INFOSECTRAIN
Educate. Excel. Empower.

AI-Powered Course

# AI-Powered Cybersecurity

## Training Course

# Course Highlights

- **40-Hour** Instructor-Led Training
- Career-oriented Skill-based Course
- Learn with Real-World Scenarios
- Industry-Standard Tools and Frameworks
- AI+ Cybersecurity Hands-On Labs
- Learn from Industry Experts
- Career Guidance and Mentorship
- Extended Post Training Support
- Access to Recorded Sessions

# About Course

InfosecTrain's AI-Powered Cybersecurity Training is designed to help professionals understand, build, and secure AI-driven systems within modern cybersecurity environments. The program integrates Artificial Intelligence with core security principles to enable learners to detect threats, analyze attack patterns, and respond using AI-based techniques. It also introduces essential Python fundamentals for working with AI applications in cybersecurity, ensuring a practical understanding of data, models, and security workflows. Through hands-on labs, real-world scenarios, and industry-aligned tools, learners gain exposure to both offensive and defensive AI security use cases. The course is designed for cybersecurity professionals, IT practitioners, and aspiring AI security specialists, bridging traditional security practices with emerging AI technologies for real-world applications.

# Course Objectives

Upon successful completion of the training, participants will be able to:

- Bridge the gap between traditional cybersecurity and modern AI systems security
- Understand how AI systems work under the hood beyond theoretical concepts
- Apply AI for both offensive and defensive cybersecurity use cases
- Secure AI systems across the full lifecycle: data, model, deployment, and operations
- Gain exposure to real-world attack techniques and defensive security controls
- Work with industry-relevant open-source AI and cybersecurity tools and frameworks
- Build AI-based security systems for real-world applications
- Use AI effectively in offensive security scenarios
- Secure AI systems end-to-end across enterprise environments
- Identify and exploit vulnerabilities in AI systems
- Implement governance, compliance, and responsible AI security practices

# Target Audience

This training is ideal for:

- Beginners in cybersecurity, with coding supported by Generative AI tools
- 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 are built as security controls
- Anyone who wants to transition to AI security roles
- Cybersecurity Professionals - Security Analysts, SOC Analysts, Security Engineers, Detection Engineers
- Offensive Security Professionals

# Pre-Requisites

Fundamental knowledge of core cybersecurity concepts is required.

# Course Content

## Part 1: Understanding and Using AI

MODULE 1

### Module 1: Introduction to AI and AI in Cybersecurity

- AI and its Evolution
- Components of an AI System
- AI vs ML vs Data Science
- Algorithm vs Model
- Types of Learning – Supervised, Unsupervised, Semi-Supervised, Reinforcement, Federated
- Types Of Models
- AI Use Cases in Cybersecurity
- Risks of AI

MODULE 2

## Module 2: Python Basics for Using AI Frameworks

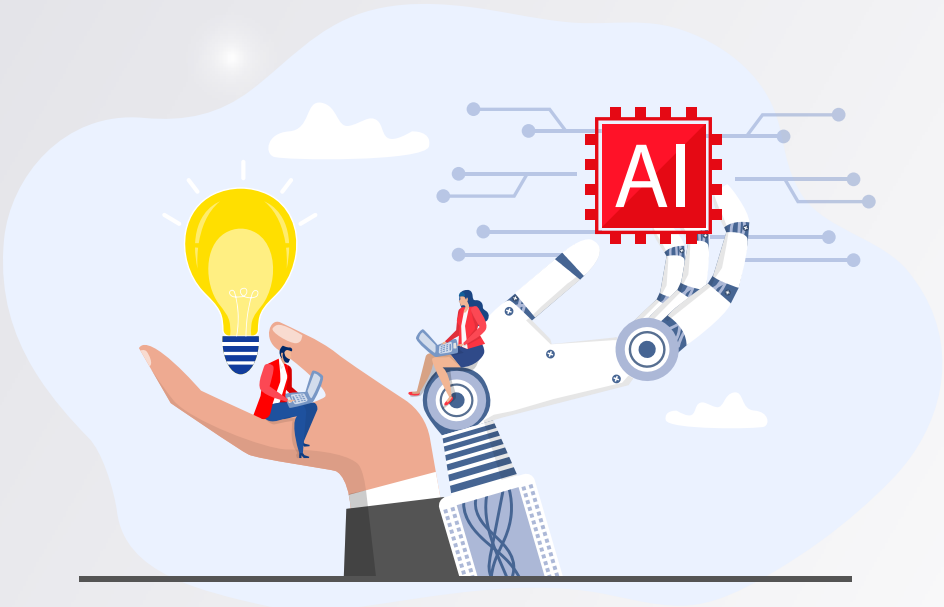
- Python Fundamentals for AI
- Python Libraries for Data Analysis and Visualisation – Pandas, NumPy, Matplotlib
- GenAI Platforms: Google Colab, Hugging Face, Ollama, LMStudio, OpenAI Platform, Google AI Studio, Anthropic, Groq
- AI Model Development Lifecycle
- Types of Data and using them for AI Model development
- Secure and Responsible use of Data in AI models and Applications

