INFOSECTRAIN
Powered by AI

InfosecTrain Certified AI Systems Professional

CYBERSECURITY

Certification Training

www.infosectrain.ai

INFOSECTRAIN
Powered by AI

Course Highlights

- 40-Hour Hands-On AI Security Training
- Covers AI Basics, Governance, Red & Blue Teaming and Cloud AI
- Labs: Adversarial Attacks, AI Red Teaming, LLM Security
- Cloud AI using Google AI Studio & Vertex AI
- Offensive AI: Recon, Payloads, Phishing, Exploits
- Defensive AI: Detection Models, Email & User Security, SIEM
- Aligned with NIST AI RMF & ISO 42001
- Mentorship & Post-training Support
- Access to Recorded Sessions

INFOSECTRAIN
Powered by AI

About Course

InfosecTrain's Certified AI Systems Professional for Cybersecurity training program offers a comprehensive introduction to securing modern AI systems across the full AI lifecycle. Designed for cybersecurity, cloud, and AI practitioners, this course blends foundational AI learning with practical security applications; ranging from responsible AI design and governance to AI-powered offense, defense, and cloud-based model deployment. Through a structured progression of concepts, guided labs, and real enterprise use cases, participants learn how AI models are built, where they fail, how to defend them, and how to operationalize secure AI workloads in real environments. This training ensures professionals gain the competencies needed to secure ML/LLM systems, enable AI-driven SOC capabilities, and confidently navigate the evolving landscape of AI governance, threats, and enterprise adoption.

INFOSECTRAIN
Powered by AI

Course Objectives

You will be able to:

- Build a holistic understanding of AI systems and their security
- Bridge the gap between AI engineering and cybersecurity
- Train professionals in Responsible AI practices
- Equip teams to secure enterprise AI and LLM deployments
- Enable AI-driven cyber defense capabilities
- Prepare learners for advanced AI security careers

INFOSECTRAIN
Powered by AI

Target Audience

- SOC Analysts, Incident Responders, Cybersecurity Professionals
- Cloud Engineers, Cloud Architects, DevSecOps Teams
- Penetration Testers & Red Teamers
- Data Scientists, ML Engineers, AI Practitioners
- Security Engineers securing ML/LLM systems
- Developers integrating AI in enterprise apps
- Anyone preparing for AI security certifications
- Professionals adopting AI in SOC & security automation

Pre-Requisites

- Understanding of basic networking concepts (TCP/IP, ports, protocols)
- Familiarity with Linux or Kali Linux fundamentals
- Basic knowledge of penetration testing concepts and tools (No AI background required, AI usage is taught within offensive workflows.)

INFOSECTRAIN
Powered by AI

Course Content

AI BASICS

Module 1

Introduction to AI (2 Hours)

- Evolution of AI
- AI Tech Stack and Components of an AI system
- Demystifying AI – Types, Key Terminologies, Learning Types
- Types Of Algorithms
- AI Applications: Predictive AI vs Generative AI
- Understanding AI Model Development
- Understanding NLP
- LLM Architecture

Lab: Understanding Generative AI technically via Open AI Playground and LM Studio

INFOSECTRAIN
Powered by AI

Module 2

Python Basics for Using AI Frameworks and building AI Models (6 Hours) – Whole module uses hands on lab

- Understanding Introductory Programming Concepts: Variables, Datatypes, Keywords, Functions (Pre-defined), Printing, User Inputs, Comments, Operators
- User Defined Functions
- Creating Program Flow with Conditionals and Loops
- Advanced Datatypes: Lists, Tuples, Sets, Dictionary
- Libraries for AI: Data Engineering Phase: Numpy, Pandas, Matplotlib, NLTK (for NLP)
- Model Engineering Phase: Scikit-learn (Machine Learning), Tensorflow (Deep Learning)
- How are AI Systems Built – The AI Model Development Lifecycle:
  - Problem Definition and Decision Boundary Identification
  - Data Sourcing, Trust Boundaries, and Data Preparation Pipelines
  - Model Selection, Design Choices, and Dependency Considerations
  - Training and Fine-tuning within Controlled Environments
  - Validation, Risk Assessment, and Approval Gates
  - Deployment and Inference Architecture (APIs, Access, Exposure)
  - Monitoring, Feedback Loops, and Drift Detection
  - Model Updates, Versioning, and Retirement
- Using No Code Low Code Frameworks for AI Model Development: AutoML
- Using GenAI Tools for AI Model Development

