

SOC Analyst — Blue Team Operations

3-Month Practical Training Programme

3 classes per week · 1 hour per class · 36 classes total

36 instruction hours + 4–6 hours per week lab practice

Live online · taught in English · open worldwide

The defensive counterpart to CEH. You build a working SOC in your own lab — SIEM, EDR, IDS — then detect, investigate and report real attack behaviour inside it.

WEEK 1

Build the SOC Lab

Stand up the environment you will defend for the next twelve weeks.

CLASS	TOPIC	TOOLS USED	WHAT YOU BUILD
1	Build your SOC lab Install VirtualBox, an Ubuntu Server for the SIEM, a Windows 10 endpoint and a Kali attacker box.	VirtualBox, Ubuntu Server, Windows 10, Kali Linux	→ A 3-machine lab with an attacker, a victim and a monitoring server.
2	Networking for defenders Protocols, ports and flows — read from the defender's side, where you see the aftermath.	Wireshark, netstat, ss, tcpdump	→ Capture traffic and identify every protocol in it by port and behaviour.
3	How a SOC actually runs Tier 1/2/3, shift handover, alert queues, escalation paths and SLAs.	Alert triage template	→ Take one alert from raw log to escalation decision and write the handover note.

WEEK 2

Logs — The Raw Material

Read the three log sources every investigation starts from.

CLASS	TOPIC	TOOLS USED	WHAT YOU BUILD
4	Linux logs Where Linux records authentication, services and errors, and how to search them fast.	journalctl, /var/log, grep, awk, cut	→ Find every failed SSH login and the source IP behind them in auth.log.
5	Windows Event Logs The Event IDs that matter: 4624, 4625, 4688, 4720, 7045 — and what each really means.	Event Viewer, wevtutil, PowerShell Get-WinEvent	→ Trace a logon, a failed logon and a new user creation across the log.
6	Sysmon — logging that is actually useful Why native Windows logging is not enough and what Sysmon adds.	Sysmon, SwiftOnSecurity config, Event ID 1/3/11	→ Install Sysmon and capture full process-creation data for an attack.

WEEK 3

Build the SIEM

Get every log into one searchable place.

CLASS	TOPIC	TOOLS USED	WHAT YOU BUILD
7	SIEM concepts and installation What a SIEM does, how it is licensed by volume, and deploying one.	Wazuh (or Splunk Free), Elastic	→ Deploy a working Wazuh manager and reach its dashboard.
8	Onboarding log sources Agents, forwarders and parsing — the unglamorous work that decides if detection works.	Wazuh agent, Winlogbeat, Filebeat	→ Ship Windows and Linux logs into the SIEM and confirm they parse.
9	Searching and querying Turning an investigation question into a query that answers it.	Wazuh query syntax, Splunk SPL, KQL	→ Write five queries that answer five real incident questions.

WEEK 4

Detection Engineering

Stop waiting for alerts and start writing them.

CLASS	TOPIC	TOOLS USED	WHAT YOU BUILD
10	Writing detection rules Rule anatomy, thresholds, and the difference between a signature and behaviour.	Sigma, Wazuh rules, YARA basics	→ Write a working brute-force detection rule and trigger it from Kali.
11	MITRE ATT&CK mapping Describing attacker behaviour in the language the whole industry uses.	ATT&CK Navigator, ATT&CK matrix	→ Map ten of your detections to techniques and find your coverage gaps.
12	Tuning out false positives The reason most SOC's drown: untuned rules. How to cut noise without going blind.	SIEM tuning, allowlists, baselining	→ Take a noisy rule and cut its false positives, measuring before and after.

WEEK 5

Endpoint Detection

See what is happening on the machine itself.

CLASS	TOPIC	TOOLS USED	WHAT YOU BUILD
13	EDR concepts and deployment What EDR sees that a SIEM cannot, and deploying an agent.	Wazuh EDR, LimaCharlie (free tier)	→ Deploy an EDR agent and trigger a real detection from the attacker VM.
14	Hunting processes and persistence Parent-child process trees, LOLBins, and where attackers hide to survive reboot.	Sysmon, Autoruns, Process Explorer, Process Hacker	→ Find a persistence mechanism planted on your own endpoint.
15	Malware triage on the endpoint Deciding quickly whether a file is malicious — safely, without running it.	VirusTotal, PEStudio, strings, CyberChef	→ Triage a suspicious binary and write a verdict with your reasoning.

WEEK 6

Network Detection

Catch what the endpoint missed.

CLASS	TOPIC	TOOLS USED	WHAT YOU BUILD
16	IDS and IPS Signature-based network detection, and why placement decides what you see.	Suricata, Snort, ET Open rules	→ Deploy Suricata and catch an Nmap scan launched from Kali.
17	Network traffic analysis Reading a capture like an analyst: who talked to whom, how often, and why that is odd.	Wireshark, tshark, Zeek	→ Find command-and-control beaconing hidden in a PCAP.
18	Flow analysis and exfiltration Spotting data leaving: volume, timing and destination anomalies.	Zeek logs, RITA, NetFlow	→ Identify a data-exfiltration pattern and quantify what left.

