Soc Operations & Blue Teaming

Program Brochure · 2026

SOC ANALYST LEVEL 1

Your first seat in the Security Operations Centre.

Beginner

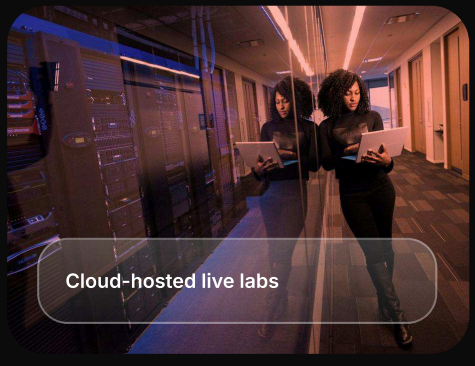
40 Hours

SAM-SOC-L1

Cybersecurity

Soc Operations & Blue Teaming

12 programs in this track



6

modules · hands-on labs · capstone project

Inside this brochure

Contents

Program overview 03
Who it's for 04
Learning outcomes 05
Program runway 06
Detailed curriculum 07
Tools & frameworks 09
Projects & capstone 10
Certification & method 11
Learning path 12
FAQs 13



AT A GLANCE

Level	**Beginner**
Duration	**40 Hours**
Modules	**6**
Certificate	**SAM-SOC-L1**

Program overview

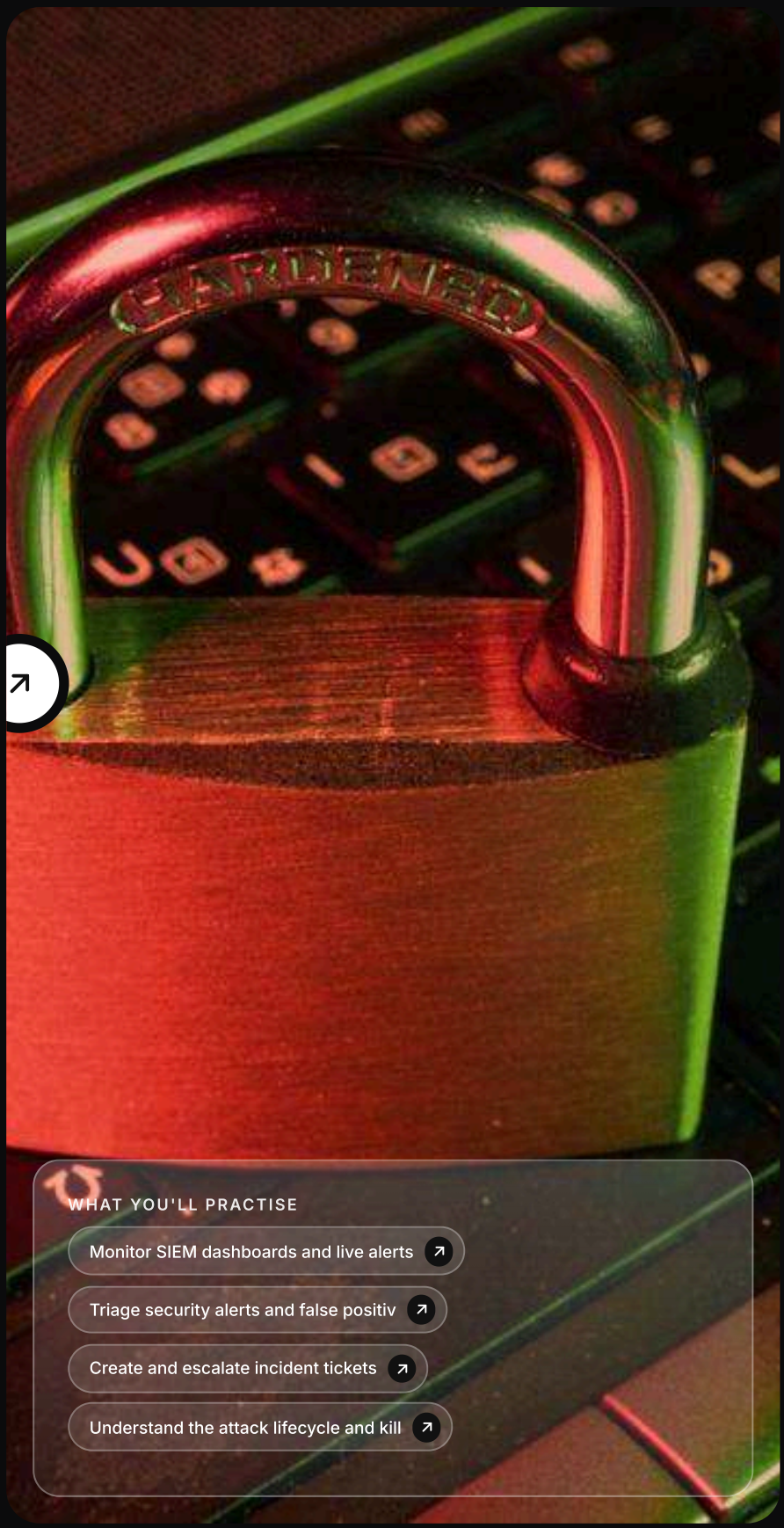
Your first seat in the Security Operations Centre.

