



SOC ANALYST TIER 1 + TIER 2 : UNIFIED PROFESSIONAL PROGRAM

600 HOURS TOTAL | OPTIMIZED PEDAGOGICAL SPLIT (THEORY VS. PRACTICAL)

Interested?

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

COURSE DESCRIPTION

The **SOC Analyst Tier 1 + Tier 2** program is a comprehensive training course intended for an audience looking to make a career change, or alternatively for those wishing to enter the professional world of defensive cyber security operations.

Students in this course will be exposed to the full spectrum of modern Security Operations Center (SOC) workflows, moving from IT foundations to advanced incident detection and response. The program emphasizes real-world simulations, utilizing enterprise-grade SIEM/SOAR tools and EDR interfaces to practice the material in environments that mirror modern corporate infrastructures. This training equips students with the technical "seat-time" required for the ongoing work of a Tier 1 or Tier 2 analyst in a rapidly changing threat landscape.

This unique training course is developed by the leading professionals in their field, and is comprised of a variety of topics required in the industry today, including Cloud Security and the revolutionary use of AI for SOC productivity. With a great emphasis on imparting practical, work-oriented knowledge, the course ensures graduates are ready to integrate into high-pressure security teams.

THE COURSE IS DIVIDED INTO TWO DISTINCT PEDAGOGICAL PHASES:

- **Part One: Systems & Security Foundations** – Mastering Windows, Linux Essentials (LPI), and Networking (CCNA Knowledge) to build a robust defense-oriented mindset.
- **Part Two: SOC Operations & AI Productivity** – Intensive training in SIEM/SOAR, Incident Response, Cloud Defense, and AI-powered analysis to accelerate investigation and reporting.

TARGET AUDIENCE:

This course is intended for anyone wishing to build a career in cyber security operations and successfully integrate into the industry as a SOC Analyst.

PREREQUISITES:

- Good basic understanding of Windows environment.
- Technical level of English reading.
- High motivation for hands-on technical learning.



PROGRAM STRUCTURE OVERVIEW

MODULE	TOPIC	TOTAL HOURS	THEORY	PRACTICAL
1	IT & Systems Foundations (Windows & Linux)	120	75	45
2	Networking & Packet Analysis	80	50	30
3	Offensive Cyber & MITRE Framework	80	25	55
4	SOC Tier 1: SIEM & Log Analysis	100	30	70
5	SOC Tier 2: Incident Response & Forensics	80	30	50
6	Cloud Security Operations	70	30	40
7	AI for SOC Productivity & Security	70	30	40
Total hours		600	270	330

DETAILED SYLLABUS CHAPTERS

MODULE 1: IT & SYSTEMS FOUNDATIONS (120 HOURS)

SUBJECT	TOTAL HOURS	THEORY	PRACTICAL
Virtualization	Architectures of VMware/ESXi vs Hyper-V.	6	4
Windows Admin	Deep dive into AD, Kerberos, GPO, and the Windows Kernel.	30	15
Linux LPI Essentials	Kernel structure, Boot process, Shell Scripting for Analysts.	25	20
Identity (IAM)	Auth mechanisms (OIDC, SAML, NTLM) & VPN logic.	14	6
Total hours		75	45



MODULE 2: NETWORKING & PACKET ANALYSIS (80 HOURS)

FOCUS: VISUALIZING THE INVISIBLE. UNDERSTANDING THE "HANDSHAKES."

SUBJECT	TOTAL HOURS	THEORY	PRACTICAL
TCP/IP & Protocols	OSI Model, DNS, HTTP/S, SMTP, SSL/TLS Handshakes.	25	5
Wireshark & DPI	Decrypting TLS, Follow Stream, Traffic Graphing.	10	15
Defensive Hardware	FW, WAF, IPS, Proxy - Placement and logic.	15	10
Total hours		50	30

MODULE 3: OFFENSIVE CYBER SECURITY (80 HOURS)

FOCUS: THINKING LIKE A HACKER. HIGH PRACTICAL FOCUS.

SUBJECT	TOTAL HOURS	THEORY	PRACTICAL
ATT&CK Framework	Mapping adversary behaviors to the matrix.	10	5
Recon & Enumeration	Nmap, Gobuster, vulnerability identification.	5	15
Exploitation	Metasploit, web attacks (SQLi/XSS), PrivEsc.	5	20
Lateral Movement	Pass-the-Hash, SMB Relay, AD Attacks.	5	15
Total hours		25	55



MODULE 4: SOC TIER 1 - SIEM & LOG ANALYSIS (100 HOURS)

SUBJECT	TOTAL HOURS	THEORY	PRACTICAL
SIEM Architecture	Data connectors, Indexing, and Search Head logic.	10	10
Log Management	Parsing Syslog, EventLogs, and JSON payloads.	10	15
Alert Triage	Handling high-volume alerts, False Positive reduction.	5	20
KQL / SPL Querying	Writing custom correlation rules and hunt queries.	5	25
Total hours		30	70

MODULE 5: SOC TIER 2 - IR & FORENSICS (80 HOURS)

FOCUS: INVESTIGATING THE "UNKNOWN."

SUBJECT	TOTAL HOURS	THEORY	PRACTICAL
Incident Management	Ticketing (Jira/TheHive) and the IR Lifecycle.	15	5
Host Forensics	MFT analysis, Registry hives, and Prefetch logs.	5	20
Memory Forensics	Investigating Volatile RAM (Volatility).	5	15
SOAR Automation	Building Playbooks for automated containment.	5	10
Total hours		30	50



MODULE 6: CLOUD SECURITY OPERATIONS (70 HOURS)

FOCUS: MODERNIZING THE SOC.

SUBJECT	TOTAL HOURS	THEORY	PRACTICAL
Cloud Architecture	Entra ID (Azure AD), AWS IAM, S3 Bucket Security	15	5
Detection in Cloud	Sentinel/GuardDuty log analysis and alerting.	10	15
Containers & K8s	Docker security, Image scanning, and Pod security.	5	20
Total hours		30	40

MODULE 7: SOC TIER 2 - IR & FORENSICS (70 HOURS)

FOCUS: THE "NEXT-GEN" FORCE MULTIPLIER.

SUBJECT	TOTAL HOURS	THEORY	PRACTICAL
LLMs for Defence	Understanding tokens, context windows, and hallucinations.	10	5
Prompt Engineering	Advanced prompting for query generation (SQL/SPL/KQL).	10	15
SOC Copiloting	Using AI for Automated Reporting and IR Summaries.	5	10
AI Governance	Data privacy and securing the "AI pipeline."	5	10
Total hours		30	40

TOTAL HOURS

600





trivian
CYBERSECURITY ACADEMY

Interested?

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