

LEADERSHIP & WORKFORCE DEVELOPMENT · FOUNDATION

Fresher Bootcamp — Cybersecurity Analyst

Your launchpad into cybersecurity.

Contents

Why this program 03

Who it's for 04

Learning outcomes 05

Program runway 06

Detailed curriculum 07

Frameworks & tools 10

Projects & capstone 11

Certification & method 12

Learning path 13

FAQs 14

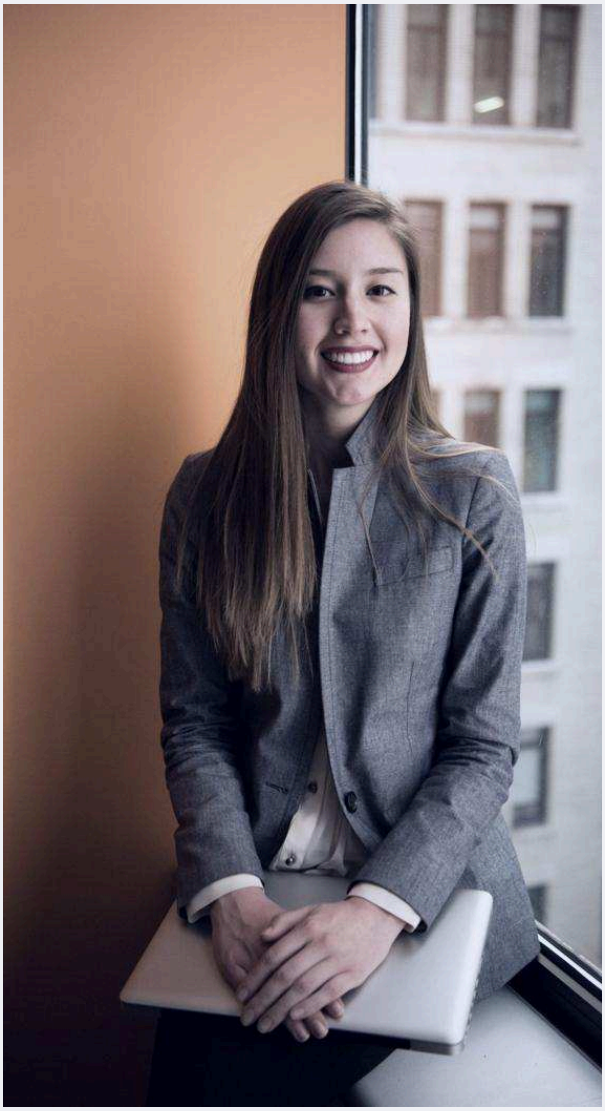


LEVEL	Foundation
DURATION	160 Hours
MODULES	8
CERTIFICATE	SAM-FBCS

Why this program

An intensive program that prepares freshers for SOC and security analyst roles.

Security operations teams need analysts who can read logs, triage alerts and investigate incidents from day one. Graduates often know theory but lack hands-on practice. This intensive bootcamp builds networking, Linux and Windows security foundations, then trains freshers in SIEM monitoring with Splunk, packet analysis with Wireshark, threat intelligence and incident response inside a realistic SOC lab environment.



160 hours of compact, practical sessions

8 focused modules, built around real work

3 projects plus a capstone presentation



Who this program is for



01

New managers

Manager bootcamp and communication skills

02

Delivery teams

PMP, Agile & Scrum, ITIL 4

03

Technology leaders

Team leadership, strategic IT, CTO program

04

HR & L&D teams

Fresher, lateral and reskilling programs

PREREQUISITES

- Graduate in IT, computer science or related field
- Basic understanding of computers and networks
- Laptop capable of running virtual machines

DESIGNED FOR

- SOC Analyst (L1)
- Junior Security Analyst
- Security Monitoring Engineer
- Incident Response Associate
- Vulnerability Management Associate

What you'll be able to do.

01 Explain networking, protocols and core security concepts clearly

02 Analyse network traffic and detect anomalies using Wireshark

03 Monitor, search and correlate security events in Splunk

04 Triage alerts and investigate incidents using structured playbooks

05 Map attacker techniques to the MITRE ATT&CK framework

06 Write clear incident reports and escalation notes

How the program works

Networking Fundamentals

OSI and TCP/IP models, IP addressing and subnetting, DNS, DHCP, HTTP and TLS, Routing and switching basics.