Foundational SOC analyst training covering security monitoring basics, alert triage, log analysis, ticketing workflows and escalation procedures using industry SIEM platforms.

Every organization needs people who can watch security alerts and act on them quickly. This program builds the core skills of a Level 1 SOC analyst — monitoring, alert triage, log analysis, ticketing and escalation — using industry SIEM platforms in a realistic SOC lab.

DELIVERY

ILT · VILT · Self-Paced



LEVEL

Beginner

DURATION

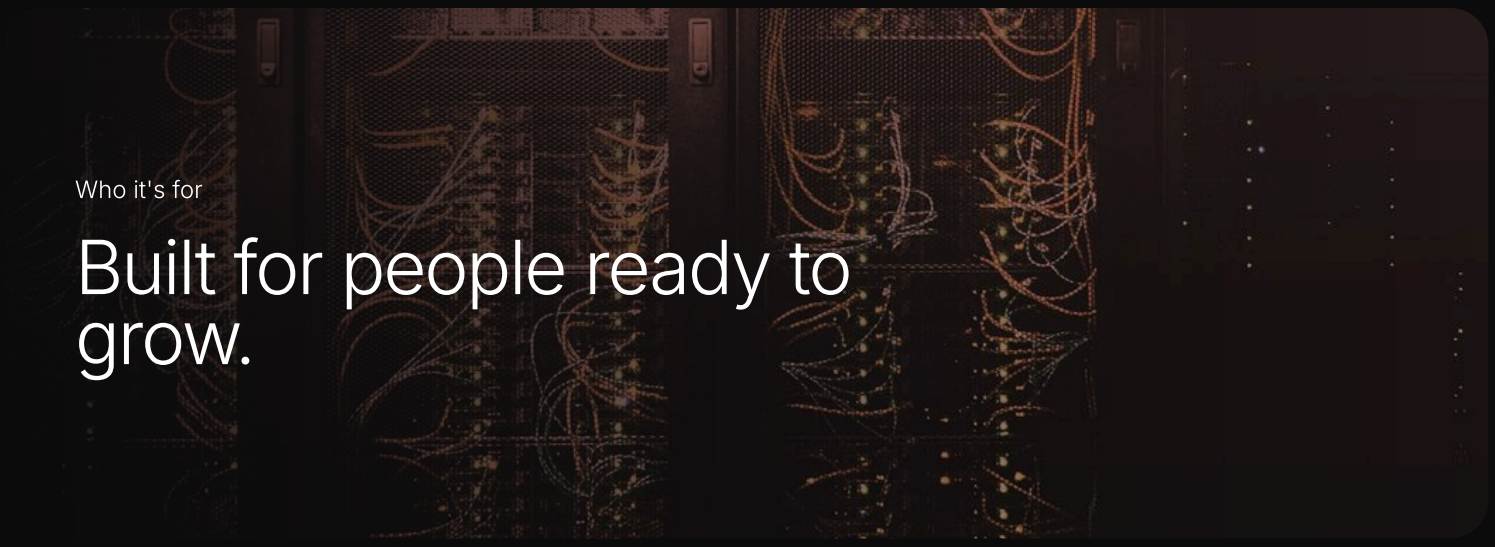
40 Hours

CERTIFICATION

SAM-SOC-L1

TRACK

Soc Operations & Blue Teaming



Who it's for

Built for people ready to grow.

