Soc Operations & Blue Teaming

Program Brochure · 2026

SECURITY MONITORING FUNDAMENTALS

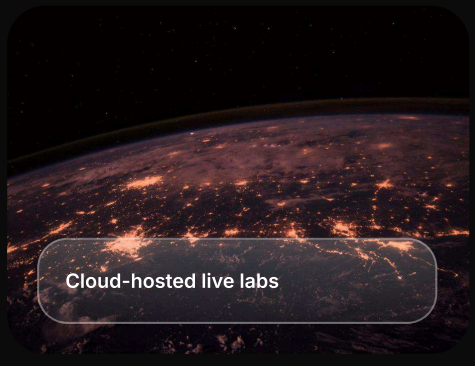
See every signal. Spot what matters.

Beginner ↗ | 25 Hours ↗ | SAM-SECMON ↗

Cybersecurity

Soc Operations & Blue Teaming

12 programs in this track



5

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

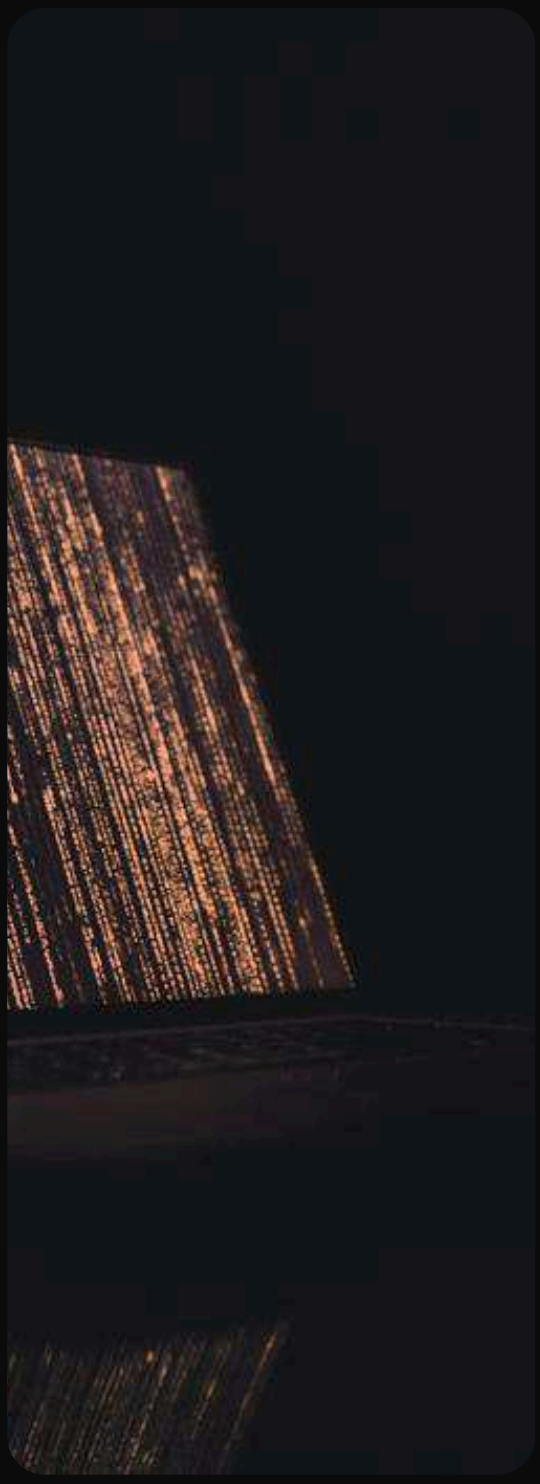
Tools & frameworks 09

Projects & capstone 10

Certification & method 11

Learning path 12

FAQs 13



AT A GLANCE

Level	**Beginner**
Duration	**25 Hours**
Modules	**5**
Certificate	**SAM-SECMON**

