INFOSECTRAIN

AI-Powered Cybersecurity

Online Training Course

Course Highlights

40-Hour Instructor-led Training

Career-oriented Skill-based Course

Highly Interactive & Dynamic Sessions

Learn from Industry Experts

Learn with Real-World Scenarios

Access to Recorded Sessions

Extended Post Training Support

Career Guidance and Mentorship

Immersive Learning

About Course

InfosecTrain's **AI-Powered Cybersecurity Training Course** is a comprehensive program tailored to meet the demands of today's rapidly evolving digital landscape. The course delves into integrating **Artificial Intelligence with cybersecurity**, providing participants with advanced skills to detect, analyze, and counter cyber threats efficiently. The course covers the fundamental concepts of Python programming, which is crucial for participants to learn and apply due to its relevance and versatility in AI and cybersecurity.

Through hands-on exercises, case studies, and industry-relevant scenarios, learners gain practical experience to tackle real-world challenges. Designed for IT Professionals, Cybersecurity Specialists, Data Engineers, and enthusiasts, the course provides learners a competitive edge to master advanced AI technologies to safeguard digital ecosystems effectively and sustainably.

Course Objectives

- Develop a strong foundation in Python programming for cybersecurity applications.
- Understand AI fundamentals and their role in enhancing cybersecurity.
- Apply supervised and unsupervised machine learning for threat detection.
- Explore neural networks and deep learning for advanced cybersecurity solutions.
- Analyze and defend against adversarial attacks on AI models.
- Implement AI-driven endpoint protection for proactive threat mitigation.
- Leverage NLP for phishing detection, log analysis, and threat intelligence.
- Strengthen identity, access management, and data protection using AI.
- Use reinforcement learning and GANs for attack simulations and defense strategies.
- Explore generative AI and LLMs for innovative cybersecurity applications.

Target Audience

- Beginners in IT field
- Any IT professional who wants to power their transition to cybersecurity with AI
- Beginners in Cybersecurity
- Cybersecurity professionals who want to know the basics of using AI to enhance cybersecurity
- Data Scientists, Data Engineers, and AI Engineers who want to transition to cybersecurity

Pre-requisites

Programming fundamentals and basic cybersecurity concepts would be beneficial, though we will revisit these basics in this course.

Course Content

Module 1 Foundations of Python Programming

- Python Fundamentals and Core Concepts
- Introduction to Basic Python Commands
- Python Variables, Operators, Datatypes (Lists, Tuples, Dictionaries), Modules, Functions, Control Flow, Randomness, Regular Expressions
- Python Libraries for AI

PRACTICAL: Using Numpy, Pandas, Matplotlib, Scikit-learn, Tensorflow, Keras, PyTorch

PRACTICAL: Hands-on with Jupyter Notebook, Google Colab, ChatGPT, Claude, etc.

Module 2 Introduction to AI

- What is AI?
- History and Development of AI
- AI – Current Scenario

AI Applications

- ✓ Descriptive, Predictive, Prescriptive, and Generative applications
- ✓ Classification and Regression
- ✓ Automation
- ✓ Reactive vs Predictive Analysis
- ✓ Anomaly Detection
- ✓ Behavior Analysis

AI Types and Categories

- ✓ Machine Learning and its types: Supervised, Unsupervised, Semi-supervised, and Reinforcement Learning

DEEP LEARNING: Perceptrons, MLP, ANN, CNN, RNN, LSTM, GAN
Natural Language Processing and LLMs

Challenges with AI

- ✓ Context and Alignment
- ✓ Explainable AI
- ✓ Hallucinations and Grounding
- ✓ AI Bias
- ✓ Regulation and Compliance
- ✓ AI Ethics, Data Privacy, Human Rights, Intellectual Property Issues
- ✓ NIST AI Risk Management Framework

- **Data Science and Feature Engineering**
  - ✓ Data Pre-processing: Data Collection, Cleaning, Integration, and Transformation
  - ✓ Feature Engineering: Creation, Selection, and Extraction
  - ✓ Dimensionality Reduction
  - ✓ Feature Scaling, Normalization, and Standardization
  - ✓ Encoding Techniques
  - ✓ Handling Imbalanced Data
  - ✓ Data Quality Assessment

Module 3 Introduction to Cybersecurity

- Basic Security Concepts and Cybersecurity Roles
- Threat Types and Landscape
- Traditional Cybersecurity vs AI-powered Cybersecurity
- Using AI for Penetration Testing
- AI in Cybersecurity Applications
  - ✓ Access Controls
  - ✓ Identity and Access Management (IAM)
  - ✓ Threat Detection and Prevention Techniques
  - ✓ Vulnerability Assessment
  - ✓ Threat Intelligence, Hunting, and Analysis
  - ✓ Monitoring with SIEM and SOAR
  - ✓ Endpoint Protection - EDR and XDR
  - ✓ Incident Response
  - ✓ Digital Forensics