**Lab Setup:** Linux VM, Using Jupyter Notebook

## Module 3: Using AI for Cyber Offense

- Using AI for:
  - ✓ Reconnaissance
  - ✓ Vulnerability Scanning
  - ✓ System Hacking

- **Hands On:** ShellGPT, Open-Source Models for Offensive Security
- **Hands On:** Generating Network Attacks Using AI
- **Hands On:** Collecting Network Attack Traffic Data: Packets and Logs.



MODULE 4

## Module 4: Building ML-based Security Controls using Generative AI

- Data Collection
- Data Processing (Including Feature Extraction & Normalization)
- Model Training
- TEVV: Test, Evaluation, Verification, Validation, and Fine Tuning
- Model Deployment, Model Monitoring and Retraining

- **Hands On:** Using Gen AI tools for Building AI models for Network Security
- **Hands On:** Building Anomaly Detector using Unsupervised Learning using Gen AI Tools
  User and Entity Behaviour Analytics (UEBA)
- **Hands On:** Building Keystroke Behaviour Analysis Detector

## Module 5: Natural Language Processing (NLP)

- Text Processing for NLP: Tokenization, Stop words removal
- NLP Feature Engineering Types

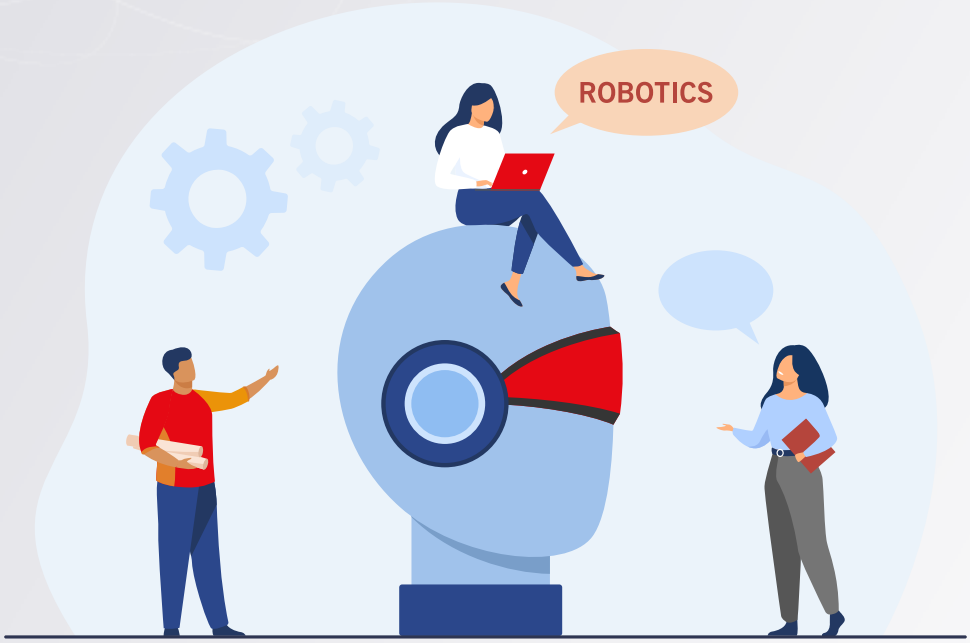
- **Hands On:** Converting Emails and Logs to Vectors
- **Hands On:** Building a Phishing Mail Detector

MODULE 6

## Module 6: Neural Networks and Deep Learning for Cybersecurity

- Perceptron
- Multi-Layer Perceptron (MLP)
- Convolutional Neural Networks (CNN)
- Recurrent Neural Networks (RNN)
- How Deep Learning enables Building Models for Complex Cybersecurity Data

**Hands On:** Building Malware Detectors Using CNN



MODULE 7

## Module 7: Generative AI and LLMs

- Generative Adversarial Networks
- Transformer Architecture
- Prompt Engineering Techniques and System Prompts
- Foundational model and fine-tuned model
- Retrieval Augmented Generation (RAG)