Linux and Windows for Security

Linux commands and permissions, Linux logs and services, Windows architecture and Active Directory, Windows Event Logs.

Security Concepts and Threats

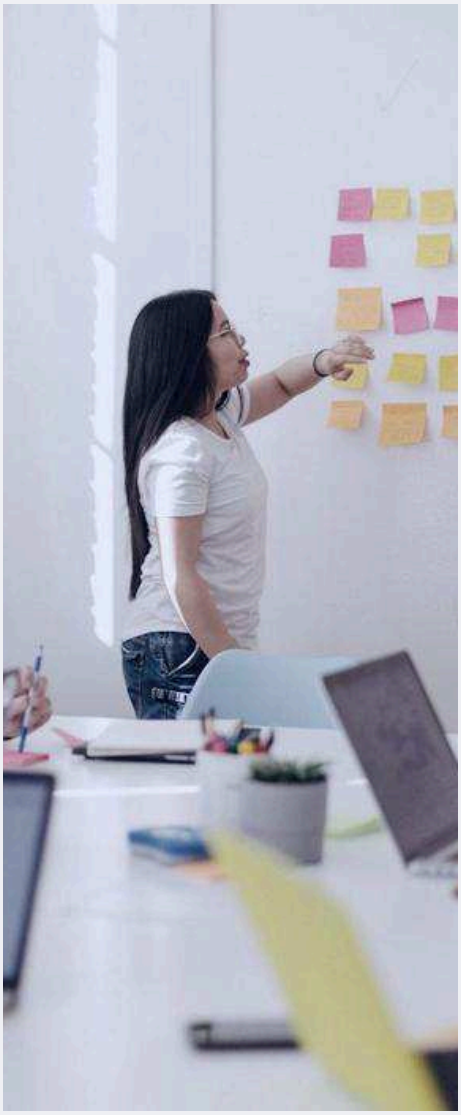
CIA triad and security controls, Malware types and phishing, Common web and network attacks, Cyber kill chain.

Network Traffic Analysis

Wireshark filters and navigation, Analysing TCP sessions, Detecting scans and beaconing, Extracting artefacts from PCAPs.

01 · Networking Fundamentals	20 hrs
02 · Linux and Windows for Security	20 hrs
03 · Security Concepts and Threats	16 hrs
04 · Network Traffic Analysis	16 hrs
05 · SIEM and Log Analysis with Splunk	28 hrs
06 · Threat Intelligence and Vulnerabilities	16 hrs
07 · Incident Response and Forensics	24 hrs
08 · SOC Simulation and Interview Prep	20 hrs

★ Capstone · End-to-End SOC Incident Investigation



The curriculum

MODULES 01–03

01 Networking Fundamentals

20 HOURS

Practical: Subnet a small office network and trace common protocols in captures.

- OSI and TCP/IP models
- IP addressing and subnetting
- DNS, DHCP, HTTP and TLS
- Routing and switching basics
- Firewalls, proxies and VPNs

02 Linux and Windows for Security

20 HOURS

Practical: Investigate suspicious logins using Linux auth logs and Windows Event Viewer.

Kali Linux Linux

- Linux commands and permissions
- Linux logs and services
- Windows architecture and Active Directory
- Windows Event Logs
- PowerShell basics
- Kali Linux overview

03 Security Concepts and Threats

16 HOURS

Practical: Map a phishing attack scenario to kill chain stages and ATT&CK techniques.

- CIA triad and security controls
- Malware types and phishing
- Common web and network attacks
- Cyber kill chain
- MITRE ATT&CK framework
- Indian CERT-In reporting overview



Curriculum, continued

MODULES 04–06

04 Network Traffic Analysis

16 HOURS

Practical: Analyse a PCAP to identify scanning, malware download and command-and-control traffic.

Wireshark

- Wireshark filters and navigation
- Analysing TCP sessions
- Detecting scans and beaconing
- Extracting artefacts from PCAPs
- IDS concepts with Suricata

05 SIEM and Log Analysis with Splunk

28 HOURS

Practical: Build Splunk searches and an alert to detect brute-force login attempts.

