**AI+ Security (120hrs and 20 Days)**

**Duration:** 120hrs

**Days:** 20

**Exam Code:** AT-2103

**Executive Summary:**

The **AI+ Security Curriculum** is a comprehensive 20-day program that offers **120 hours of hands-on training** to equip learners with the necessary skills to integrate **AI** in **cybersecurity**. The curriculum is structured to provide a **strong foundation in both AI and cybersecurity** concepts, gradually advancing through key areas like machine learning, deep learning, natural language processing (NLP), and practical applications for real-world security challenges.

**Day 1–2: Module 1 - Introduction to AI and Cybersecurity (6 hours per day)**

---

**Module 1: Introduction to AI and Cybersecurity**

- **Topic 1.1: Introduction to Artificial Intelligence (AI)**
  - Definition of AI
  - Subfields of AI (Machine Learning, Deep Learning, NLP)
  - Applications of AI in various industries
  - Use-cases
  - Case study
- **Topic 1.2: Basics of Cybersecurity**
  - The CIA Triad: Confidentiality, Integrity, Availability
  - Types of cyberattacks: Malware, Phishing, DDoS, etc.
  - Overview of cybersecurity frameworks
  - Use-cases
  - Case study
  - Hands-on

- **Topic 1.3: AI and Cybersecurity Intersection**
    - Use cases for AI in Cybersecurity
    - AI's role in threat detection, prevention, and automation
    - Ethical considerations when using AI for security tasks
    - Use-cases
    - Case study
    - Hands-on

---

**Day 3–4: Module 2 - Python for AI and Cybersecurity (6 hours per day)**

---

**Module 2: Python for AI and Cybersecurity**

- **Topic 2.1: Python Basics for Cybersecurity**
    - Introduction to Python programming
    - Basic data structures in Python: Lists, Tuples, Dictionaries
    - Functions and error handling
    - Hands-on
- **Topic 2.2: Python Libraries for Security Automation**
    - Introduction to Python libraries: Pandas, NumPy
    - Automating tasks using **Scapy** for network traffic analysis
    - **PyCryptodome** for implementing encryption/decryption
    - Use-cases
    - Case study
    - Hands-on
- **Topic 2.3: Building Basic Security Tools in Python**
    - Writing scripts for **log analysis** and **network scanning**
    - **Creating a vulnerability scanner** and automating simple security tasks

- Use-cases
- Case study
- Hands-on

---

**Day 5–6: Module 3 - Supervised Learning for Cybersecurity (6 hours per day)**

---

**Module 3: Supervised Learning for Cybersecurity**

- **Topic 3.1: Introduction to Machine Learning**
  - Overview of **Supervised Learning**
  - Types of algorithms: **Classification vs. Regression**
  - **Training models** with labeled data
  - Use-cases
  - Case study
  - Hands-on
- **Topic 3.2: Supervised Learning Algorithms for Malware Detection**
  - Overview of **Random Forests**, **SVM**, **Logistic Regression**
  - **Feature extraction** for malware data
  - **Model evaluation** metrics: Precision, Recall, F1-Score
  - Use-cases
  - Case study
  - Hands-on
- **Topic 3.3: Phishing Detection using Supervised Learning**
  - Feature extraction from **emails** (subject, sender, body content)
  - Building a **Phishing Email Classifier** with **Logistic Regression**
  - Use-cases
  - Case study

- Hands-on

---

**Day 7–8: Module 4 - Deep Learning for Advanced Threat Detection (6 hours per day)**

---

**Module 4: Deep Learning for Advanced Threat Detection**

- **Topic 4.1: Introduction to Deep Learning**
  - Overview of **Neural Networks**
  - Types of Neural Networks: **Feedforward**, **CNNs**, **RNNs**
  - **Training deep neural networks** for cybersecurity tasks
  - Use-cases
  - Case study
  - Hands-on
- **Topic 4.2: Using CNNs for Malware Detection**
  - Introduction to **Convolutional Neural Networks (CNNs)**
  - **CNNs** for malware classification based on file features
  - **Model training** and **evaluation** with deep learning models
  - Use-cases
  - Case study
  - Hands-on
- **Topic 4.3: Using RNNs and LSTMs for Anomaly Detection**
  - Understanding **Recurrent Neural Networks (RNNs)** and **LSTM (Long Short-Term Memory)** networks
  - Applications of **RNNs/LSTMs** for **sequential data analysis** like **network traffic analysis**
  - **Model performance metrics** and handling time-series data
  - Use-cases
  - Case study