01

Fresh graduates & career switchers

Start with SOC-L1 or Ethical Hacking Fundamentals

02

SOC & IT teams

Level up to SIEM, EDR, DFIR and threat hunting

03

Pen testers & red teamers

Web, network, API, mobile and red-team programs

04

Security leaders

GRC, ISO 27001, risk and CISO leadership

PREREQUISITES

Basic computer and internet knowledge	01
Curiosity about how attacks are detected	02
None — beginner friendly	03

ROLES THIS PREPARES YOU FOR

- SOC Analyst L1 ↗
- Security Monitoring Analyst ↗
- NOC/SOC Operator ↗
- IT Security Support ↗

Learning outcomes

What you'll be able to do.



01	Explain the role and workflow of a SOC
02	Monitor SIEM dashboards and prioritise alerts
03	Analyse common log sources for suspicious activity
04	Triage alerts and separate false positives
05	Document and escalate incidents correctly
06	Map alerts to the attack lifecycle

Program runway

Module by module.

6
modules · 40 hours

01	**Security & SOC Foundations** CIA triad and security basics, SOC roles and tiers, Common threat types	5 hrs
02	**Networking for Analysts** TCP/IP and common ports, DNS, HTTP and email flows, Firewalls and proxies	6 hrs
03	**Log Sources & Analysis** Windows event logs, Linux system logs, Firewall and proxy logs	7 hrs
04	**SIEM Fundamentals** SIEM architecture, Dashboards and searches, Basic search queries	8 hrs
05	**Alert Triage & Ticketing** Alert prioritisation, True vs false positives, Enrichment with threat intel	7 hrs
06	**Incident Handling Basics** Incident response lifecycle, Phishing investigation basics, Malware alert handling	7 hrs
★	**Capstone · Day in the SOC** Assessment, capstone review and certification	

The syllabus.

Modules 01–03

Module 01

Security & SOC Foundations

5 hours

Hands-on lab
Tour a simulated SOC and map its tools and roles.

TOPICS COVERED

- CIA triad and security basics
- SOC roles and tiers
- Common threat types
- Cyber kill chain overview
- Security policies and procedures

Module 02

Networking for Analysts

6 hours

Hands-on lab
Review packet captures to identify normal and suspicious traffic.

TOPICS COVERED

- TCP/IP and common ports
- DNS, HTTP and email flows
- Firewalls and proxies
- Reading packet captures
- Network indicators of attack

Module 03

Log Sources & Analysis

7 hours

Hands-on lab
Investigate failed-login patterns across Windows and Linux logs.

TOPICS COVERED

- Windows event logs
- Linux system logs
- Firewall and proxy logs
- Authentication logs
- Log normalisation basics

Linux

LEARN BY DOING

Every module ends in a guided hands-on lab — 6 labs across the programme.

Syllabus, continued.

Modules 04–06

Module 04

SIEM Fundamentals

8 hours

Hands-on lab
Build searches and a dashboard for authentication events in a SIEM.

TOPICS COVERED

- SIEM architecture
- Dashboards and searches
- Basic search queries
- Alert rules overview
- Use-case basics

Module 05

Alert Triage & Ticketing

7 hours

Hands-on lab
Triage a queue of simulated alerts and raise tickets.

TOPICS COVERED

- Alert prioritisation
- True vs false positives
- Enrichment with threat intel
- Ticketing workflows
- Escalation criteria

Module 06

Incident Handling Basics

7 hours

Hands-on lab
Handle a simulated phishing incident from alert to escalation.