Program overview

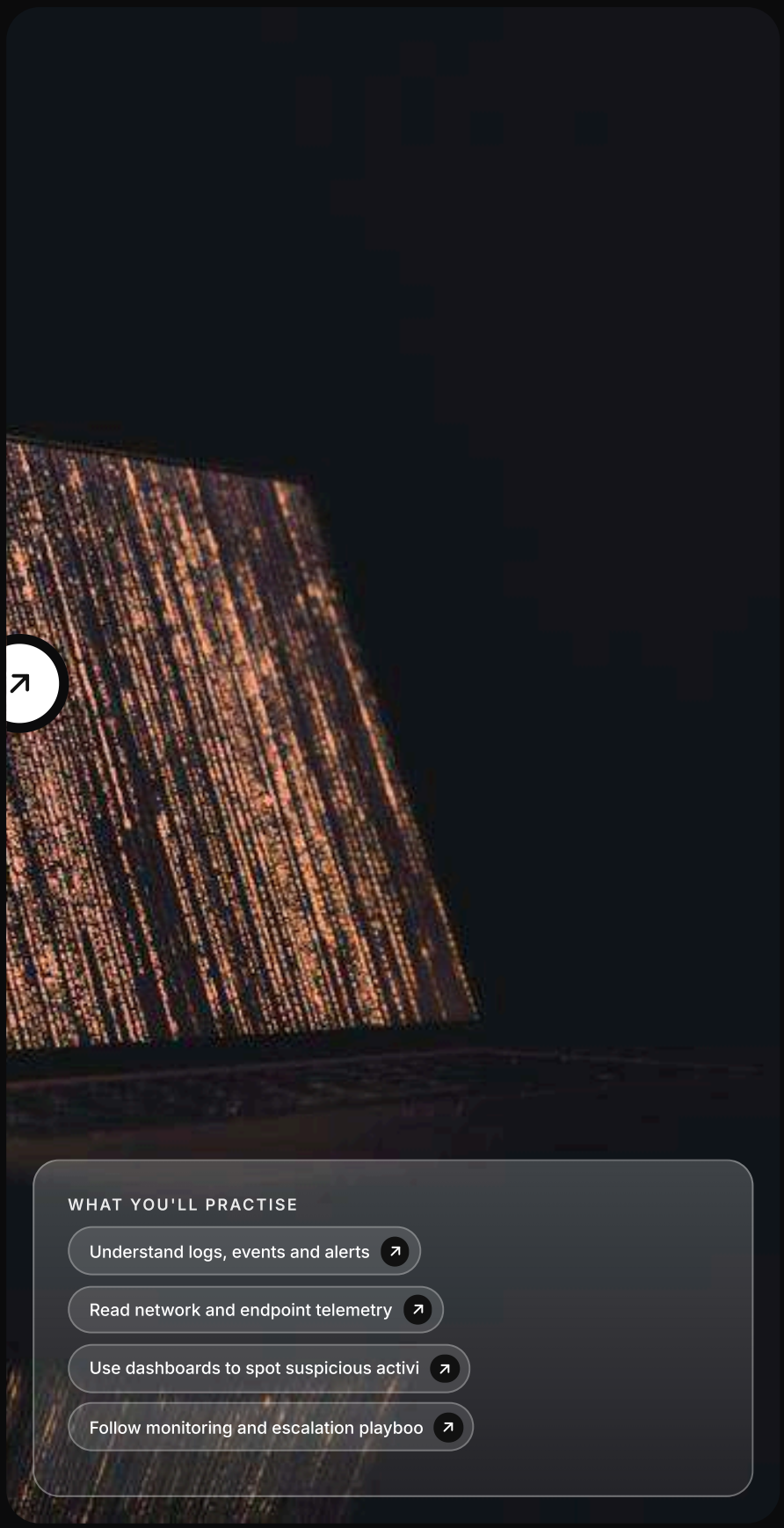
See every signal. Spot what matters.

An entry program on how organizations watch their networks, endpoints and logs — and how analysts turn raw events into actionable alerts.

Security monitoring is how organizations notice trouble early. This short program explains logs, events, alerts and dashboards, and how analysts turn raw telemetry into signals worth acting on — a practical starting point for SOC and IT roles.

