
# Track 2: AI Security & Ethics

Level 3.5 to Level 5.5 · 270 Hours Total

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

# Program Summary

**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.

**Cloud Lab Integration** with every module, including isolated security lab ranges

**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 from AI Foundations to Secure Architecture

At EduBlends Academy, we provide a structured learning pathway that allows students to build their expertise in artificial intelligence, security operations and AI governance across their graduation journey.

1. **Start with Level 3.5 — Foundation of AI Technology:** Learners build the AI concepts, ethics and governance base — Python for security automation, machine learning and deep learning foundations with TensorFlow and PyTorch, responsible AI, and the regulatory frameworks that govern AI systems.
2. **Progress to Level 4.5 — AI Security Fundamentals:** Learners move into threat modeling, SOC operations and cyber defense — SIEM operations with Splunk and QRadar, vulnerability assessment with Nessus, penetration testing with Metasploit, and the attack surface specific to AI systems.
3. **Advance to Level 5.5 — AI Security Architect:** In the final phase, learners design enterprise-grade secure AI architecture — hardening containerised workloads with Docker and Kubernetes, cloud security on AWS and Azure, Zero Trust design, AI risk and assurance, and a panel-assessed capstone project.

**By following this structured pathway, students complete the full track within their graduation period, emerging as industry-ready professionals with a designed, defended and documented secure AI deployment to their name.**

# Track 2 – AI Security & Ethics

**Level 3.5 → Level 5.5 · 270 hours total · 28 practical lab sessions and one panel-assessed capstone**

## Program Levels

| Level | Title | Hours | Focus |
|---|---|---|---|
| **Level 3.5** | Foundation of AI Technology | 90 hrs | AI concepts, ethics, and governance |
| **Level 4.5** | AI Security Fundamentals | 90 hrs | Threat modeling, SOC, and cyber defense |
| **Level 5.5** | AI Security Architect | 90 hrs | Enterprise-grade secure AI architecture |

## Job Roles

| Role | Level | Primary Modules |
|---|---|---|
| **AI Ops Associate** | 3.5 | Python for AI, ML foundations, deep learning frameworks, responsible AI |
| **AI Cyber Analyst** | 3.5 → 4.5 | Threat modeling, vulnerability assessment, the AI attack surface |
| **SOC Specialist** | 4.5 | SOC operations with Splunk and QRadar, incident response playbooks |
| **AI Security Architect** | 5.5 | Container and cloud security, Zero Trust design, AI risk and assurance, capstone |

## Certifications

IBM AI Security · Azure Security Engineer (AZ-500) · AWS · Microsoft · NIELIT

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

## Entry Requirements

The half-level coding indicates a bridge entry point. Level 3.5 assumes basic computer literacy and familiarity with operating systems and networking concepts, but no prior programming or security experience. Level 4.5 requires completion of Level 3.5 or equivalent Python and AI foundations. Level 5.5 requires completion of Level 4.5 or demonstrable security operations experience.

# Program Frameworks – Level 3.5: Foundation of AI Technology

**90 hours · AI concepts, ethics, and governance · 10 practical lab sessions**

## M1 | Python for AI & Security Automation  20 hrs

| Module / Topic | Practical Lab Sessions |
|---|---|
| • Python fundamentals, OOP, file handling, scripting for log and data processing, working with APIs | **Lab 1:** Write Python scripts to parse and summarise system log files.<br>**Lab 2:** Automate a data collection task using Python and a REST API |

## M2 | AI Principles & Machine Learning Foundations  20 hrs

| Module / Topic | Practical Lab Sessions |
|---|---|
| • The AI landscape, supervised and unsupervised learning, the ML workflow, evaluation metrics, NLP and computer vision basics | **Lab 3:** Build and evaluate a classification model end to end.<br>**Lab 4:** Apply a pre-trained NLP model to classify text records |

## M3 | Deep Learning with TensorFlow & PyTorch  20 hrs

| Module / Topic | Practical Lab Sessions |
|---|---|
| • Neural networks, activation functions, backpropagation, training loops, convolutional networks, framework comparison | **Lab 5:** Build and train a neural network in TensorFlow/Keras; tune the training loop.<br>**Lab 6:** Rebuild the same model in PyTorch and compare performance and workflow |

## M4 | AI Ethics, Fairness & Responsible AI  15 hrs

| Module / Topic | Practical Lab Sessions |
|---|---|
| • Bias and fairness, explainability, transparency, inclusivity, environmental impact of AI systems | **Lab 7:** Audit a model for demographic bias and document the findings.<br>**Lab 8:** Produce model explanations and write a plain-language transparency note |