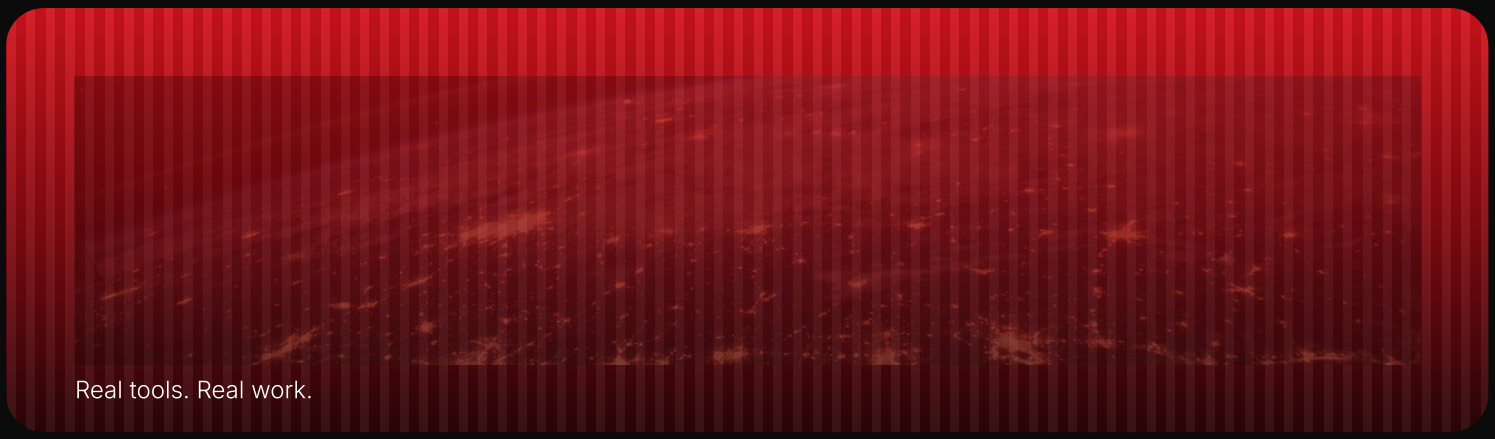
TOPICS COVERED

- Incident response lifecycle
- Phishing investigation basics
- Malware alert handling
- Containment hand-offs
- Shift reporting



CAPSTONE

Day in the SOC



Splunk
SIEM search, dashboards & alerting

Elastic
ELK / Elastic SIEM analytics

Wireshark
Packet capture & traffic analysis

VirusTotal
File, URL & IOC reputation

Linux
Server & CLI fundamentals

Frameworks & standards

- MITRE ATT&CK
- NIST CSF
- ISO 27001

FOCUS AREAS

Monitor SIEM dashboards and live alerts	01
Triage security alerts and false positives	02
Create and escalate incident tickets	03
Understand the attack lifecycle and kill chain	04



LAB ACCESS

24×7 cloud labs for the length of the program

01

SOC Alert Triage Playbook

Create a step-by-step triage playbook for the five most common alert types in the lab SOC.