- Hands-on

---

**Day 9–10: Module 5 - Natural Language Processing (NLP) for Cybersecurity (6 hours per day)**

---

**Module 5: Natural Language Processing (NLP) for Cybersecurity**

- **Topic 5.1: Introduction to NLP**
  - Overview of **NLP** and its applications in cybersecurity
  - **Text preprocessing** techniques: Tokenization, Lemmatization, Stop-word removal
  - Use-cases
  - Case study
  - Hands-on
- **Topic 5.2: Using NLP for Phishing Detection**
  - NLP techniques for analyzing **email content** and detecting **phishing attacks**
  - Feature extraction for **phishing emails**: Analyzing sender, subject, and body text
  - Building a **Phishing Email Classifier** using **NLP techniques**
  - Use-cases
  - Case study
  - Hands-on
- **Topic 5.3: Extracting Threat Intelligence using NLP**
  - Using **NER (Named Entity Recognition)** to identify malicious entities in text (e.g., **IP addresses**, **URLs**, **file hashes**)
  - Automating **threat intelligence extraction** from security logs, reports, and news articles using **SpaCy** and **NLTK**
  - Use-cases

- Case study
- Hands-on

---

**Day 11–12: Module 6 - Advanced Cybersecurity Concepts with AI (6 hours per day)**

---

**Module 6: Advanced Cybersecurity Concepts with AI**

- **Topic 6.1: AI for Malware Detection and Classification**
  - Advanced malware detection using **Deep Learning models** (CNNs, RNNs)
  - **Model training** on large datasets of **malware** samples and **benign** files
  - Use-cases
  - Case study
  - Hands-on

- **Topic 6.2: AI in Cloud Security**
  - Using **AI** for **cloud security**: **DDoS detection**, **data protection**, and **threat prevention**
  - Use-cases
  - Case study
- **Topic 6.3: AI in IoT Security**
  - AI applications in **IoT security**: Detecting **anomalies** in IoT device behavior
  - Leveraging **AI models** to secure **smart devices** and IoT networks
  - Use-cases
  - Case study
  - Hands-on

---

**Day 13–14: Module 7 - Implementing and Managing AI-Driven Security Solutions (6 hours per day)**

---

**Module 7: Implementing and Managing AI-Driven Security Solutions**

- **Topic 7.1: Building AI Pipelines for Security**
    - Overview of **AI Pipelines**: Steps in building and deploying **AI models** for cybersecurity tasks
    - **Data collection**, **preprocessing**, and **model training** pipelines for security solutions
    - Use-cases
    - Case study
    - Hands-on
- **Topic 7.2: Managing False Positives and False Negatives**
    - Techniques for reducing **false positives** and **false negatives** in AI models used for **security analysis**
    - Balancing **precision and recall** in real-time detection systems
    - Use-cases
    - Case study
    - Hands-on
- **Topic 7.3: Continuous Model Retraining and Updates**
    - **Model drift** and the need for continuous retraining
    - Strategies for updating AI models to detect **new threats** in evolving cybersecurity environments

---

**Day 15: Module 8 - AI-Driven Incident Response (6 hours)**

---

**Module 8: AI-Driven Incident Response**

- **Topic 8.1: Introduction to Incident Response**

- **Incident Response** phases: **Detection**, **Containment**, **Eradication**, **Recovery**, and **Lessons Learned**
- **AI** for automating these phases, especially **detection** and **containment**
- Use-cases
- Case study
- Hands-on

- **Topic 8.2: Real-Time Detection and Automated Response**
  - Using **AI** for **real-time detection** of threats and **automating incident response**
  - Case studies on AI-driven tools for **automated threat containment** and **real-time remediation**
  - Use-cases
  - Case study
  - Hands-on

---

**Day 16–17: Module 9 - Ethical AI in Cybersecurity (6 hours per day)**

---

**Module 9: Ethical AI in Cybersecurity**

- **Topic 9.1: Introduction to Ethical AI**
  - Ethical challenges in using **AI** for cybersecurity
  - **Bias** in AI models: Understanding and mitigating its impact on security decisions
- **Topic 9.2: Addressing Bias and Ensuring Fairness**
  - Techniques for detecting and addressing **bias** in cybersecurity AI models
  - **Fairness metrics** and ensuring AI models don't unfairly target certain groups or individuals
- **Topic 9.3: Transparency and Explainability**

- The importance of making **AI-driven security systems** transparent and interpretable
- Tools and frameworks for **explaining AI decisions** in cybersecurity (e.g., why a file was flagged as malicious)
- Use-cases
- Case study
- Hands-on

---

**Day 18–19: Module 10 - Capstone Project and Final Review (6 hours per day)**

---

**Module 10: Capstone Project and Final Review**

- **Topic 10.1: Designing the AI-Driven Cybersecurity Solution**
  - Step-by-step guide for designing and implementing a cybersecurity solution using **AI** (e.g., **phishing detection**, **malware classification**)
  - **Data collection**, model selection, feature extraction, and training
  - **Projects**
- **Topic 10.2: Final Project Review**
  - Reviewing key concepts: **AI pipelines**, **supervised learning**, **deep learning** in security
  - **Project presentations** guidelines by instructor.

---

**Day 20: Module 10 - Capstone Project and Final Review (continued) (6 hours)**

**Module 10: Capstone Project and Final Review (continued)**

- **Topic 10.3: Project Presentation**
  - Capstone projects by instructor with real world problem statement and challenges.
  - **Presentation skills** for showcasing AI-driven cybersecurity solutions

- **Topic 10.4: Project Feedback**
    - Instructor’s feedback on projects