DELIVERY

Instructor-led · Live virtual · Blended



LEVEL

Beginner

DURATION

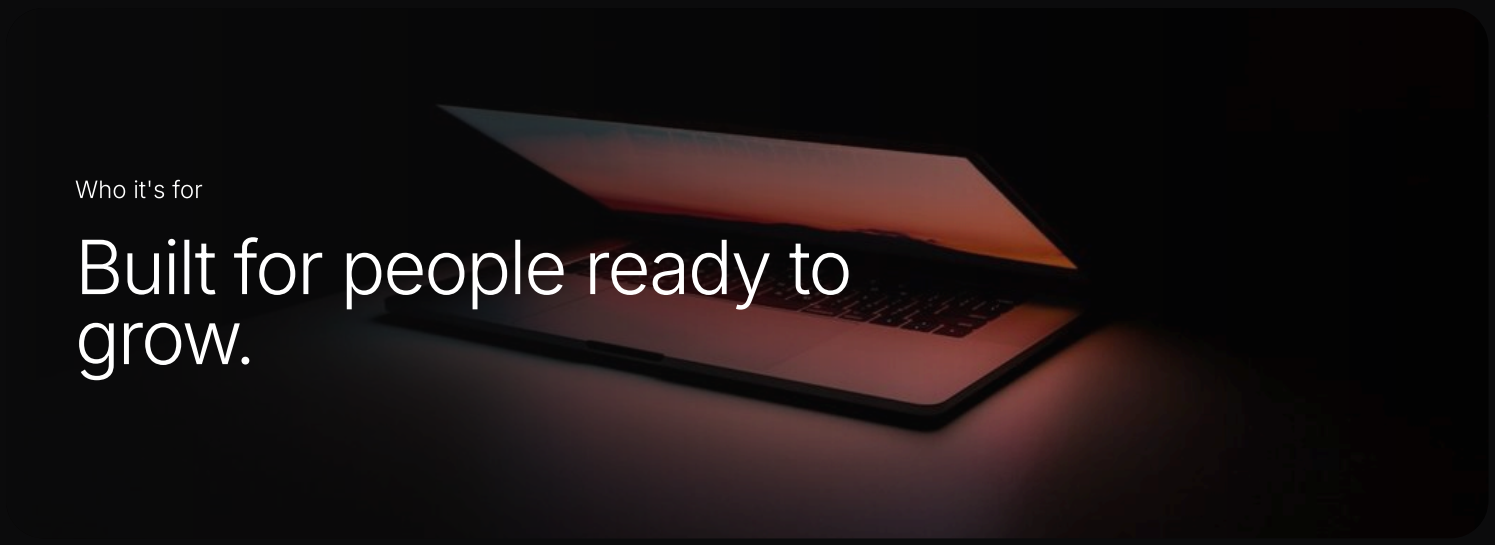
25 Hours

CERTIFICATION

SAM-SECMON

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 knowledge	01
Familiarity with Windows or Linux	02
None — beginner friendly	03

ROLES THIS PREPARES YOU FOR

- Security Monitoring Analyst ↗
- IT Support with security duties ↗
- Junior SOC Analyst ↗
- NOC Engineer ↗

Learning outcomes

What you'll be able to do.



01	Describe how security monitoring works end to end
02	Identify key log and telemetry sources
03	Read dashboards to spot unusual activity
04	Distinguish events, alerts and incidents
05	Follow a monitoring and escalation playbook
06	Write a clear monitoring summary

Program runway

Module by module.

5
modules · 25 hours

01	**Monitoring Concepts** Why monitor, Events, alerts and incidents, Visibility and coverage	4 hrs
02	**Telemetry Sources** Network telemetry, Endpoint telemetry, Identity and access logs	6 hrs
03	**Dashboards & Baselines** Building baselines, Reading dashboards, Thresholds and anomalies	6 hrs
04	**Alert Handling** Alert quality, Prioritisation, Enrichment basics	5 hrs
05	**Reporting & Next Steps** Shift summaries, Metrics that matter, Continuous improvement	4 hrs
★	**Capstone · Monitoring Readiness Review** Assessment, capstone review and certification	

The syllabus.

Modules 01–03

Module 01

Monitoring Concepts

4 hours

Hands-on lab
Classify sample records as events, alerts or incidents.

TOPICS COVERED

- Why monitor
- Events, alerts and incidents
- Visibility and coverage
- Monitoring roles

Module 02

Telemetry Sources

6 hours

Hands-on lab
Collect and compare logs from lab endpoints and servers.