02

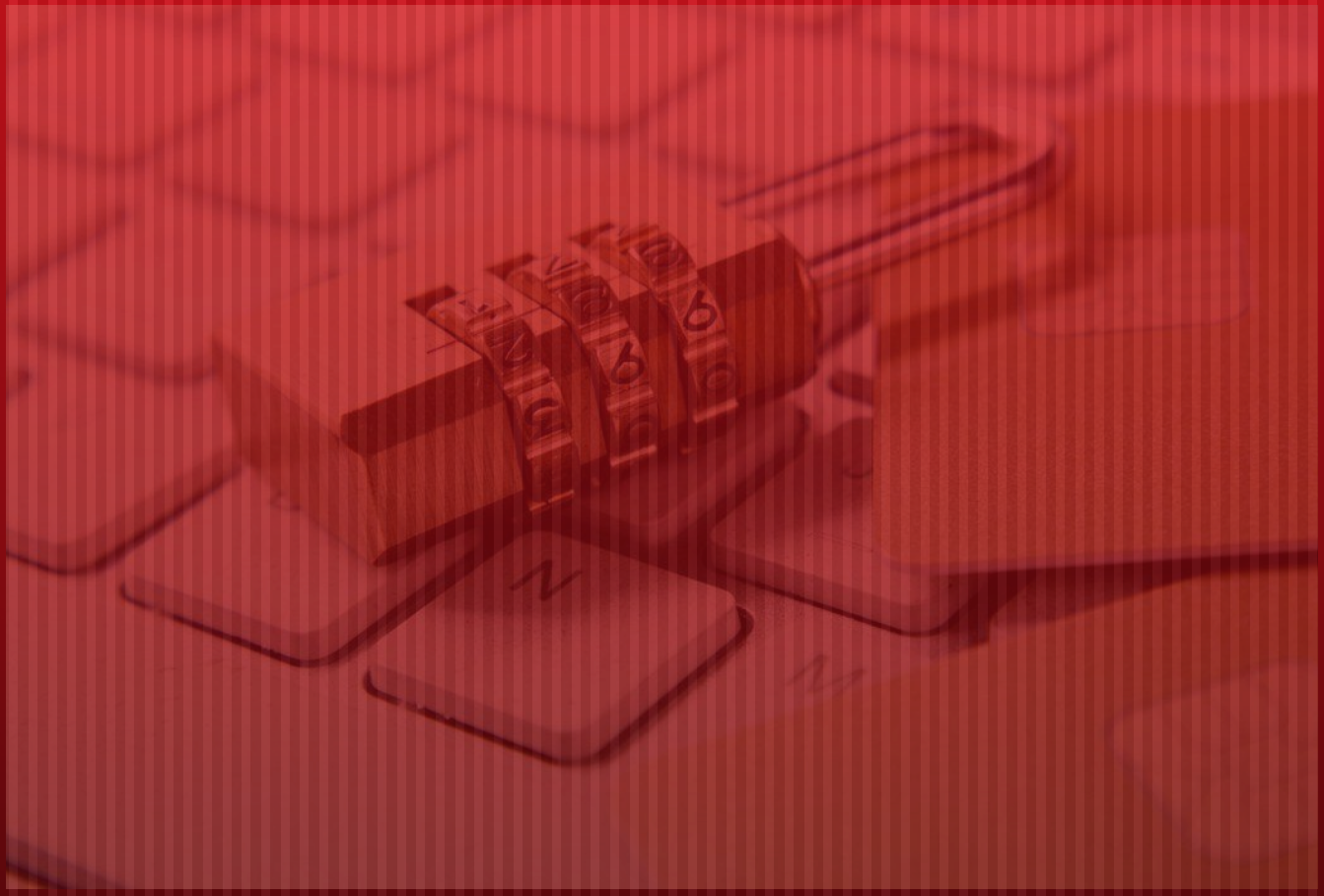
Authentication Monitoring Dashboard

Build a SIEM dashboard that tracks logins, failures and unusual access across lab systems.

03

Phishing Investigation Report

Investigate a simulated phishing campaign and write a clear incident summary for escalation.



Capstone project

Day in the SOC

Work a full simulated SOC shift: monitor dashboards, triage a live alert queue, investigate two incidents, escalate correctly and present a shift handover report to mentors.

Real-world scenario ↗ Mentor review ↗ Portfolio ready ↗

Certification

SAM-SOC-L1

Awarded on successful completion of the program assessments.

- MCQ assessments
- Practical lab evaluation
- Project & capstone review
- Final presentation



The SAM Learning Framework™

Scenario · Apply · Master · Mentor

Phase 01

Scenario

Real-world attack and use-case scenarios open every module.

Phase 02

Apply

Hands-on lab work, CTF challenges and live projects.

Phase 03

Master

Assessment, peer review and certification prep.

Phase 04

Mentor

Post-program career guidance and support.

DELIVERY MODELS

- Instructor-Led (ILT)
- Virtual Instructor-Led
- Self-Paced Online
- E-Learning Licensing
- Blended Learning
- Corporate Onsite
- Bootcamp Intensive

Learning path · Soc Operations & Blue Teaming

Where this program fits.

Beginner	Intermediate	Advanced	Expert
You are here	4 programs	3 programs	3 programs

Before this

A starting point — no prerequisite program needed.

Up next

SOC Analyst Level 2 (SOC-L2)	60 Hours
SIEM Operations & Analytics	48 Hours
EDR Operations & Endpoint Detection	32 Hours
XDR — Extended Detection & Response	40 Hours



CAREER ROLES

SOC Analyst L1 ↗ | Security Monitoring Analyst ↗ | NOC/SOC Operator ↗ | IT Security Support ↗

Questions, answered.

Q01

Do I need prior experience?

No prior security experience is needed — the program starts from the fundamentals. Mentors help you close any gaps in the first weeks.

Q02

How is the program delivered?

Sessions are instructor-led in a classroom, live virtual, or blended, with recordings and lab time between sessions. Corporate batches can be scheduled onsite or online.

Q03

Will I get a certificate?

Yes. After completing the assessments for SOC Analyst Level 1 (SOC-L1) — MCQs, practical lab evaluation and project work — you receive the program certificate listed in this brochure.

Q04

Are labs and tools included?

Yes. You work in cloud-hosted, isolated lab environments with industry tools, with lab access available throughout the program for practice.

Q05

Is there career support?

You get 90 days of post-program mentorship, resume and interview guidance, and access to the Samcommunity community. Placement outcomes depend on individual effort and are not guaranteed.

Let's talk

START
SOC ANALYST LEVEL 1.

academy@samcommunity.in

corporate@samcommunity.in

samcommunity.in

@samcommunity_

Learn practical skills. Grow with mentors.

Xylyn Samcommunity Private Limited · DPIIT-recognized startup · Surat, Gujarat, India