Splunk

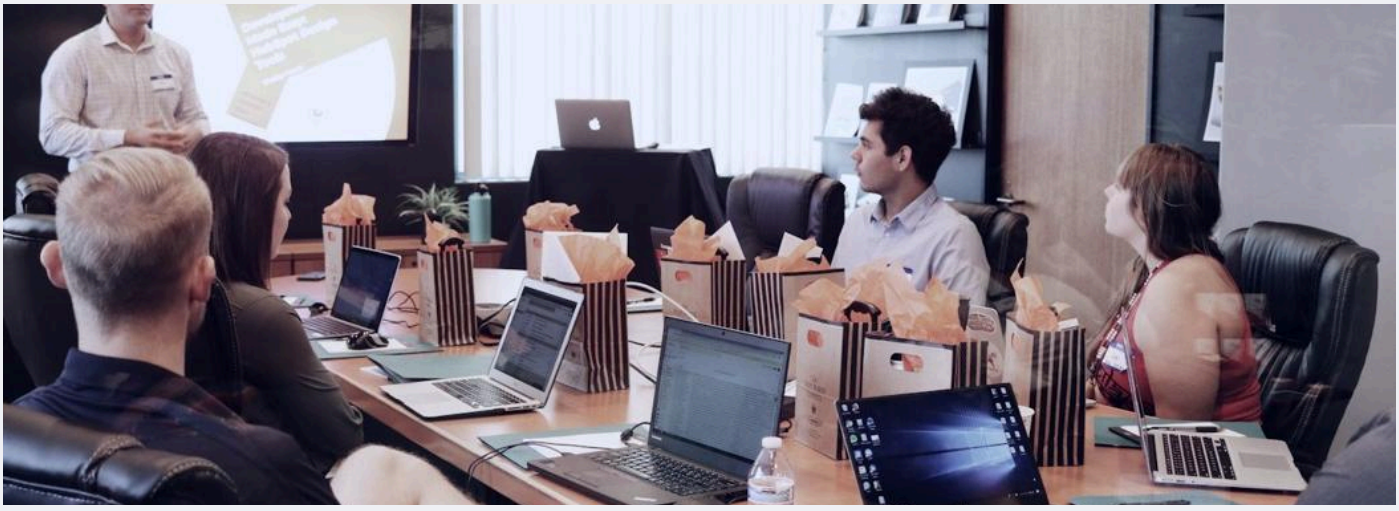
- SOC structure and analyst tiers
- Log sources and ingestion
- Splunk SPL searching
- Dashboards and alerts
- Correlation and use cases
- Alert triage workflow

06 Threat Intelligence and Vulnerabilities

16 HOURS

Practical: Enrich alert IOCs using open threat intelligence sources and summarise findings.

- IOCs and threat feeds
- OSINT for analysts
- Vulnerability scanning basics
- CVSS scoring and prioritisation
- Patch management workflow



Curriculum, continued

MODULES 07–08

07 Incident Response and Forensics

24 HOURS

Practical: Respond to a simulated ransomware alert following a playbook end to end.

- NIST incident response life cycle
- Playbooks and runbooks
- Endpoint investigation basics
- Memory and disk forensics introduction
- Containment and eradication
- Incident documentation

08 SOC Simulation and Interview Prep

20 HOURS

Practical: Work a simulated SOC shift, triaging alerts and escalating confirmed incidents.

- Shift-based SOC simulation
- Ticketing and escalation
- Report writing practice
- Resume and LinkedIn for security
- Mock technical interviews



What you'll focus on.

