INFOSECTRAIN
Educate. Excel. Empower.

AI-Powered Course

Cybersecurity AI Foundation Program

Course Highlights

- **40-Hour** Instructor-Led Training
- AI-Driven Pentesting
- Learn AI by Building
- Attack AI Models
- Secure AI Models
- AI Governance Mapping
- AI-Powered Security Operations
- Hands-On Labs throughout the Course
- Extended Post Training Support

About Course

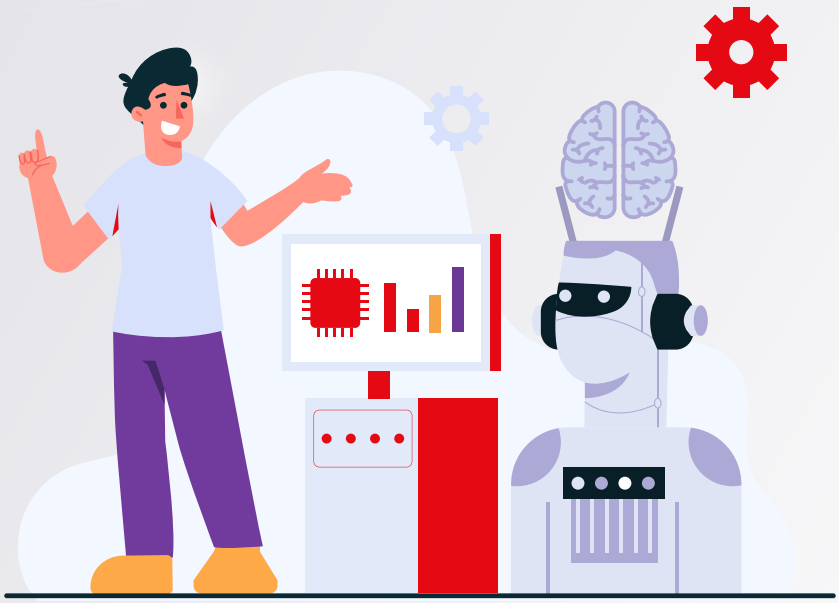
InfosecTrain's Cybersecurity AI Foundation Program is a comprehensive program tailored to meet the demands of today's rapidly evolving digital landscape. This beginner level course delves into integrating Artificial Intelligence with cybersecurity, providing participants with advanced skills to detect, analyze, and counter cyber threats efficiently. The course bridges the gap between traditional cybersecurity and modern AI security with hands-on coverage, which is very crucial for participants.

Through hands-on exercises, case studies, and industry-relevant scenarios, learners understand how AI systems actually work under the hood. Designed to explain how AI is secured across the full lifecycle: Data → Model → Deployment → Operations, this course provides exposure to real attack techniques and defensive controls.

Course Objectives

After completion of this course, you will be able to:

- Understand how AI systems work and how they apply to security
- Build AI-based Security Systems
- Identify and Exploit AI Vulnerabilities
- Secure AI Systems
- Implement Governance and Compliance
- Use AI for Defensive (SOC) and Offensive Security



Target Audience

This training is ideal for:

- Cybersecurity Professionals – Security Analysts, SOC Analysts, Security Engineers, Detection Engineers
- Offensive Security Professionals
- GRC Professionals and Security Auditors who want to understand how AI systems work
- Security Professionals who want to learn how to leverage Open-source AI tools and LLMs securely in their workflow
- Anyone who wants to understand how AI models as a security control are built
- Anyone who wants to transition to AI Security Roles

Pre-Requisites

- Fundamental Knowledge of Security Concepts
- No coding or AI Knowledge required