WEEK 7

Threat Intelligence and Hunting

Go looking for what no alert fired on.

CLASS	TOPIC	TOOLS USED	WHAT YOU BUILD
19	IOCs and threat feeds Indicators, their short shelf life, and enriching an artefact properly.	MISP, AlienVault OTX, VirusTotal, AbuseIPDB	→ Enrich an IP, a hash and a domain, and judge the confidence of each.
20	Threat hunting methodology Hypothesis-driven hunting — forming a question the data can answer.	SIEM, hunting templates	→ Run a structured hunt for living-off-the-land binary abuse.
21	Hunting with ATT&CK Using the matrix to pick hunts that matter instead of hunting at random.	ATT&CK Navigator, SIEM queries	→ Hunt for PowerShell abuse (T1059.001) and document what you found.

WEEK 8

Phishing and Email Defence

Handle the attack type that actually arrives every day.

CLASS	TOPIC	TOOLS USED	WHAT YOU BUILD
22	Phishing email analysis Reading full headers, tracing the real sender and judging a link safely.	Email headers, MXToolbox, URLScan.io, VirusTotal	→ Dissect a real phishing header and write the verdict.
23	Malicious attachment analysis Macros, embedded objects and scripts — extracted without executing them.	oletools, olevba, CyberChef, oledump	→ Extract and decode a macro payload from a document safely.
24	Email authentication controls SPF, DKIM and DMARC: what each proves, and what they do not stop.	dig, MXToolbox, DMARC analysers	→ Audit a domain's email authentication and write the gaps.

WEEK 9

Incident Response

Work an incident from detection to closure.

CLASS	TOPIC	TOOLS USED	WHAT YOU BUILD
25	The IR lifecycle NIST phases, roles, and decisions that must be made before the incident, not during.	NIST SP 800-61, IR plan template	→ Write an incident-response plan for a ransomware scenario.
26	Containment and eradication Isolating a host without destroying evidence, and sweeping for the same IOCs elsewhere.	Host isolation, firewall blocks, IOC sweep	→ Contain a compromised lab host and sweep the rest for the same indicators.
27	Evidence handling Order of volatility, chain of custody, and imaging a disk defensibly.	FTK Imager, chain-of-custody form	→ Take a forensic image and complete the custody documentation.

WEEK 10

Digital Forensics

Prove what happened, with evidence.

CLASS	TOPIC	TOOLS USED	WHAT YOU BUILD
28	Disk forensics File systems, deleted data, and building a timeline that tells the story.	Autopsy, FTK Imager, Sleuth Kit	→ Recover deleted files and build a timeline of attacker activity.
29	Memory forensics What only exists in RAM: injected code, live connections, and unencrypted secrets.	Volatility 3, memory dumps	→ Find an injected process inside a memory image.
30	Windows artefacts Registry, Prefetch, ShimCache, Amcache, jump lists — proof a program ran.	Registry Explorer, KAPE, PECmd	→ Prove a specific program executed, with artefact evidence.

WEEK 11

Cloud, Identity and Automation

Defend the places logs now actually live.

CLASS	TOPIC	TOOLS USED	WHAT YOU BUILD
31	Cloud and identity monitoring Sign-in logs, impossible travel, MFA fatigue and token theft.	Azure AD sign-in logs, AWS CloudTrail	→ Detect an impossible-travel sign-in and decide the response.
32	Detecting Active Directory attacks What Kerberoasting, AS-REP roasting and DCSync look like in the logs.	Sysmon, Event ID 4769/4662, BloodHound (defensive)	→ Detect a Kerberoast and a DCSync run against your lab DC.
33	SOAR and automation Automating the repetitive 80% so analysts spend time on the 20% that needs a human.	Shuffle, TheHive, Cortex	→ Build a playbook that auto-enriches every new alert.

WEEK 12

Live Incident, Reporting and Career

Run a real incident end to end and be ready to be hired.

CLASS	TOPIC	TOOLS USED	WHAT YOU BUILD
34	Live incident simulation — part 1 An unannounced intrusion in your lab: detect it, scope it, contain it.	Your full SIEM/EDR/IDS stack	→ Detect and scope a simulated intrusion you were not warned about.
35	Incident part 2 and report writing Root cause, timeline, impact and recommendations a manager can act on.	TheHive, IR report template	→ Write a client-grade incident report with a defensible timeline.
36	SOC career preparation and capstone The interview questions that actually get asked, and presenting your work.	CV and portfolio review	→ Present your investigation and defend your conclusions under questioning.

Lab and conduct. Every technique in this programme is practised inside a lab you build yourself, on machines and networks you own. Students are never asked to touch a third-party system. The same techniques are illegal without written authorisation from the system owner, and the course teaches the authorisation and scoping process alongside the tooling.

Requirements. A computer with 8 GB RAM or more and roughly 100 GB free disk space, plus a stable internet connection. Every tool used in this outline is free or has a free tier — there is no additional software cost.