



EDUBLENDS

Fuel Your Future.

Fuel your **Future**

Dive into Edublends Academy's world of opportunities with industry internships, specialized training, and globally recognized certifications



Track 2: Network Security Engineering

Basic to Advanced · 270 Hours Total

At EduBlends, we don't just train—we create future industry leaders!

Program Summary

Design, defend and monitor secure network architectures — from foundational monitoring to specialist SOC, cloud and threat intelligence roles.



Program Duration

270 hours across 3 levels
(approx. 20 weeks)



Weekly effort

12-15 hours a week



Learning Mode: Online and Offline
Classes, including Pre-Recorded
Videos, Live Sessions, and Interactive
Q&A Sessions.



Cyber Range & Cloud Lab access
with isolated attack and defence
environments



**Industry-Sponsored Internship
Facilitation**



Certificate Upon successful
completion of each level, participants
will be awarded a verified digital
certificate by EduBlends and Industry

A Progressive Learning Pathway Aligned to Your Graduation

At EduBlends Academy, we provide a structured learning pathway that allows students to build cybersecurity expertise across their graduation journey, with each level mapped to a semester window and a defined exit role.

1. **Basic Level (Sem 3–4) — Cybersecurity Technician:** Foundational monitoring and network defence. Exit role: Junior SOC Analyst.
2. **Intermediate Level (Sem 5) — Network Security Engineer:** Secure architecture, SIEM and security analytics. Exit role: Network Security Engineer.
3. **Advanced Level (Sem 7) — Security Specializations:** Elective specialisation in SOC, cloud security or threat intelligence. Exit role: SOC Analyst · Cloud Security Engineer · Threat Intelligence Analyst.

By following this structured pathway, students complete the full track within their graduation period, emerging as industry-ready professionals with a portfolio of evidenced, lab-based security work.

Track 2 – Network Security Engineering

Basic → Advanced · 270 hours total · 30 practical lab sessions and a panel-assessed capstone

Program Levels

Level	Title	Semester	Hours	Focus
Basic	Cybersecurity Technician	Sem 3–4	90 hrs	Foundational monitoring and network defence
Intermediate	Network Security Engineer	Sem 5	90 hrs	Secure architecture, SIEM and security analytics
Advanced	Security Specializations	Sem 7	90 hrs	Elective specialisation in SOC, cloud security or threat intelligence

Target Roles

Level	Semester	Role
Basic	Sem 3–4	Junior SOC Analyst — foundational monitoring and network defence tasks in a supervised environment
Intermediate	Sem 5	Network Security Engineer — designing, implementing, and maintaining secure network architectures
Advanced	Sem 7	SOC Analyst · Cloud Security Engineer · Threat Intelligence Analyst

Certification Alignment

Level	Certifications
Basic — Cybersecurity Technician	IBM Cybersecurity Analyst Professional Certificate · Microsoft SC-200
Intermediate — Network Security Engineer	AWS Certified Security – Specialty · Google Professional Cloud Security Engineer · IBM Cybersecurity Analyst Professional Certificate
Advanced — Security Specializations	Microsoft SC-200 · Google Professional Cloud Security Engineer

Vendor certification examinations are sat separately and are not included in programme fees. Preparation coverage is indicative and does not guarantee an examination pass.

Top Recruiters

IBM · Microsoft Azure · Google · AWS

Recruiter names indicate the employers and sectors our graduates target; they do not constitute a placement guarantee or a formal hiring partnership.

Entry Requirements

The Basic level is open entry; no prior programming or security experience is assumed. The Intermediate level requires completion of the Basic level or equivalent networking and Linux competence. The Advanced level requires completion of the Intermediate level or demonstrable hands-on security experience.

Program Frameworks – Basic Level: Cybersecurity Technician

Sem 3–4 • 90 hours • Foundational monitoring and network defence • 10 practical lab sessions

M1 | Networking Foundations for Security 20 hrs

Module / Topic

- OSI and TCP/IP models, routing and switching, addressing, common protocols and their weaknesses

Practical Lab Sessions

Lab 1: Build a routed lab topology and verify connectivity end to end.

Lab 2: Map protocol weaknesses across the topology and record mitigations

M2 | Packet Capture & Analysis with Wireshark 20 hrs

Module / Topic

- Capture and display filters, protocol decoding, stream reassembly, identifying scans and exfiltration

Practical Lab Sessions

Lab 3: Capture and decode traffic across three protocols; extract a transferred file.

Lab 4: Identify scanning and beaconing behaviour in a provided capture

M3 | Host & Network Enumeration with Nmap 16 hrs

Module / Topic

- Host discovery, port states, service and OS fingerprinting, timing and evasion, scripting engine basics

Practical Lab Sessions

Lab 5: Enumerate a lab subnet and produce a full service inventory.

