



# 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 4: Cyber Intelligence & Cloud Security

Basic to Advanced · 270 Hours Total

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

# Program Summary

Secure multi-cloud estates and turn telemetry into intelligence — from network fundamentals to cloud architecture and SOAR automation.



## 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) — Cybersecurity Trainee Foundations:** Network protocols, intrusion detection and Linux administration. Exit role: Cybersecurity Trainee.
2. **Intermediate Level (Sem 5–6) — Cybersecurity Analysis & Cloud Infrastructure:** Multi-cloud identity, access control and monitoring. Exit role: Cloud Security Engineer.
3. **Advanced Level (Sem 7–8) — Cloud Cybersecurity & Intelligence:** Cloud-native detection at scale, SOAR automation and OSINT. Exit role: Cloud Security Architect · 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 4 – Cyber Intelligence & Cloud Security

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

## Program Levels

| Level        | Title                                         | Semester | Hours  | Focus                                                           |
|--------------|-----------------------------------------------|----------|--------|-----------------------------------------------------------------|
| Basic        | Cybersecurity Trainee Foundations             | Sem 3    | 90 hrs | Network protocols, intrusion detection and Linux administration |
| Intermediate | Cybersecurity Analysis & Cloud Infrastructure | Sem 5–6  | 90 hrs | Multi-cloud identity, access control and monitoring             |
| Advanced     | Cloud Cybersecurity & Intelligence            | Sem 7–8  | 90 hrs | Cloud-native detection at scale, SOAR automation and OSINT      |

## Target Roles

| Level        | Semester | Role                                                                                                                 |
|--------------|----------|----------------------------------------------------------------------------------------------------------------------|
| Basic        | Sem 3    | Cybersecurity Trainee — building awareness of network protocols, intrusion detection, and basic Linux administration |
| Intermediate | Sem 5–6  | Cloud Security Engineer                                                                                              |
| Advanced     | Sem 7–8  | Cloud Security Architect · Intelligence Analyst                                                                      |

## Certification Alignment

| Level                                                        | Certifications                                                                                                                                                                            |
|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Basic — Cybersecurity Trainee Foundations                    | Microsoft SC-100 Cybersecurity Architect Expert · AWS Certified Security – Specialty · Google Professional Cloud Security Engineer · IBM Cloud Security Engineer Professional Certificate |
| Intermediate — Cybersecurity Analysis & Cloud Infrastructure | Google Professional Cloud Security Engineer · AWS Certified Security – Specialty                                                                                                          |
| Advanced — Cloud Cybersecurity & Intelligence                | AWS Certified Security – Specialty · Microsoft AZ-500 · Google Professional Cloud Security Engineer · IBM Cybersecurity Analyst Professional Certificate                                  |

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

TCS · HCLTech · Infosys · Genpact · Wipro · Google

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 Trainee Foundations

Sem 3 · 90 hours · Network protocols, intrusion detection and Linux administration · 10 practical lab sessions

## M1 | Linux Administration for Security 20 hrs

### Module / Topic

- Command line, users and permissions, services and daemons, package management, system and audit logging

### Practical Lab Sessions

- Lab 1:** Build, harden and audit a Linux server against a baseline standard.  
**Lab 2:** Configure centralised logging and verify audit trail completeness

## M2 | Network Protocols & Traffic Inspection 20 hrs

### Module / Topic

- TCP/IP stack, DNS, HTTP and TLS, protocol abuse patterns, capture and inspection with Wireshark

### Practical Lab Sessions

- Lab 3:** Inspect and decode DNS, HTTP and TLS sessions in a live capture.  
**Lab 4:** Identify protocol abuse and tunnelling in a provided capture

## M3 | Intrusion Detection & Prevention 18 hrs

### Module / Topic

- IDS versus IPS, signature and anomaly detection, rule syntax, deployment topology, tuning for false positives

### Practical Lab Sessions

- Lab 5:** Deploy an IDS in the lab and write custom rules for two attack patterns.  
**Lab 6:** Tune the ruleset against live traffic and measure the false positive rate

## M4 | Cloud Fundamentals & Shared Responsibility 18 hrs

### Module / Topic

- Cloud service models, the shared responsibility model, core cloud services, regions and availability, cost and risk basics

### Practical Lab Sessions

- Lab 7:** Deploy a minimal cloud workload and map every shared responsibility boundary.  
**Lab 8:** Assess the deployment against a cloud security baseline

## M5 | Security Operations Foundations 14 hrs

### Module / Topic

- Threat landscape, attack lifecycle, security controls taxonomy, ticketing and escalation, documentation

### Practical Lab Sessions

- Lab 9:** Map a real-world breach to the attack lifecycle and identify failed controls.  
**Lab 10:** Produce an escalation and communication plan for a simulated incident

# Program Frameworks – Intermediate Level: Cybersecurity Analysis & Cloud Infrastructure

Sem 5–6 • 90 hours • Multi-cloud identity, access control and monitoring • 10 practical lab sessions

## M1 | Identity & Access Management Across Clouds 22 hrs

### Module / Topic

- Identity models, roles and policies, federation and SSO, least privilege, privilege escalation paths in cloud IAM

### Practical Lab Sessions

- Lab 1:** Design and implement least-privilege IAM across two cloud providers.  
**Lab 2:** Audit an over-permissioned account and remediate the escalation paths