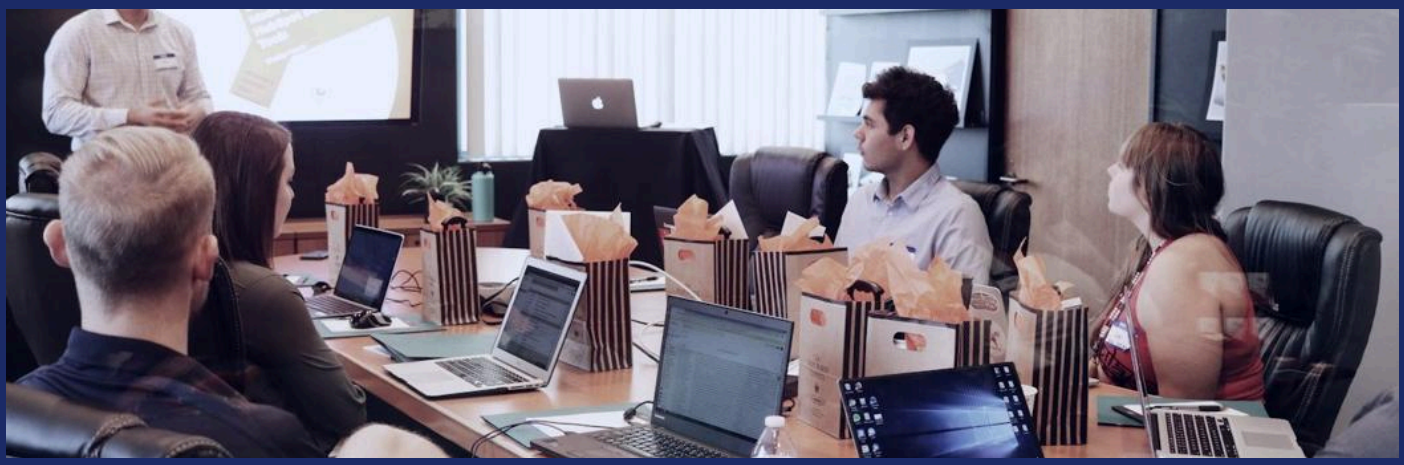
MITRE ATT&CK 01

CERT-In 02

Networking Fundamentals 03

Linux and Windows for Security 04

Security Concepts and Threats 05



Splunk
SIEM search, dashboards & alerting

Wireshark
Packet capture & traffic analysis

Kali Linux
Security testing distribution

Linux
Server & CLI fundamentals

Projects & capstone

01

Traffic Analysis Report

Investigate a packet capture in Wireshark and document the malicious activity found, key indicators and recommended detections.