Lab 6: Use the Nmap scripting engine to identify weak service configurations

M4 | Vulnerability Assessment with OpenVAS 16 hrs

Module / Topic

- Scan policy design, credentialed scanning, CVSS interpretation, false positive validation, reporting

Practical Lab Sessions

Lab 7: Run a credentialed OpenVAS scan and validate the top findings manually.

Lab 8: Produce a remediation report ranked by risk

M5 | Digital Evidence Basics with Autopsy 18 hrs

Module / Topic

- Filesystem structures, artefact recovery, timeline analysis, keyword search, documentation standards

Practical Lab Sessions

Lab 9: Examine a disk image in Autopsy and recover deleted artefacts.

Lab 10: Build an incident timeline and write an evidence log

Program Frameworks – Intermediate Level: Network Security Engineer

Sem 5 • 90 hours • Secure architecture, SIEM and security analytics • 10 practical lab sessions

M1 | Secure Network Architecture Design 20 hrs

Module / Topic

- Defence in depth, segmentation and micro-segmentation, DMZ design, secure remote access, zero trust principles

Practical Lab Sessions

Lab 1: Design a segmented enterprise architecture with documented trust zones.

Lab 2: Implement and test access controls between the zones

M2 | Offensive Testing with Kali & Metasploit 18 hrs

Module / Topic

- Testing methodology, service exploitation, privilege escalation, validating defensive controls

Practical Lab Sessions

Lab 3: Exploit a lab host and escalate privileges; record every control bypassed.

Lab 4: Re-test after hardening and quantify the improvement

M3 | SIEM Deployment & Detection Engineering 20 hrs

Module / Topic

- Log sources and normalisation, correlation rules, detection engineering, dashboards, alert tuning

Practical Lab Sessions

Lab 5: Onboard three log sources into a SIEM and normalise the fields.

Lab 6: Write correlation rules for lateral movement and validate them against test traffic

M4 | Python for Security Analytics 18 hrs

Module / Topic

- Parsing logs at scale, enrichment with threat data, automation of triage tasks, reporting scripts

Practical Lab Sessions

Lab 7: Write a Python parser that extracts and enriches indicators from raw logs.

Lab 8: Automate a repetitive triage task and measure the time saved

M5 | Incident Response Operations 14 hrs

Module / Topic

- IR lifecycle, containment strategies, eradication and recovery, playbooks, post-incident review

Practical Lab Sessions

Lab 9: Execute a containment playbook against a simulated intrusion.

Lab 10: Run a post-incident review and produce lessons-learned actions

Program Frameworks – Advanced Level: Security Specializations

Sem 7 · 90 hours · Elective specialisation in SOC, cloud security or threat intelligence · 10 practical lab sessions

M1 | Specialisation A — SOC Analyst: Splunk & ELK 20 hrs

Module / Topic

- Search language, data models, detection content, dashboards and reporting, real-time threat detection

Practical Lab Sessions

Lab 1: Build detection content and dashboards in Splunk against live log feeds.

Lab 2: Replicate the detections in the ELK stack and compare the two approaches

M2 | Specialisation B — Cloud Security: AWS, Azure & GCP 20 hrs

Module / Topic

- Identity and access management, workload isolation, native detection services, multi-cloud posture management

Practical Lab Sessions

Lab 3: Configure least-privilege IAM and encryption across two cloud providers.

Lab 4: Enable native threat detection and review the findings generated

M3 | Specialisation C — Threat Intelligence: OSINT & Malware Analysis 20 hrs

Module / Topic

- Intelligence lifecycle, OSINT collection, adversary profiling, static and dynamic malware analysis, IOC extraction

Practical Lab Sessions

Lab 5: Build an adversary profile from open sources and map it to MITRE ATT&CK.

Lab 6: Analyse a malware sample in an isolated lab and extract indicators

M4 | Cross-Domain Threat Hunting 16 hrs

Module / Topic

- Hypothesis-driven hunting, telemetry coverage, behavioural analytics, hunt documentation and hand-off to detection

Practical Lab Sessions

Lab 7: Run a hypothesis-driven hunt across endpoint and network telemetry.

Lab 8: Convert a successful hunt into a permanent detection rule

M5 | Specialisation Capstone 14 hrs

Module / Topic

- Applied project within the chosen specialisation, evidence and documentation, panel defence

Capstone Lab

Lab 9: Deliver a specialisation project end to end with full documentation.

Lab 10: Present findings and defend the approach to a panel

Track 2 Toolkit – Core Tools & Technologies

Every tool below is used in a defined lab session at the level shown.

