Teaming Labs	Using "Atomic Red Team" to simulate attacks and verify detection gaps.	10
False Positive Tuning	Large-scale noise reduction and high-fidelity alert design.	10
Total hours		50



MODULE 2: ADVANCED MALWARE ANALYSIS & REVERSE ENGINEERING (60 HOURS)

FOCUS: MOVING BEYOND "SANDBOX" REPORTS INTO THE ACTUAL ASSEMBLY CODE OF A THREAT.

SUBJECT	TOTAL HOURS	HOURS
Advanced Static Analysis	Identifying packers, cryptors, and obfuscation techniques.	10
Introduction to x86/64 ASM	Reading assembly code to understand CPU instructions during execution.	10
Reverse Engineering Labs	Using Ghidra and IDA Pro to deconstruct malicious binaries.	15
Debugging & Behavior	Dynamic debugging with x64dbg/OllyDbg to find C2 domains in real-time.	15
De-obfuscating Scripts	Handling "Fileless" malware (PowerShell, VBS, and JS loaders).	10
Total hours		60



MODULE 3: PROACTIVE THREAT HUNTING (50 HOURS)

FOCUS: FINDING THE "SILENT" ATTACKER THAT HAS ALREADY BYPASSED ALL AUTOMATED DEFENSES.

SUBJECT	TOTAL HOURS	HOURS
Hunting Frameworks	Hypothesis-based hunting using the Targeted Hunting (TaHiTI) model.	5
Python for SOC T3	Writing scripts for automated log enrichment and API-based data gathering.	15
Living off the Land (LotL)	Hunting for WMI, PowerShell, and Certutil abuse in enterprise logs.	10
Advanced KQL/SPL	Using advanced functions (make-series, mv-expand, join) for anomaly detection.	10
C2 Beacon Detection	Identifying command-and-control heartbeats via network entropy analysis	10
Total hours		50



MODULE 4: ADVANCED DFIR (DIGITAL FORENSICS & INCIDENT RESPONSE) (50 HOURS)

FOCUS: POST-MORTEM RECONSTRUCTION. DISCOVERING THE "ROOT CAUSE" OF A BREACH.

SUBJECT	TOTAL HOURS	HOURS
Memory Forensics	Using Volatility to find rootkits, injected DLLs, and hidden processes.	15
Network Forensics	Investigating full PCAPs and Zeek logs to reconstruct data exfiltration.	10
Timeline Reconstruction	Correlating MFT, Registry, and Event Logs into a "Master Attack Timeline."	15
Cloud-Native IR	Investigating identity-based persistent threats in Azure AD and AWS IAM.	10
Total hours		50

MODULE 5: SECURITY ARCHITECTURE, SOAR & LEADERSHIP (40 HOURS)

FOCUS: ORCHESTRATION AND STRATEGIC MANAGEMENT OF THE SOC.

SUBJECT	TOTAL HOURS	HOURS
SOAR Engineering	Building automated playbooks for enrichment and containment via APIs.	15
Threat Intelligence (CTI)	Operationalizing MISP/OpenCTI feeds into active defense mechanisms.	5
Incident Leadership	Handling crisis communication, executive reporting, and legal/PR liaison.	10
Cloud-Native IR	Auditing SOC efficiency using Metrics (MTTD/MTTR) and Maturity Models.	10
Total hours		40





trivian
CYBERSECURITY ACADEMY

Interested?

info@trivian.nl | 085 - 760 81 85 | Boeing Avenue 254, 1119 PZ Schiphol-Rijk