TOPICS COVERED

- Network telemetry
- Endpoint telemetry
- Identity and access logs
- Cloud activity logs

Module 03

Dashboards & Baselines

6 hours

Hands-on lab
Build a baseline dashboard and spot deviations.

TOPICS COVERED

- Building baselines
- Reading dashboards
- Thresholds and anomalies
- Visualising trends



LEARN BY DOING

Every module ends in a guided hands-on lab — 5 labs across the programme.

Syllabus, continued.

Modules 04–05

Module 04

Alert Handling

5 hours

Hands-on lab
Prioritise a set of mixed alerts using a playbook.

TOPICS COVERED

- Alert quality
- Prioritisation
- Enrichment basics
- Escalation paths

Module 05

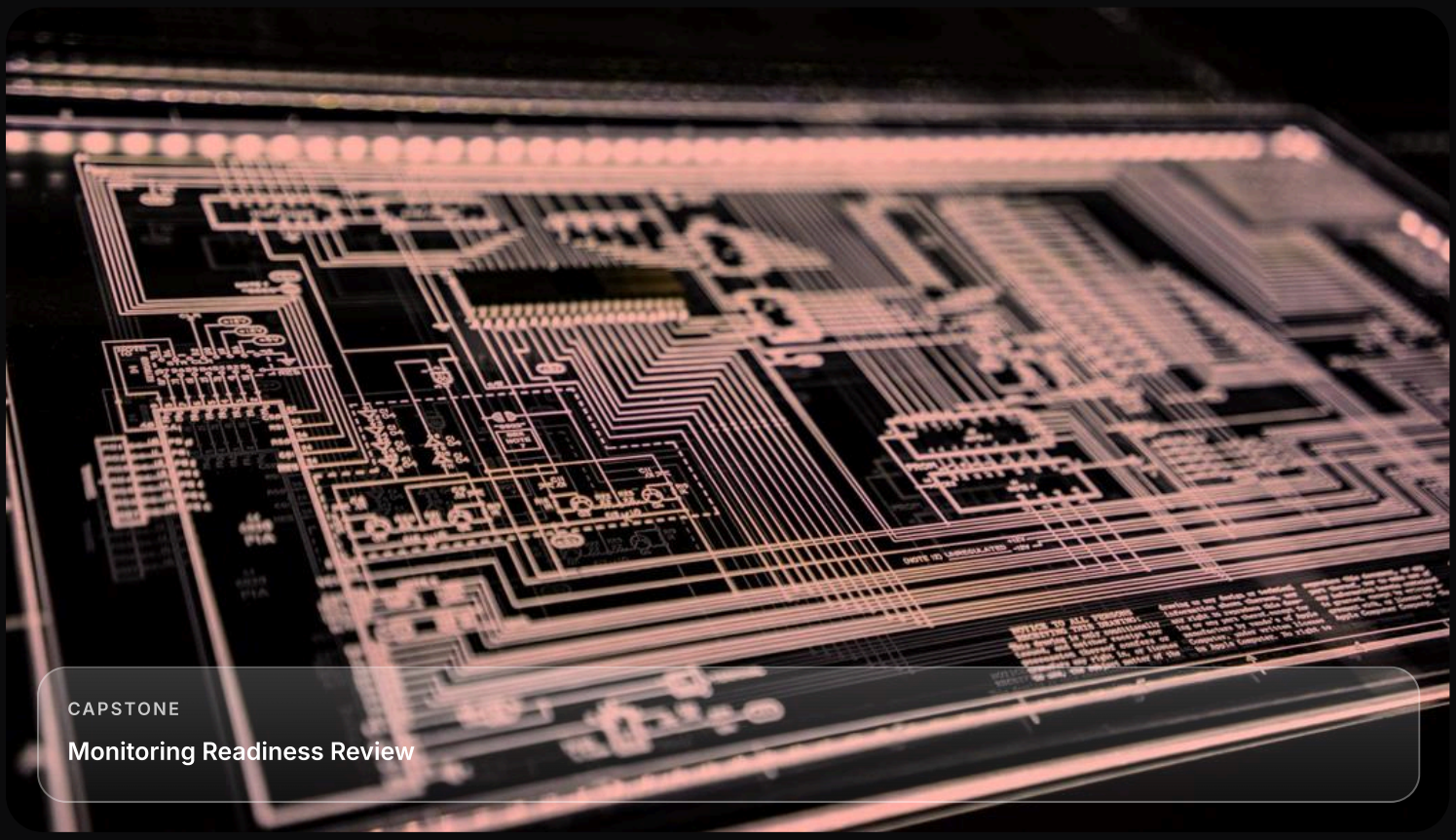
Reporting & Next Steps

4 hours

Hands-on lab
Write a monitoring summary for a simulated week.

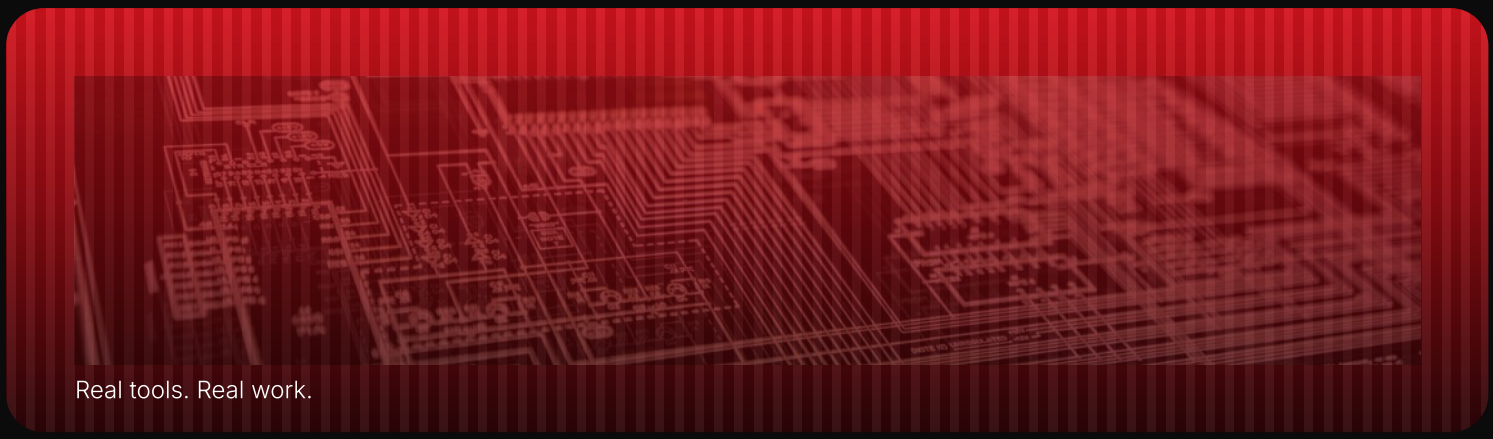
TOPICS COVERED

- Shift summaries
- Metrics that matter
- Continuous improvement
- Path to SOC roles



CAPSTONE

Monitoring Readiness Review



splunk>

Splunk
SIEM search, dashboards & alerting

Elastic
ELK / Elastic SIEM analytics

Wireshark
Packet capture & traffic analysis

Linux
Server & CLI fundamentals

Frameworks & standards

- MITRE ATT&CK ↗
- NIST CSF ↗
- ISO 27001 ↗

FOCUS AREAS

Understand logs, events and alerts	01
Read network and endpoint telemetry	02
Use dashboards to spot suspicious activity	03
Follow monitoring and escalation playbooks	04



LAB ACCESS

24×7 cloud labs for the length of the program

01

Telemetry Coverage Map

Map which lab systems send which logs and identify visibility gaps.

02

Baseline Dashboard

Create a dashboard showing normal activity and highlight anomalies.

03

Weekly Monitoring Report

Summarise a week of simulated activity for a security manager.



Capstone project

Monitoring Readiness Review

Assess a small lab organization's monitoring coverage, build dashboards and alerts for key risks, and present recommendations to mentors.

Real-world scenario | Mentor review | Portfolio ready

Certification

SAM-SECMON

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.