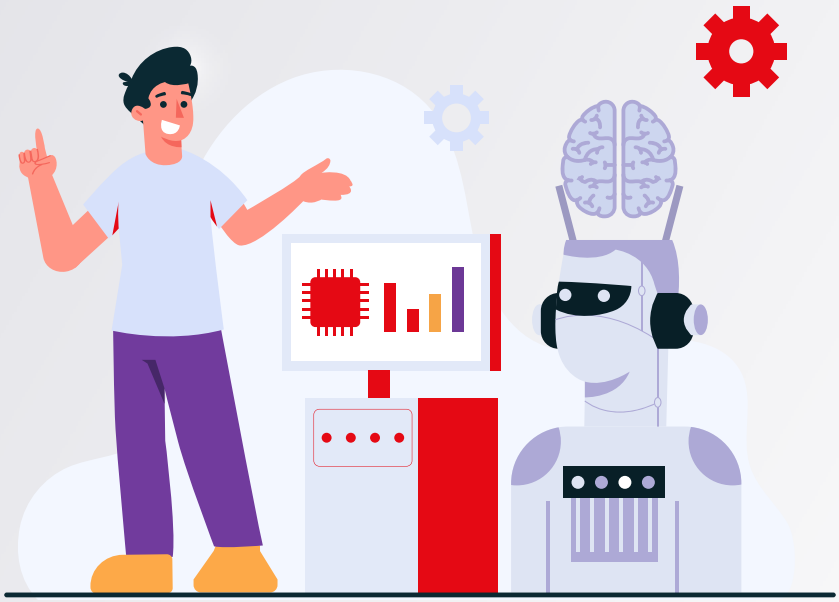
- **Hands On:** Building a Gen AI-Based Custom **Chatbot**
- **Hands On:** Using Gen AI for Summarizing **Threat Intelligence and Vulnerability Reports**

MODULE 8

## Module 8: SIEM-IDS-Integration, Deployment, and Monitoring of AI Models

- Ingesting IDS Logs into SIEM (ELK Stack)
- Data Parsing using AI
- Setting up the Data and Model Pipelines
- Monitoring and Observability
- Dealing with Data Lag and Model Drift
- Secure Retraining Mechanisms

- **Hands On:** FastAPI for Deploying and Serving Models
- **Hands On:** **AI Observability** with OpenLLMetry + Phoenix

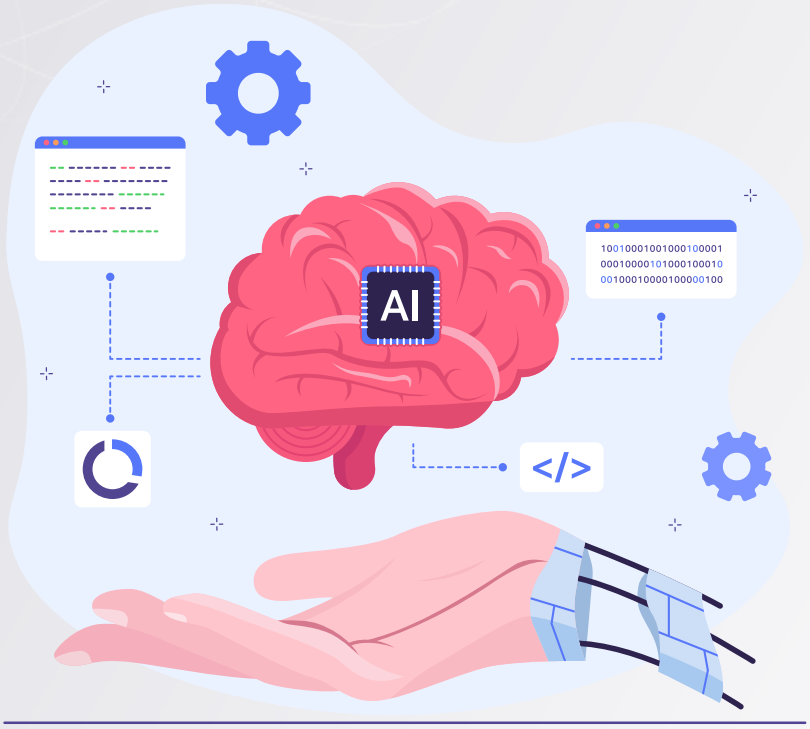


MODULE 9

## Module 9: Agentic AI for Security Operations

- Components To Build Agentic AI
- Agentic AI: Autonomous agents, Reasoning, Action: tool use, and multi-agent orchestration frameworks
- Model Context Protocol (MCP): architecture, use cases, and security implications
- Agent topology design principles