Course Content

Part 1 - AI Fundamentals

MODULE 1

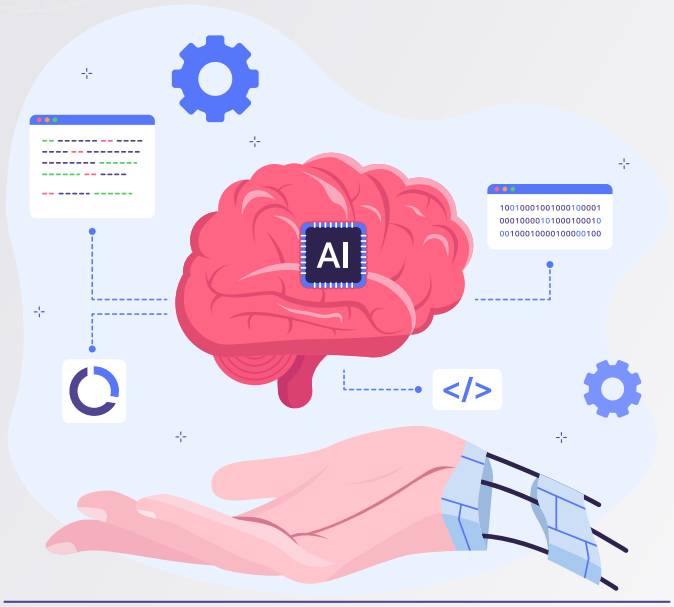
Module 1: Introduction to AI

- What is Artificial Intelligence: AI, Machine Learning, Deep Learning
- Components of an AI System
- Brief history and evolution: from rule-based systems to modern deep neural networks
- How Machines Learn: Supervised learning, Unsupervised learning, Reinforcement learning
- Types of AI Models and What They Do: Classification models, Regression models, Clustering models, Language models
- AI Model development lifecycle
- AI Tools Landscape: Huggingface, OpenWebUI, GenAI platforms, Open-source model platforms for running models locally: Ollama, LM Studio
- AI Risks and Responsible AI use
- Prompt Engineering Techniques

MODULE 2

Module 2: Python Basics for Using AI Frameworks

- Python Fundamentals for AI
- Lab Setup: Linux VM, Using Jupyter Notebook
- Google Colab: free cloud compute for coding and AI/ML experiments
- Python Libraries for Data Analysis and Visualisation: Pandas, NumPy, Matplotlib
- Types of Data and using them for AI Model development
- Secure and Responsible use of Data in AI models and Applications

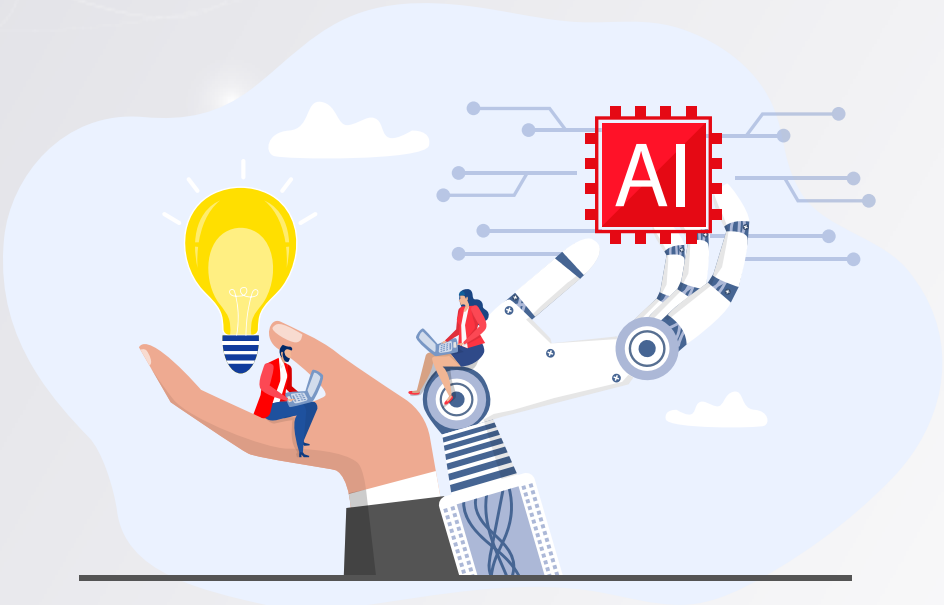


MODULE 3

Module 3: Machine Learning for Security

- Libraries and frameworks for Machine Learning and Deep Learning
- Data Collection
- Data Processing (Including Feature Extraction and Normalization)
- Algorithm selection and Model Training
- TEVV: Test, Evaluation, Verification, and Validation and Fine Tuning
- Model Deployment, Model Monitoring and Retraining

Practical Lab: Building AI (ML and DL) models for Network Security by using GenAI



MODULE 4

Module 4: Natural Language Processing (NLP)

- Libraries and frameworks for NLP
- Text Processing for NLP: Tokenization, Stop words removal, Embeddings
- NLP Feature Engineering Types
- Converting Emails and Logs to Vectors