## M5 | AI Governance & Regulatory Frameworks  15 hrs

| Module / Topic | Practical Lab Sessions |
|---|---|
| • NIST AI Risk Management Framework, ISO/IEC 42001, EU AI Act, data protection obligations, AI policy and assurance | **Lab 9:** Map an AI use case against the NIST AI RMF and identify control gaps.<br>**Lab 10:** Draft an AI acceptable-use and governance policy for a sample organisation |

# Program Frameworks – Level 4.5: AI Security Fundamentals

**90 hours · Threat modeling, SOC, and cyber defense · 10 practical lab sessions**

## M1 | Security Fundamentals & Threat Modeling  18 hrs

**Module / Topic**

- CIA triad, network and system security basics, attack surface analysis, STRIDE, MITRE ATT&CK

**Practical Lab Sessions**

**Lab 1:** Build a STRIDE threat model for an AI-enabled application.
**Lab 2:** Map an attack chain against the MITRE ATT&CK framework

## M2 | SOC Operations with Splunk & QRadar  22 hrs

**Module / Topic**

- SIEM architecture, log ingestion and parsing, correlation rules, alert triage, incident response playbooks

**Practical Lab Sessions**

**Lab 3:** Ingest log sources into Splunk; build searches, dashboards and correlation rules.
**Lab 4:** Triage a simulated alert queue in QRadar and execute an incident response playbook

## M3 | Vulnerability Assessment with Nessus  15 hrs

**Module / Topic**

- Vulnerability management lifecycle, scanning strategy, CVSS scoring, prioritisation, remediation reporting

**Practical Lab Sessions**

**Lab 5:** Run an authenticated Nessus scan on a lab network and interpret the results.
**Lab 6:** Produce a prioritised remediation report from scan output

## M4 | Penetration Testing with Metasploit  15 hrs

**Module / Topic**

- Penetration testing methodology, rules of engagement, reconnaissance, exploitation, post-exploitation, reporting

**Practical Lab Sessions**

**Lab 7:** Exploit a vulnerable lab host using Metasploit and document the kill chain.
**Lab 8:** Write a penetration test report with findings, evidence and remediation advice

## M5 | The AI Attack Surface  20 hrs

**Module / Topic**

- Prompt injection, training data poisoning, model inversion and extraction, adversarial examples, model supply chain risk

**Practical Lab Sessions**

**Lab 9:** Craft and defend against prompt injection attacks on an LLM application.
**Lab 10:** Generate adversarial examples against an image classifier and test defences

# Program Frameworks – Level 5.5: AI Security Architect

**90 hours · Enterprise-grade secure AI architecture · 8 lab sessions and a panel-assessed capstone**

## M1 | Securing Containerised AI Workloads 20 hrs

| Module / Topic | Practical Lab Sessions |
|---|---|
| • Docker image security, registry scanning, Kubernetes architecture, RBAC, network policies, secrets management | **Lab 1:** Harden a Docker image for an ML service; scan it and remediate the findings.<br>**Lab 2:** Deploy the service to Kubernetes with RBAC, network policies and managed secrets |

## M2 | Cloud Security for AI on AWS & Azure 22 hrs

| Module / Topic | Practical Lab Sessions |
|---|---|
| • Identity and access management, key management, workload isolation, cloud security posture, native monitoring and detection services | **Lab 3:** Configure IAM roles, encryption and least-privilege access for an AI workload.<br>**Lab 4:** Enable cloud-native threat detection and review the generated security findings |

## M3 | Zero Trust & Enterprise Secure AI Architecture 18 hrs

| Module / Topic | Practical Lab Sessions |
|---|---|
| • Zero Trust principles, reference architectures, segmentation, secure MLOps pipelines, architecture documentation | **Lab 5:** Design a Zero Trust reference architecture for an enterprise AI platform.<br>**Lab 6:** Add security gates to an MLOps pipeline and document the resulting controls |

## M4 | AI Risk, Assurance & Incident Response 14 hrs

| Module / Topic | Practical Lab Sessions |
|---|---|
| • AI risk registers, third-party and model supply chain assurance, incident response for AI systems, audit evidence | **Lab 7:** Build an AI risk register and assurance checklist for a model in production.<br>**Lab 8:** Run a tabletop incident response exercise for a compromised model endpoint |

## M5 | Capstone: Secure AI Architecture Project 16 hrs

| Module / Topic | Capstone Lab: Full project |
|---|---|
| • Design, build, defend and document a secure AI deployment | Threat model an AI system, harden and deploy the container to a cloud environment, configure monitoring and detection, produce the architecture and risk documentation, and present to panel |