**Demo:** Using Agentic AI for **generating Triage Reports**



# Part 2: Attacking, Governing, and Securing AI

MODULE 10

## Module 10: Adversarial Attacks on AI

- Poisoning: Data and Model
- Setting up Backdoor with Trigger-Based Poisoning
- Evasion
- Evading AI-Based Detectors
- Theft: Data and Model
- Inversion and Inference Attacks
- OWASP Machine Learning Security Top 10
- OWASP Top 10 for Large Language Model Applications
- OWASP Top 10 for Agentic Applications

- **Hands On:** Honeytokens in prompts and vector stores
- **Hands On:** Automated LLM pentesting using Garak

MODULE 11

## Module 11: Security Architecture Principles Applied to AI

- Secure Infrastructure reference architecture for AI Workloads
- Defense-in-depth for AI pipelines
- Zero-trust architecture for AI services
- Role of AI Gateway
- Segmentation of data, model, and inference layers
- Identity and Access Control for AI Systems

- **Hands On:** Deploying AI Gateway
- **Hands On:** Shadow AI Discovery using Proxy Server

MODULE 12

## Module 12: Data Security in AI Systems

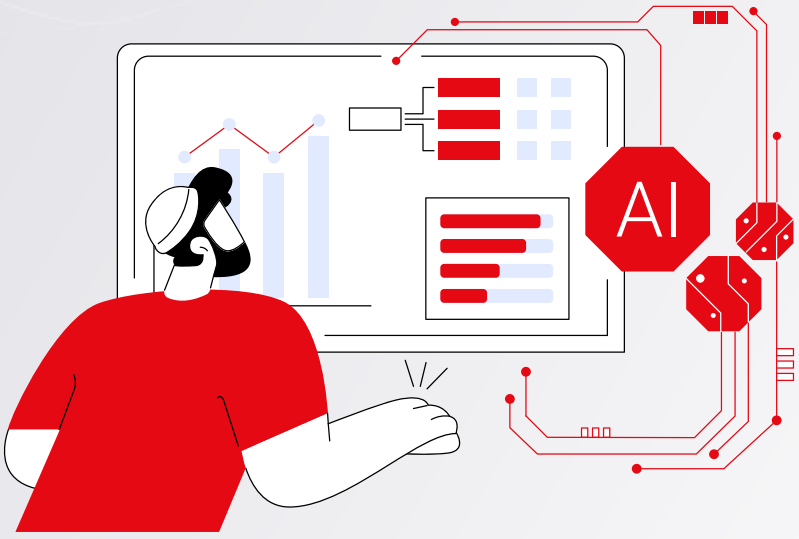
- Data Confidentiality, Integrity, and Availability
- The AI data leakage threat surface
- Secure Data Collection and Ingestion
- Data Sanitization and De-identification Techniques: Data Anonymization, Pseudo-anonymization, Minimization, Masking, Redaction
- Secure Data Processing: Data Classification, Data Quality, and Validation
- Dataset Watermarking
- Privacy Preserving Learning Techniques
- Secure Data Usage During Inference
- Dealing with Data Lag after Model Deployment
- Data Lineage and Provenance Tracking: Audit Logging, Versioning

**Hands On:** Using Microsoft Presidio

## Module 13: AI Governance

- AI Ethics
- Properties of a Responsible AI System
- Data Governance
- Model Governance
- Mapping Infosec controls to NIST AI RMF functions (Govern, Map, Measure, Manage) and ISO 42001 Annex A controls
- EU AI Act risk tiers and their implications for security controls

**Hands On:** **Governance control mapping** exercise



## Module 14: Implementing Governance and Security Controls for AI

- Adversarial Training and Testing
- Techniques to check Sampling and Algorithmic Bias
- Ensuring Explainability in AI Systems
- Data and Model Versioning
- Guardrails for LLMs: System Prompt Hardening, Prompt
- Firewalls (Input and Output Guards)
- Integrating Prompt Injection Detector with LLMs
- Proprietary and open-source guardrails: LLM-Guard, Nemo Guardrails, Guardrails-AI, LlamaGuard
- Applying Rate Limiting and Cost Budgeting in the AI Gateway
- Observability, Monitoring, Evaluation, & Logging Tools for LLMs
- Building a Governance Evidence Pack for an AI Application
- Threat Modelling Frameworks: MITRE ATLAS, MAESTRO Framework for Agentic AI systems
- Security Roles, Responsibilities & Operating Model for AI

- **Hands On:** Deploying a pre-built Prompt Injection Detector and interpreting its alerts
- **Hands On:** Third-party AI Component Supply Chain Assessment

INFOSECTRAIN

Educate. Excel. Empower.

## Contact us

www.infosectrain.com
sales@infosectrain.com

## Follow us on