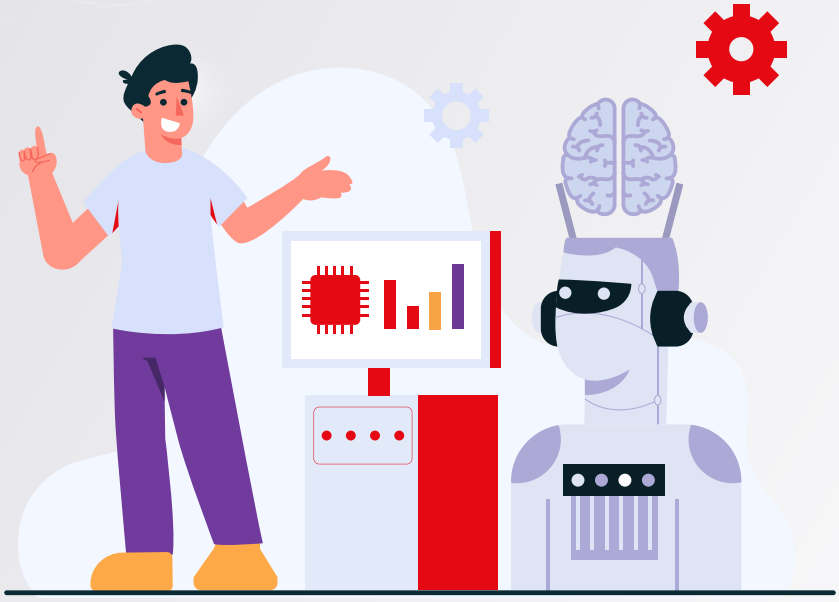
Practical Lab: Building a Phishing Mail Detector

MODULE 5

Module 5: Generative AI, LLMs and Agentic AI

- Generative Adversarial Networks
- Transformer Architecture
- System Prompts and User Prompts
- Prompt Engineering Techniques
- Foundational model and fine-tuned model
- Retrieval Augmented Generation (RAG)
- Agentic AI: Autonomous agents, Planning, Reasoning, Action: tool use, and multi-agent orchestration frameworks
- Agentic AI Frameworks: Langchain, CrewAI
- Model Context Protocol (MCP)

Practical Lab: Building a Gen AI Based Custom Chatbot & Agent



Part 2 - AI Security and Governance

Module 6: Attacking AI

- Poisoning: Data and Model Poisoning
- Backdoor Attacks with Trigger-Based Poisoning
- Evasion Attacks: Evading AI-Based Detectors
- Model and Data Theft
- Inversion and Membership Inference Attacks
- OWASP Machine Learning Security Top 10
- Prompt Injection: Direct and Indirect
- Jailbreaking Techniques
- OWASP Top 10 for Large Language Model Applications
- OWASP Top 10 for Agentic Applications

Practical Lab: Automated LLM Pentesting using Garak

MODULE 7

Module 7: Securing AI

- Threat Modelling: MITRE ATLAS, MAESTRO Framework
- Defense-in-Depth for AI
- Secure Infrastructure Architecture for AI Systems
- Data Security in AI Systems
- Adversarial Training and Bias Checking
- Guardrails for LLMs: System Prompt Hardening, Input and Output Guards
- Open-Source Guardrail Tools: LLM-Guard, Guardrails-AI, LlamaGuard
- AI Gateway: LiteLLM
- Monitoring and Observability for AI Systems: MLFlow, Arize Phoenix
- Rate Limiting & Cost Budgeting
- Data and Model Versioning
- Access control for AI
- Data and Model Integrity
- AI Supply Chain Security

Practical Lab: Integrating guardrails with AI models

MODULE 8

Module 8: AI Governance

- AI Ethics & Properties of a Responsible AI System
- Data Governance & Model Governance
- NIST AI RMF (Govern/Map/Measure/Manage) and ISO 42001 Annex A Controls
- EU AI Act risk tiers
- Security Roles & Operating Model for AI

Practical Lab: Governance control mapping exercise

Part 3 - Security Operations and Offensive Security using AI

Module 9: Offensive Security using AI

- AI in the Penetration Testing Lifecycle: Reconnaissance, Scanning, Exploitation, Reporting
- Reconnaissance using AI: OSINT Tools, AI-Generated Recon Scripts
- Intelligent Scanning and Enumeration: Nmap with AI, AI-Generated Scan Profiles
- AI-Enhanced Password Attacks: Wordlist Generation, Brute Force Automation
- Web Application Pentesting with AI
- Social Engineering with AI: AI-Generated Phishing Emails
- Covering Tracks and Maintaining Access with AI-Generated Scripts

Practical Lab: AI-Assisted Reconnaissance, Network Scan, Exploitation, and Pentest Report Writing

Module 10: Security Operations using AI

- Security Operations: Structure, Roles, and Core Functions
- Signature based detection principles
- AI Integration in Security Operations
- Using ML+Signatures for best results
- AI for Log Analysis: Windows Event Logs, Network Logs
- AI for Alert Triage and False Positive Reduction
- Threat Intelligence: IOCs, MITRE ATT&CK, AI-Assisted IOC Correlation
- Vulnerability Management with AI: CVE Explanation, Prioritization, Remediation
- Incident Response Lifecycle with AI-Guided Playbooks
- User and Entity Behaviour Analytics (UEBA)
- Malware detection using AI
- Using AI with SIEM tools (ELK Stack)

Practical Lab: Analysis of IDS Logs using Generative AI and Agentic AI

INFOSECTRAIN

Educate. Excel. Empower.

Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on