02

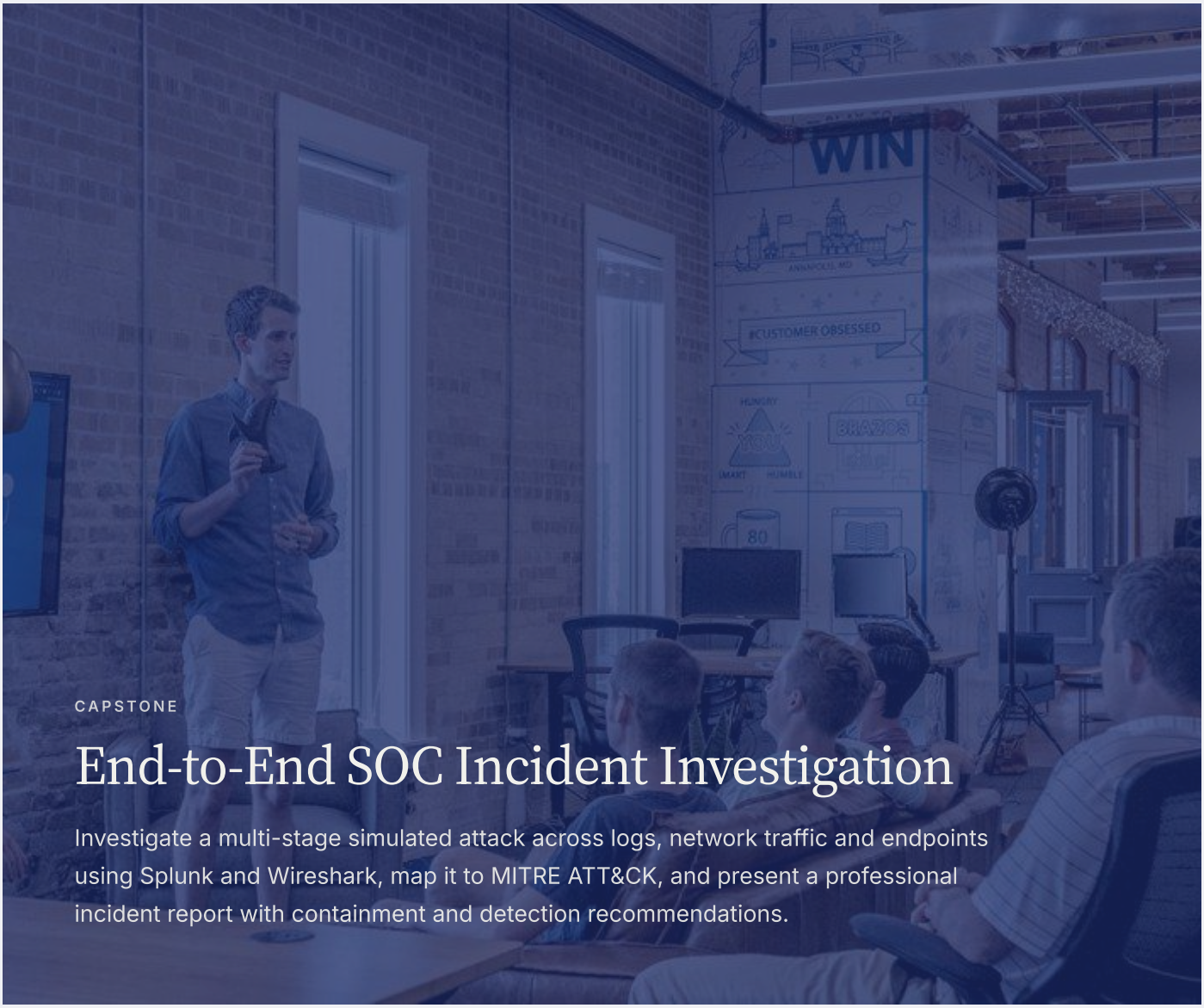
Splunk Detection Dashboard

Build Splunk searches, alerts and a dashboard to detect brute force, malware and suspicious admin activity.

03

Incident Response Playbook

Write a step-by-step playbook for phishing incidents covering triage, containment, eradication, communication and lessons learned.



CAPSTONE

End-to-End SOC Incident Investigation

Investigate a multi-stage simulated attack across logs, network traffic and endpoints using Splunk and Wireshark, map it to MITRE ATT&CK, and present a professional incident report with containment and detection recommendations.

CERTIFICATION

SAM-FBCS

Awarded on successful completion of the program assessments.

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

HOW YOU LEARN · THE SAM LEARNING FRAMEWORK™

01 Scenario

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

02 Apply

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

03 Master

Assessment, peer review and certification prep.

04 Mentor

Post-program career guidance and support.



Delivery: Instructor-Led (ILT) · Virtual Instructor-Led · Self-Paced Online · E-Learning Licensing · Blended Learning · Corporate Onsite

Where this program fits

Foundation	Intermediate	Advanced	Expert	Executive
You are here	4 programs	6 programs	2 programs	1 programs

BEFORE THIS

A starting point — no prerequisite program needed.

UP NEXT

Project Management for IT (PMP Prep)	56 Hours
Agile & Scrum Master Certification	32 Hours
ITIL 4 Foundation	32 Hours
Lateral Hire Upskilling Program	80 Hours



Questions, answered

Do I need prior experience to join?

No prior security experience is needed. The bootcamp is designed for freshers and starts with networking and operating system fundamentals before moving into SOC tools, investigations and incident response.

How is the program delivered and scheduled?

Delivery is instructor-led, either live virtual or blended with in-person sessions. Batch timings, weekday or weekend options and corporate cohort schedules are confirmed at enrolment, with session materials provided for revision.

What certification will I receive?

Learners who attend the sessions and pass the required assessments receive the Samcommunity Academy SAM-FBCS certificate of completion. It recognises the skills demonstrated in the program and is not a third-party vendor credential.