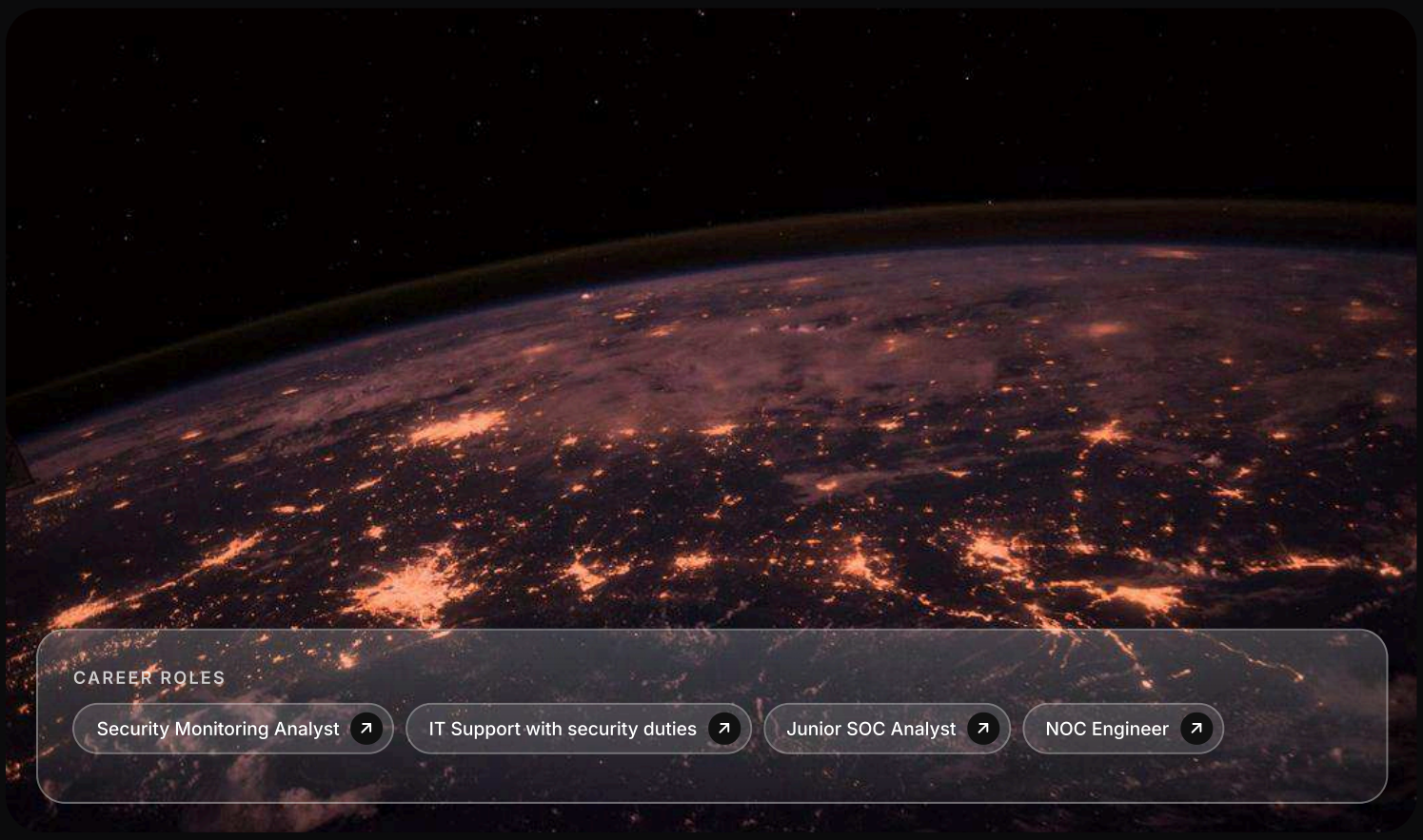
Beginner	Intermediate	Advanced	Expert
You are here	4 programs	3 programs	3 programs

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

- Security Monitoring Analyst
- IT Support with security duties
- Junior SOC Analyst
- NOC Engineer

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 Security Monitoring Fundamentals — 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 SECURITY MONITORING FUNDAMENTALS.

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