## M2 | Securing Cloud Workloads 20 hrs

### Module / Topic

- Network controls and security groups, encryption at rest and in transit, key management, workload isolation, secure baselines

### Practical Lab Sessions

- Lab 3:** Harden a cloud workload against a published security baseline.  
**Lab 4:** Implement encryption and key rotation, then verify enforcement

## M3 | Cloud Monitoring & Logging 18 hrs

### Module / Topic

- CloudWatch and equivalents, log aggregation, metrics and alarms, audit trails, retention and cost management

### Practical Lab Sessions

- Lab 5:** Configure end-to-end logging and alerting for a multi-tier workload.  
**Lab 6:** Build a monitoring dashboard and alert on a simulated compromise

## M4 | Cloud Security Posture Management 16 hrs

### Module / Topic

- Benchmark frameworks, configuration drift, automated compliance checks, remediation workflows, reporting

### Practical Lab Sessions

- Lab 7:** Run a posture assessment against a benchmark and score the estate.  
**Lab 8:** Automate remediation for the three highest-risk misconfigurations

## M5 | Multi-Cloud Governance & Compliance 14 hrs

### Module / Topic

- Governance models, policy as code, data residency, regulatory obligations, evidence for audit

### Practical Lab Sessions

- Lab 9:** Implement policy-as-code guardrails and test them against violations.  
**Lab 10:** Assemble an audit evidence pack for a compliance review

# Program Frameworks – Advanced Level: Cloud Cybersecurity & Intelligence

Sem 7–8 • 90 hours • Cloud-native detection at scale, SOAR automation and OSINT • 10 practical lab sessions

## M1 | Cloud-Native Detection with Chronicle SIEM 20 hrs

### Module / Topic

- Telemetry ingestion at scale, detection rule authoring, entity resolution, retro-hunting, tuning

### Practical Lab Sessions

- Lab 1:** Ingest multi-cloud telemetry into Chronicle and author detection rules.  
**Lab 2:** Run a retro-hunt across historical data and validate the findings

## M2 | SOAR & Response Automation 20 hrs

### Module / Topic

- Playbook design, orchestration across tools, automated enrichment and containment, human-in-the-loop controls

### Practical Lab Sessions

- Lab 3:** Build a SOAR playbook that enriches and triages an alert automatically.  
**Lab 4:** Extend it to automated containment with an approval gate, then test it

## M3 | Open-Source Intelligence & Adversary Tracking 18 hrs

### Module / Topic

- Intelligence lifecycle, collection planning, source validation, adversary infrastructure, ATT&CK mapping

### Practical Lab Sessions

- Lab 5:** Build an adversary profile from open sources with validated sourcing.  
**Lab 6:** Map the adversary's techniques to ATT&CK and derive detection priorities

## M4 | Enterprise Cloud Security Architecture 18 hrs

### Module / Topic

- Reference architectures, zero trust in cloud, landing zones, resilience and recovery, architecture documentation

### Practical Lab Sessions

- Lab 7:** Design a secure multi-cloud landing zone with documented controls.  
**Lab 8:** Review the design against a threat model and revise it

## M5 | Architecture & Intelligence Capstone 14 hrs

### Module / Topic

- Applied project spanning architecture, detection and intelligence, documentation, panel defence

### Capstone Lab

- Lab 9:** Deliver a secure cloud architecture with detection and response coverage.  
**Lab 10:** Present the design and threat assessment to a panel

# Track 4 Toolkit – Core Tools & Technologies

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

| Category              | Tools / Platforms                                       |
|-----------------------|---------------------------------------------------------|
| Traffic Inspection    | Wireshark                                               |
| Detection             | IDS / IPS                                               |
| Operating System      | Linux                                                   |
| Multi-Cloud Platforms | AWS · Azure · GCP                                       |
| Identity              | IAM                                                     |
| Monitoring            | CloudWatch and native monitoring services               |
| Cloud SIEM            | Chronicle SIEM — cloud-native threat detection at scale |
| Automation            | SOAR — automated incident orchestration and response    |
| Intelligence          | OSINT tooling                                           |

## Tools by Level

| Level                                                        | Toolset                                                                                                                        |
|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Basic — Cybersecurity Trainee Foundations                    | Wireshark · IDS / IPS · Linux                                                                                                  |
| Intermediate — Cybersecurity Analysis & Cloud Infrastructure | AWS · Azure · GCP · IAM · CloudWatch and native monitoring services                                                            |
| Advanced — Cloud Cybersecurity & Intelligence                | Chronicle SIEM — cloud-native threat detection at scale · SOAR — automated incident orchestration and response · OSINT tooling |

## 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 Cyber Intelligence & Cloud Security track spans three levels and 270 hours, delivered through 30 structured lab sessions and a panel-assessed capstone. Learners progress from network protocols, intrusion detection and linux administration at the Basic level, through multi-cloud identity, access control and monitoring at Intermediate, to cloud-native detection at scale, soar automation and osint 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) 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 5–6) 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 7–8) 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 Trainee Foundations (Sem 3)** for students beginning their graduation, providing the core tools and foundations to start the journey
- **Intermediate — Cybersecurity Analysis & Cloud Infrastructure (Sem 5–6)** for students who have completed the Basic level, and for individuals looking to upskill into hands-on security roles
- **Advanced — Cloud Cybersecurity & Intelligence (Sem 7–8)** 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.