- Case Studies

PRACTICAL: Machine Learning Lifecycle

DOMAIN-SPECIFIC PREPROCESSING: Security Log, Network Packet, Spam/Phishing, Malware Binary, User Behavior, and Authentication Data Preprocessing

Module 4 Adversarial Attacks on AI

- Types of Attacks
  - ✓ Evasion, Poisoning, Model Extraction
- OWASP Machine Learning Security Top Ten
- Mitigation Techniques

Module 5 Supervised Machine Learning for Cybersecurity

- Classification and Regression Problems and Understanding ML Algorithms: Linear Regression, Logistic Regression, SVMs, Decision Trees, Naive Bayes

PRACTICAL: Implementing a Network Scanner (Scapy Library)

- Network Traffic Monitoring and Log Collection
- Converting Network Logs into Datasets

PRACTICAL: Spam/Phishing Detection

- Understanding Classification Reports and Confusion Matrix
- Optimization Strategies and Ensemble Learning: Bagging, Boosting, Stacking

Module 6 Unsupervised Machine Learning for Cybersecurity

- Unsupervised ML Algorithms
- Model creation using Clustering Algorithms

PRACTICAL: Network Anomaly Detection

- Types of Network Attacks and Best ML Algorithms for different scenarios

PRACTICAL: Botnet Detection

PRACTICAL: Intrusion Detection System

Module 7 Neural Networks and Deep Learning for Cybersecurity

- **Neural Network Basics**
    - ✓ Perceptrons, Activation Functions, Gradient Descent, Backpropagation
    - ✓ Multi-Layer Perceptrons

PRACTICAL: Building a Spam Detector using perceptrons

- **Deep Learning Algorithms**
    - ✓ Feedforward Neural Networks (FFNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM), Convolutional Neural Networks (CNNs)
    - ✓ Python Libraries for Deep Learning

PRACTICAL: Handwritten digit recognition

Module 8 Protecting Endpoints Using AI

- Malware Detection
- Malware Types and Detection Tools

PRACTICAL: Signature Detection with Hash Values

- Rule-based Malware Detection using YARA

PRACTICAL: Heuristics-based Detection with PE File Headers

- Dynamic Behavior Analysis with Cuckoo Sandbox

PRACTICAL: Malicious URL Detection

- Decision Trees and Random Forest Algorithms, Gradient Boost, and AdaBoost Techniques
- Polymorphic Malware Detection using HMMs
- Malware Detection with Deep Learning

PRACTICAL: Malware Detection from Images using CNNs

Module 9 Natural Language Processing (NLP)

- **Text Processing Basics:** Tokenization, Stemming/Lemmatization, Stop Words, N-grams
- **Traditional NLP**: Bag of Words, TF-IDF, Word2Vec, GloVe

PRACTICAL: Spam Detection using NLP (NLTK Library, TF-IDF)

PRACTICAL: System Log Threat Detection

Module 10 Identity, Access Management, and Data Protection using AI

- User Identification and Authentication
- UEBA, Authentication Abuse Prevention

PRACTICAL: Password Strength Determination

PRACTICAL: Keystroke Recognition Authentication

- Usability vs Security

PRACTICAL: Biometric Authentication using Facial Recognition

- Dimensionality Reduction, Eigenvalues, Eigenvectors, Eigenfaces

PRACTICAL: ML-Based Steganography for Data Protection

- HIPAA Data Breaches: Exploration and Visualization

Module 11 Threat Hunting, Incident Response, and Forensics using AI

- **Methodologies and Models**: Cyber Kill Chain, Diamond Model of Intrusion Analysis
- Predictive Analytics in Incident Response
- Digital Forensics

PRACTICAL: AI-assisted Threat Hunting and Forensics using ELK Stack

Module 12 Reinforcement Learning and Generative Adversarial Networks (GANs)

- Introduction to GANs
- Generators, Discriminators, Loss Functions, Training Process
- Synthetic Data Generation

PRACTICAL: Pen Testing Networks with GANs

- Bypassing Malware Detectors with MalGANs
- Bypassing Machine Learning Systems with Reinforcement Learning

Module 13 Introduction to Generative AI and LLMs

- **History and Development:** Transformers Architecture, Attention, BERT, GPT Models
- Prompt Engineering concepts
- **Using Generative AI in Cybersecurity**
  - ✓ Governance, Risk, and Compliance
  - ✓ Security Awareness, Code Analysis, and Secure Development
  - ✓ Vulnerability Assessment, Red Teaming, and Penetration Testing
  - ✓ Threat Monitoring and Detection
  - ✓ Incident Response
- OWASP Top 10 for LLM Applications

Module 14 Implementing AI Security Controls

- Data Lifecycle Security: Encryption, Anonymization, Access Controls
- Secure AI Model Development and Deployment
- AI Robustness and Validation
- AI System Monitoring and Auditing

PRACTICAL: MITRE ATLAS

INFOSECTRAIN

Educate. Excel. Empower.

Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on