K7 ACADEMY

SOC Analyst Professional Programme

Overview

The SOC Analyst Professional Programme is an advanced, hands-on course for candidates who have completed the SOC Foundation Programme or have equivalent experience. Across 60 hours, you will master penetration testing fundamentals, EDR and Sysmon deep-dives, SIEM deployment, threat hunting, memory forensics, Python automation, YARA rules, SOAR playbooks, and full incident response – all mapped to MITRE ATT&CK.

Mode	Duration	Level
Online/Offline Classes	60 Hours	Intermediate to Advanced

Who Should Enrol?

- SOC Foundation Programme graduates
- Tier 1 SOC Analysts looking to move to Tier 2/Tier 3
- Security Engineers wanting Blue Team depth
- Penetration Testers exploring the defensive perspective
- Incident Responders & Threat Hunters seeking structured upskilling

Learning Outcomes

- Perform ethical hacking reconnaissance, exploitation, and privilege escalation
- Detect Active Directory attacks (Kerberoasting, Pass-the-Hash, Golden Ticket)
- Deploy and tune Sysmon and correlate events with EDR telemetry
- Install, configure, and write detection rules in an SIEM platform
- Conduct memory forensics using Volatility to identify injected code
- Write Python scripts for log parsing, IOC extraction, and alert automation
- Author YARA rules for custom malware detection signatures
- Build and execute SOAR playbooks for automated incident response
- Perform hypothesis-driven threat hunting with MITRE ATT&CK
- Integrate threat intelligence (MISP, OpenCTI, IOC feeds) into SOC workflows
- Lead an end-to-end incident response lifecycle and produce professional reports

Modules

Module 1 – Penetration Testing & Ethical Hacking

- Scope & Rules of Engagement – Passive & Active Reconnaissance
- Kali Linux and MITRE ATT&CK Mapping
- Performing Vulnerability Assessments
- Network Security Testing – Network Penetration Testing
- Post-Exploitation, Privilege Escalation & Documentation
- Active Directory Attacks – Kerberoasting, Pass-the-Hash, DCSync, Golden Ticket
- Understanding Web Application Security – OWASP Top 10
- Web Application Testing and Tools (Burp Suite, OWASP ZAP)

Module 2 – Sysmon, EDR & Advanced Log Analysis

- Sysmon – Architecture, Installation & Configuration
- Sysmon Event IDs Deep Dive (1,3,7,8,10,11,13,22,25...)
- Writing & Tuning Sysmon Config (SwiftOnSecurity/ olafhartong templates)
- Explore K7 Cyber Protect 360 – EDR platform
- EDR Log Analysis – Process Trees, Parent-Child Relationships
- Malware Analysis with EDR + Sysmon Correlation
- Log Management & Retention – Syslog, Beats, Fluentd, Chain of Custody
- Windows ETW (Event Tracing for Windows)

Module 3 – SIEM: Build, Tune & Detect

- SIEM Architecture – Manager, Indexer, Dashboard & Agents
- SIEM Installation & Agent Deployment (Linux + Windows)
- SIEM Rules, Decoders & Alert Tuning
- Integrating Sysmon with SIEM for Windows Telemetry
- File Integrity Monitoring (FIM) with SIEM
- SIEM Architecture and Log Correlation
- MITRE ATT&CK

Module 4 – Bootcamp 1: SOC vs Red Team Exercise

- SOC Exercise – Red Team Launches, Blue Team Detects & Responds
- Post-Exercise Debrief

Module 5 – SOC Operations: Detection, Forensics & Scripting

- Detecting Malware on Endpoints – In-Depth Endpoint Log & Process Analysis
- Network Traffic Analysis, SIEM Integration & Incident Detection
- Email Header & Phishing Analysis – SPF/DKIM/ DMARC, URL Detonation
- Memory Forensics Basics – Volatility, RAM Dumps, Injected Code Detection
- Python for SOC Analysts – Log Parsing, IOC extraction, Automation Scripts
- YARA Rule Writing – Custom Malware Detection Signatures

Module 6 – Incident Response, Threat Hunting & SOAR

- Incident Detection, Triage & Prioritisation – NIST IR Phases, Playbook Development
- Threat Hunting – Hypothesis-driven Hunting with ATT&CK
- Threat Intelligence – MISP, OpenCTI, IOC Feeds & TIP Integration
- Incident Reporting, Communication & Documentation Standards
- Introduction to SOAR – Automation Playbooks & Cortex Analysers
- Threat Intelligence Lifecycle — Collection, Processing, Dissemination, Feedback Loop
- MISP Hands-On – Creating events, Sharing IOCs, Importing external threat feeds
- SOAR Playbook Build Lab — Automated phishing response: Enrich → Block → Ticket

Module 7 – Bootcamp 2: Final Assessment & Capstone

- Final Practical Assessment – Multi-Stage IR Scenario
- Capstone Activity
- Peer Review & Report Critique – Review, grade and improve each other's IR reports

Tools & Technologies Covered

Kali Linux
Offensive security platform

Burp Suite
Web application testing

OWASP ZAP
Web vulnerability scanner

Nmap/Netcat
Network recon & exploitation

Metasploit (intro)
Exploitation framework

Sysmon
Windows telemetry & event logging

K7 Cyber Protect 360 – EDR
Endpoint detection & response

Wazuh SIEM
SIEM deployment & tuning

Elasticsearch/Kibana
Log indexing & dashboards

Volatility 3
Memory forensics framework

Python 3
SOC scripting & automation

YARA
Malware detection rules

MISP
Threat intelligence platform

OpenCTI
Threat intelligence management

Shuffle SOAR
Security automation playbooks

Wireshark
Network traffic analysis

TheHive/Cortex
Incident case management

MITRE ATT&CK Navigator
Technique mapping & coverage

Career Opportunities

Role

- SOC Analyst – Tier 2/Tier 3
- Threat Intelligence Analyst
- Incident Response Analyst
- Detection Engineer
- Threat Hunter
- Security Engineer (Blue)
- SIEM/SOAR Engineer

Certification & Assessment

- Module-wise Quizzes
- Lab Submission Reports – graded hands-on exercises
- Final Certification Exam – Passing Score: 70%

K7 ACADEMY

www.k7academy.com

202607201