INFOSECTRAIN
Powered by AI

AI GOVERNANCE

Module 3

Considerations for Building a Responsible AI System (2 Hours)

- Why AI Governance Matters: Trust, Ethics, Compliance, Risk
- Key Governance Principles: Safety, Fairness, Explainability, Privacy, Robustness, Auditability
- Regulatory Frameworks, Standards and Compliance: NIST AI RMF, ISO 42001
- AI Regulations and Guidelines Worldwide: EU AI Act, OECD AI Principles

INFOSECTRAIN
Powered by AI

Module 4

AI Cloud Governance (4 Hours)

- Why Cloud Complicates AI Governance: Scalability, Multi-region Data, Opaque AI Services
- The Shared Responsibility Model: What's Governed by Cloud Provider vs. Customer in AI Workloads
- Mapping Existing AI Governance Principles (Fairness, Explainability, Privacy) to Cloud Controls (IAM, DLP, Encryption, Audit Logs)
- Data Governance: Cloud Data Lineage, Provenance, and Labeling
- Accountability, Managing Data Residency and Sovereignty (Multi-region Storage Policies)
- Model Governance: Model Versioning, Approval, and Explainability Tracking
- Cloud Risk, Compliance & Audit Controls

INFOSECTRAIN
Powered by AI

AI RED TEAMING

Module 5

Using AI for Cyber Offense (3 Hours)

- Automated Reconnaissance: Passive Recon Script Generation, Company Profiling
- Vulnerability Scanning: Automating NMAP Scan Task
- Generation and Scan Report Assessment
- Payload Generation & Obfuscation
- Phishing & Social Engineering: Email Generation and Pretext Building using AI
- Exploitation Assistance: Explain CVEs, Convert Exploit POCs, Automate Shell Handling using AI

Tools: OpenAI, Shell GPT, Open-Source Models from Hugging Face and Ollama

INFOSECTRAIN
Powered by AI

Module 6

Pentesting AI Systems (4 Hours)

- AEvasion, Poisoning and Theft
- ML Top 10
- LLM Top 10

Lab: Pentesting ML and DL Models with FGSM and ART

Lab: LLM Vulnerability Scanning using Garak

INFOSECTRAIN
Powered by AI

AI BLUE TEAMING

Module 7

Building AI-based Security Controls using the AI Model Development Lifecycle (6 Hours) (Whole module uses hands on lab)

- Security Controls for Network Security
- Security Controls for Email Security
- Security Controls for User Security
- Security Controls for Endpoint Security

Module 8

Using AI for Security Analysis (4 Hours) (Whole module uses hands on lab)

- Integrating Custom Models with SIEM tools (ELK stack)
- Using AI for Log Analysis
- Using AI Tools and Models for Security Analysis
- Agentic AI (Crew AI) for SOC Environment

INFOSECTRAIN
Powered by AI

Module 9

Securing AI Systems (5 Hours)

- Threat Modelling of AI Systems (Lab: MITRE ATT&CK and ATLAS, STRIDEGPT)
- Model Versioning and Monitoring (Lab: MLFLOW)
- Model Explainability (Lab: LIME and SHAP)
- Model Fairness (Lab: What-if tool)
- Securing ML and DL Models with Adversarial Training (Lab: ART, Cleverhans)
- Rate Limiting (Lab: Building Rate Limiter for LLMs using Langchain)
- Applying Guardrails on LLMs to Protect Against Adversarial Attacks
- (Lab: LLM-Guard, Guardrails AI, Models from Hugging Face)

INFOSECTRAIN
Powered by AI

AI AND CLOUD

Module 10

Using the Cloud Environment to Build AI Models (4 Hours)

- Fundamentals of using AI in the Cloud and Deploying AI on the Cloud
- Google AI Studio Essentials
- Introduction to Vertex AI
- Vertex AI Pipelines

Lab: Building & Deploying an ML Model on GCP using Vertex Ala

INFOSECTRAIN
Powered by AI

Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on