# Track 2 Toolkit – Core Tools & Technologies

**Students graduate fluent across the AI and security stack — from model building to SOC operations and secure cloud architecture.**

| Category | Tools / Platforms |
|---|---|
| **AI Development** | Python · TensorFlow · PyTorch |
| **Security Platforms** | Splunk · QRadar · Nessus · Metasploit |
| **Infrastructure & Cloud** | Docker · Kubernetes · AWS · Azure |

## Where Each Tool Is Taught

| Level | Tools Introduced | Modules |
|---|---|---|
| **Level 3.5 — Foundation of AI Technology** | Python, TensorFlow, PyTorch | M1 Python for AI & Security Automation; M2 AI Principles & ML Foundations; M3 Deep Learning with TensorFlow & PyTorch |
| **Level 4.5 — AI Security Fundamentals** | Splunk, QRadar, Nessus, Metasploit | M2 SOC Operations; M3 Vulnerability Assessment; M4 Penetration Testing; M5 The AI Attack Surface |
| **Level 5.5 — AI Security Architect** | Docker, Kubernetes, AWS, Azure | M1 Securing Containerised AI Workloads; M2 Cloud Security for AI; M3 Zero Trust Architecture; M5 Capstone |

## Lab Environments

All practical sessions run in EduBlends cloud lab environments. Offensive security exercises are delivered on isolated, purpose-built lab ranges under defined rules of engagement, and GPU-backed instances are provisioned for the Level 3.5 deep learning modules.

# Program Experience

**AI & Deep Learning**

Python · TensorFlow · PyTorch


**Ethics & Governance**

NIST AI RMF · ISO 42001 · EU AI Act


**Threat Modeling**

STRIDE · MITRE ATT&CK · Attack Surface

**SOC Operations**

Splunk · QRadar · Incident Response

**Offensive Security**

Nessus · Metasploit · Adversarial ML


**Secure Architecture**

Docker · Kubernetes · AWS · Azure

The AI Security & Ethics track spans three levels and 270 hours, delivered through 28 structured virtual lab sessions and a panel-assessed capstone project. Learners progress from AI concepts, deep learning frameworks, ethics and governance at Level 3.5, through threat modeling, SIEM-based SOC operations, vulnerability assessment, penetration testing and the AI-specific attack surface at Level 4.5, to container and cloud security, Zero Trust design and AI risk assurance at Level 5.5. Every topic is reinforced with real datasets and isolated lab ranges that mirror live industry workflows, so that graduates leave with a designed, defended and documented secure AI deployment.

# Expected outcomes

### Advanced Industrial Internship Certifications

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

### For the Industrial, By the Industry

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

### Cloud Lab Facilities

Cloud lab hours for industrial problems, including isolated security ranges and GPU-backed environments for the deep learning modules

### Personalized Mentorship

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

### Students Blending Team

EduBlends blends the students for the industry-ready

### 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.


### 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 AI security products, assurance services and SaaS solutions.

# 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** | Cloud lab and security range 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** | Level 3.5 is designed for students and early-career IT professionals with basic systems and networking familiarity who want a structured entry into artificial intelligence, AI ethics and governance. |
| **Career Builders** | Level 4.5 suits IT support staff, network engineers and system administrators who want to move into security operations, and to add the AI-specific attack surface to their existing defensive skill set. |
| **Career Switchers** | Level 4.5 also serves mid-career professionals working outside security who want credible, hands-on SOC, vulnerability assessment and penetration testing capability before making a career change. |
| **Specialists & Founders** | Level 5.5 is for learners who have completed Levels 3.5 and 4.5, or who bring equivalent security operations experience, and want to move into secure AI architecture and assurance — or to launch an AI security venture through the entrepreneurial programme. |

**Progressive Learning Pathway:** Our curriculum is structured to provide a seamless learning experience, starting from AI foundations, ethics and governance at Level 3.5 through to enterprise secure AI architecture and assurance at Level 5.5.

- **Level 3.5 — Foundation of AI Technology** for 2nd-year graduate students, providing the Python, machine learning, deep learning, ethics and governance foundations to begin the journey
- **Level 4.5 — AI Security Fundamentals** for 3rd-year students who have completed Level 3.5, and for individuals looking to upskill into security operations and defensive roles
- **Level 5.5 — AI Security Architect** for students who have finished Levels 3.5 and 4.5, and experienced individuals transitioning into architecture, assurance or entrepreneurship

## Programs Key Features

**Why Choose Our Courses?**

**Cutting-Edge Cloud Lab:** Gain hands-on experience with our cloud lab, offering isolated security ranges for offensive exercises and GPU-backed computational power for neural network training.

**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're a beginner at Level 3.5 or designing secure architectures at Level 5.5.

| | Cloud Lab 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.*