



N X 2 2 0

PRACTITIONER • LEVEL 3

SOC Analyst

10

MODULES

288

LAB TASKS

119

CTF CHALLENGES

73

TOPICS

10

COURSE BOOKS

197

SLIDES

10 COURSE BOOKS INCLUDED

SOC Analyst

N X 2 2 0



This program transforms students into skilled SOC Analysts by diving deep into the tools and tactics of modern cyber defense. You will start by mastering Windows domain operations and advanced logging with Sysmon, giving you total visibility into system activity. From there, you'll get hands-on with industry-standard firewalls and intrusion detection systems like pfSense and Snort. The journey continues into the heart of security monitoring, where you'll learn to navigate SIEM platforms like Splunk and the ELK stack. The program concludes with high-level threat hunting using the MITRE ATT&CK framework, leaving you fully prepared to detect, analyze, and respond to complex cyber incidents.

CURRICULUM & WHAT EACH MODULE COVERS

MODULE	TASKS
01 Event Analysis	37
User and Group Account Management Events · Windows Event Viewer Fundamentals · Monitoring Windows Defender and Firewall · +7 more	
02 Firewalls	20
Detecting Scans and Attacks via Firewall Logs · Investigating Firewall Logs for Incident Reports · pfSense Fundamentals and Shell Access · +3 more	
03 IDS/IPS	26
Auditing Rule Sets to Identify Threats · Snort Rule Structure and Syntax · Analyzing Snort Alerts · +1 more	
04 Domain Events	25
Domain Environment Setup and Event Viewer Basics · Domain User Account Lifecycle Events · PowerShell for Bulk Event Log Queries · +7 more	
05 SIEM	32
Monitoring Active Directory and Domain Controllers · Exploring Logs with Kibana Discover · Investigating Malicious Activity with ELK · +3 more	
06 MITRE ATT&CK	35
Detecting Defense Evasion via Disabled Endpoint Protection · Monitoring Snort Service Health via Syslog Severity · Lab Environment and Centralized Logging Pipeline · +6 more	
07 Log Analysis	37
Web Server Access Log Analysis (access.log) · SSH Authentication Log Analysis (auth.log) · Linux Audit Framework Analysis (audit.log) · +4 more	
08 Splunk	28
Aggregating and Displaying Results with SPL Commands · Windows Event Log Monitoring with Splunk · Installing and Configuring the Splunk Server · +8 more	
09 Threat Hunting	30
Writing and Refining YARA Detection Rules · Detecting Attacker Techniques with Sysmon · Foundations of Threat Hunting and Windows Event Logging · +2 more	
10 Incident Response	18
Network Traffic Analysis for Phishing Detection · Analyzing Logs for Network and Web-Based Attacks · Incident Response Frameworks and Playbooks · +2 more	

GOOD TO KNOW

Best after a level 1-2 programme · Self-paced or trainer-led · Cy, the AI helper, answers in the student's own language

HOW EVERY MODULE RUNS

Lab



Extra at 80%



Timed test at 85%



Slides at 90%

A REAL TASK FROM MODULE 9 — THREAT HUNTING

"Install Sysmon with -n for network monitoring on the Windows client and perform a brute-force attack on the RDP service. Analyze the Sysmon Event log and identify the Task Category for the relevant event."

Finish with a capstone project · interview preparation · City & Guilds Assured certificate

DATA AS OF 2026-10-12 · V261012