Category	Tools / Platforms
Traffic Analysis	Wireshark
Scanning	Nmap
Vulnerability Management	OpenVAS
Forensics	Autopsy
Offensive Testing	Kali Linux · Metasploit
Detection	SIEM platforms
Analytics	Python for Security Analytics
SOC Analyst	Splunk · ELK Stack
Cloud Security	AWS · Azure · GCP
Threat Intelligence	OSINT tooling · Malware analysis

Tools by Level

Level	Toolset
Basic — Cybersecurity Technician	Wireshark · Nmap · OpenVAS · Autopsy
Intermediate — Network Security Engineer	Kali Linux · Metasploit · SIEM platforms · Python for Security Analytics
Advanced — Security Specializations	Splunk · ELK Stack · AWS · Azure · GCP · OSINT tooling · Malware analysis

Lab Environments

All practical sessions run in EduBlends cyber range and cloud lab environments. Offensive exercises are delivered on isolated, purpose-built ranges under defined rules of engagement, and forensic work uses write-blocked images and verified acquisition procedures.

Program Experience



The Network Security Engineering track spans three levels and 270 hours, delivered through 30 structured lab sessions and a panel-assessed capstone. Learners progress from foundational monitoring and network defence at the Basic level, through secure architecture, siem and security analytics at Intermediate, to elective specialisation in soc, cloud security or threat intelligence at Advanced. Every topic is reinforced in isolated cyber range and cloud lab environments that mirror live industry workflows, so that graduates leave with evidenced, portfolio-grade security work.

Expected outcomes



Advanced Industrial Internship Certifications

Differentiate yourself from your peers by earning the industrially recognized Advanced industrial internship Certification



Students Blending Team

EduBlends blends the students for the industry-ready



For the Industrial, By the Industry

Learn and apply concepts on industry projects from industry, along with personalized industry mentorship



Industry Integration Layer

This program is designed with integrated industry collaboration, where enterprise partners contribute to curriculum alignment, real-world problem statements, and internship pathways.



Cyber Range & Cloud Lab Facilities

Isolated attack and defence ranges, forensic workstations and cloud sandboxes for real industrial problems



360 Degree Career Support — Entrepreneurial Program

Idea-to-Enterprise Catalyst by EduBlends Academy is a structured entrepreneurial program that guides innovators from ideation to execution, helping them build and scale tech-driven businesses such as security consultancies, managed services and SaaS solutions.



Personalized Mentorship

Get unparalleled personalized mentorship and doubt resolution from industrialists and academicians.

Sample Weekly Program Planner



4–5 hours

Live interaction with the programme learning facilitator



1–2 hours

Recorded video lecture with faculty



1 hour

Group discussion with industrial mentor and academic instructor



4–5 hours

Cyber range and cloud lab practice exercises



2 hours

Rigorous, graded assignments to apply and reinforce the material

12–15 hours

Total weekly effort

Who Is This Program For?

Career Launchers

The Basic level (Sem 3–4) is designed for students and early-career IT professionals with no prior security background who want a structured, hands-on entry into cybersecurity.

Career Builders

The Intermediate level (Sem 5) suits IT support staff, network engineers and system administrators who want to move into hands-on security engineering and analysis roles.

Career Switchers

The Intermediate level also serves mid-career professionals working outside security who want credible, evidenced capability before making a career change.

Specialists & Founders

The Advanced level (Sem 7) is for learners who have completed the earlier levels, or who bring equivalent experience, and want to move into specialist and consultant roles — or to launch a security venture through the entrepreneurial programme.

Progressive Learning Pathway: Our curriculum is structured to provide a seamless learning experience, from foundational security skills at the Basic level through to specialist practice at Advanced.

- **Basic — Cybersecurity Technician (Sem 3–4)** for students beginning their graduation, providing the core tools and foundations to start the journey
- **Intermediate — Network Security Engineer (Sem 5)** for students who have completed the Basic level, and for individuals looking to upskill into hands-on security roles
- **Advanced — Security Specializations (Sem 7)** for students who have finished the earlier levels, and experienced individuals transitioning into specialist roles or entrepreneurship

Programs Key Features

Why Choose Our Courses?

Cyber Range & Cloud Lab: Gain hands-on experience in isolated attack and defence ranges with forensic workstations and cloud sandboxes, for real-world, industry-level security projects.

Industrial Internships & Expert Mentorship: Work on live industry projects, receive guidance from practising security professionals, and get the support you need for your career or entrepreneurial journey.

Personalized Instructor Support: Learn from experienced instructors committed to your growth, whether you are triaging your first alert or leading a full-scope engagement.

	Cyber Range Access	Industry-Integrated Internship	Live Mentorship by Industry Experts	Entrepreneurship Support
Coursera				
Udemy				
UpGrad Online				
Scaler Academy				
Simplilearn				
Unacademy				
EduBlends Academy	✓	✓	✓	✓

Comparison rows left intentionally blank pending verification. Competitor feature claims must be sourced, dated and evidenced before publication.