AI Cybersecurity 16-Week Curriculum

I Phase 1: Foundations (Weeks 1–4)

Goal: Build your base in cybersecurity + AI/ML fundamentals.

🗒 Week 1 – Cybersecurity Essentials ✅

- Module 1: Model of hierarchical complexity
- Module 2: CIA Triad (Confidentiality, Integrity, Availability), Authentication, Authorization, Accounting (AAA)
- Module 3: Network security basics (firewalls, IDS, IPS)
- Module 4: Cryptography 101 (hashing, symmetric vs. asymmetric)
- Module 5: Security policies & threat landscape (malware, phishing)
    - Module 6–7: Practice lab → Set up a virtual lab (VirtualBox + Kali + Ubuntu), Learn about Git and GitHub

🗒 Week 2 - Incident Response & Security...

- Module 1: Incident Response lifecycle (NIST model)
- Module 2: Digital forensics basics
- Module 3: SIEM overview (Splunk / ELK stack intro)
- Module 4: Security monitoring & logging
- Module 5: Lab → Collect and analyze logs in ELK
- Recap + flashcards

🗒 Week 3 - AI/ML Fundamentals ✅

- Module 1: Intro to AI vs. ML vs. Deep Learning
- Module 2: Supervised vs. unsupervised learning
- Module 3: Data preprocessing & feature engineering
- Module 4: Training vs. testing sets, overfitting, bias
- Module 5: Lab → Build a basic ML classifier (scikit-learn, Iris dataset)
- Quiz + review notes

🗒 Week 4 – Practical ML Foundations ✅

- Module 1: Neural networks overview
- Module 2: Gradient descent & optimization basics
- Module 3: Intro to TensorFlow & PyTorch
- Module 4: ML pipeline in cybersecurity use cases
- Module 5: Lab → Train a simple spam classifier using Naive Bayes
- Reflection journal

Phase 2: Blue Team AI for Cyber Defense (Weeks 5–8)

Goal: Use AI for detection & response.

Week 5 – Threat Detection with ML

- Module 1: Intrusion Detection Systems (IDS/IPS)
- Module 2: Dataset overview (KDD99, NSL-KDD, UNSW-NB15)
- Module 3: Feature extraction for network data
- Module 4: Lab → Train anomaly detection model with scikit-learn
- Module 5: Evaluate precision, recall, F1 in cybersecurity context

Week 6 – Malware & Phishing Detection

- Module 1: Malware classification (static vs. dynamic analysis)
- Module 2: Using ML for phishing detection
- Module 3: Lab → Train ML model to classify phishing URLs
- Module 4: Adversarial examples in malware detection
- Module 5: Writeup → Security blog-style report on findings

Week 7 – Security Monitoring with AI

- Module 1: SIEM + AI integrations (Splunk Machine Learning Toolkit)
- Module 2: Log anomaly detection with ML
- Module 3: Lab → Detect anomalies in server logs using Python
- Module 4: Case study: Microsoft Sentinel AI features
- Module 5: Mini-project → Build simple log anomaly dashboard

Week 8 – Blue Team AI Capstone

- Build a prototype ML-powered IDS
- Document pipeline: data preprocessing → model training → evaluation → alert generation
- Deliverable: Report + working demo

Phase 3: Red Team Adversarial AI & Threats (Weeks 9-12)

Goal: Learn how attackers exploit AI systems.

Week 9 – Adversarial ML Basics

- Module 1: Attack surface of ML systems
- Module 2: Evasion attacks (adversarial examples)
- Module 3: Data poisoning
- Module 4: Model inversion & extraction
- Module 5: Lab → Use CleverHans to generate adversarial examples

Week 10 – Generative AI Risks

- Module 1: Deepfakes & synthetic media
- Module 2: AI-assisted phishing (LLM-driven)
- Module 3: Malware generation w/ LLMs (theory, controlled lab only)
- Module 4: Case studies (AI misuse in real incidents)
- Module 5: Discussion + writeup on ethical concerns

Week 11 – Red Teaming AI Models

- Module 1: Threat modeling for AI systems
- Module 2: Prompt injection & LLM attacks
- Module 3: Adversarial fuzzing for ML models
- Module 4: Lab → Attempt model evasion on trained IDS
- Module 5: Document findings

Week 12 – Red Team AI Capstone

- Design and document an adversarial attack on a basic ML

system (lab only)
- Deliverable: Report (attack method + defense recommendations)

Phase 4: Governance & Enterprise AI Security (Weeks 13–16)

Goal: Secure real-world deployments and understand compliance.

Week 13 – Governance & Risk

- Module 1: NIST AI Risk Management Framework
- Module 2: EU AI Act overview
- Module 3: U.S. AI Executive Orders & policies
- Module 4: Privacy regulations (GDPR, HIPAA)
- Module 5: Case study → AI governance failures

Week 14 – Enterprise AI Security Tools

- Module 1: AI in SOC workflows
- Module 2: Endpoint protection w/ AI (CrowdStrike, SentinelOne)
- Module 3: AI for threat intel (Recorded Future, Darktrace)
- Module 4: Lab → Build a mock SOC playbook integrating AI alerts
- Module 5: Group presentation (if team learning)

Week 15 – Future Trends in AI Security

- Module 1: Explainable AI (XAI) in cybersecurity
- Module 2: Federated learning for privacy
- Module 3: AI in IoT and OT security
- Module 4: Quantum-safe cryptography + AI
- Module 5: Research paper review

Week 16 – Final Capstone

- Build & present a **full-stack AI security solution**:

- ML-powered anomaly detection
- Attack simulation + defense
- Governance checklist applied
- Deliverable: Final report + demo system

By the end of Week 16:
You'll have gone through **defensive AI, offensive AI, adversarial ML, and governance**, with 3 mini-capstones + 1 final project.