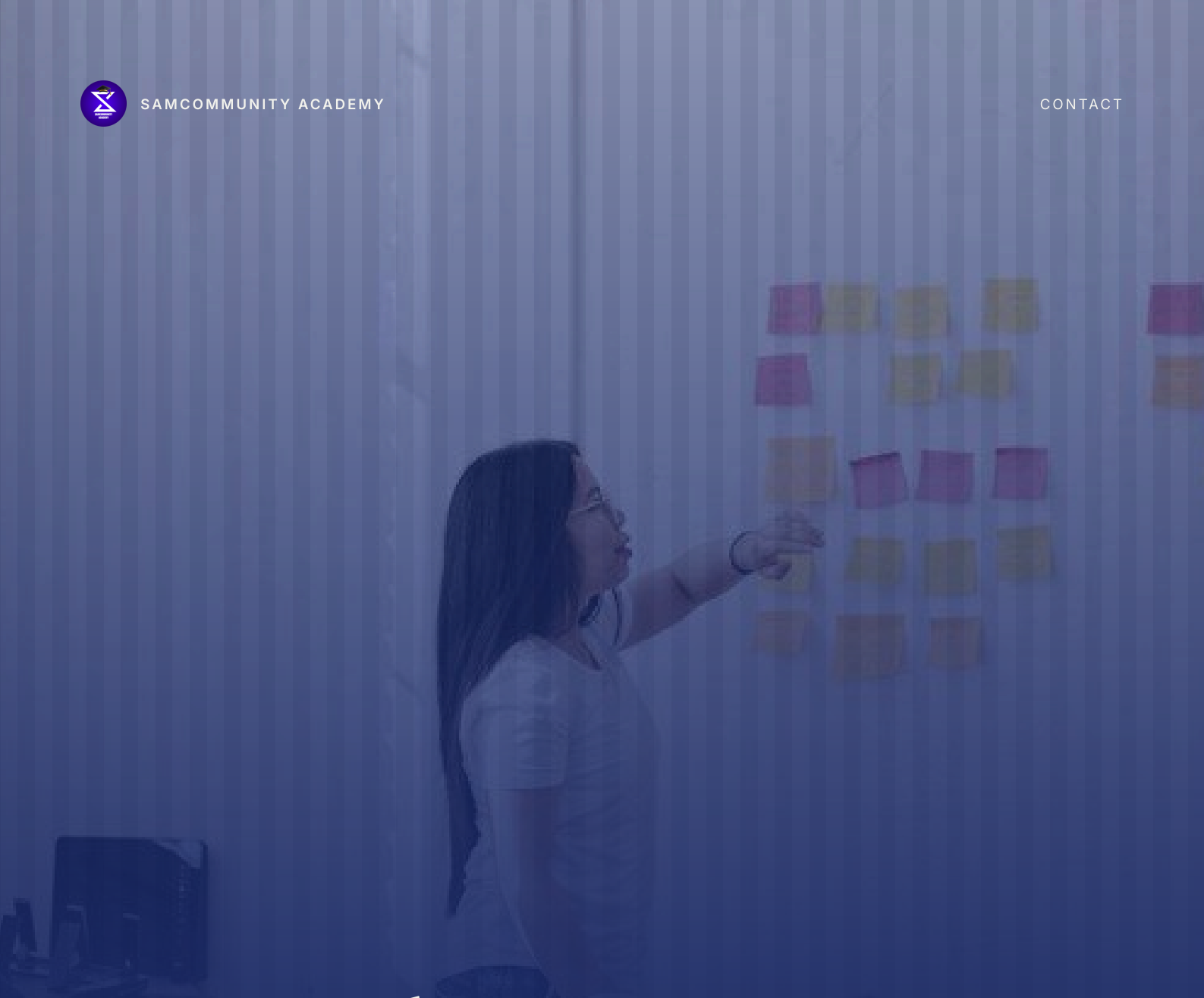
Will I get access to labs, tools and materials?

Yes. Learners work in a SOC lab with Splunk, Wireshark, Kali Linux and Linux and Windows virtual machines. All exercises run in isolated lab environments; a laptop that supports virtualisation is recommended.

Is career support included?

Learners receive guidance on applying the skills at work, including mentor discussions and, where relevant, resume or portfolio feedback. Samcommunity Academy does not guarantee jobs, promotions or salaries; outcomes depend on individual effort.





Begin with Fresher Bootcamp — Cybersecurity Analyst.

INDIVIDUALS

academy@samcommunity.in

CORPORATE & INSTITUTIONS

corporate@samcommunity.in