multisoft
Systems

CompTIA SecAI+ Training

COURSE CONTENT

GET IN TOUCH

Multisoft Systems
B - 125, Sector - 2, Noida

(+91) 9810-306-956

info@multisoftsystems.com

www.multisoftsystems.com

About Multisoft

Train yourself with the best and develop valuable in-demand skills with Multisoft Systems. A leading certification training provider, Multisoft collaborates with top technologies to bring world-class one-on-one and certification trainings. With the goal to empower professionals and business across the globe, we offer more than 1500 training courses, which are delivered by Multisoft's global subject matter experts. We offer tailored corporate training; project Based Training, comprehensive learning solution with lifetime e-learning access, after training support and globally recognized training certificates.

About Course

CompTIA SecAI+ Training by Multisoft Systems is designed to help professionals understand the rapidly evolving field of artificial intelligence security and its role in modern cybersecurity strategies. As organizations increasingly adopt AI and machine learning technologies, protecting these systems from cyber threats, vulnerabilities, and misuse has become critical.

Module 1: Introduction to Artificial Intelligence Security

- ✓ Overview of Artificial Intelligence and Machine Learning
- ✓ Importance of AI Security in Modern Cybersecurity
- ✓ AI Security Threat Landscape
- ✓ Key Terminologies in AI and ML Security
- ✓ AI Systems and Their Components
- ✓ Security Challenges in AI-driven Environments

Module 2: Fundamentals of Machine Learning and AI Models

- ✓ Types of Machine Learning (Supervised, Unsupervised, Reinforcement Learning)
- ✓ AI Model Development Lifecycle
- ✓ Data Collection and Preparation
- ✓ Training, Testing, and Validation of AI Models
- ✓ AI Model Deployment and Monitoring
- ✓ Common AI Frameworks and Platforms

Module 3: AI Threats and Vulnerabilities

- ✓ Adversarial Machine Learning Attacks
- ✓ Data Poisoning Attacks
- ✓ Model Evasion and Manipulation Techniques
- ✓ Model Theft and Inference Attacks
- ✓ Insider Threats in AI Systems
- ✓ Identifying AI-specific Vulnerabilities

Module 4: Securing AI Data and Training Pipelines

- ✓ Data Integrity and Data Protection Techniques
- ✓ Secure Data Collection and Storage
- ✓ Data Privacy and Confidentiality in AI

- ✓ Securing AI Training Pipelines
- ✓ Managing Data Bias and Data Quality Risks
- ✓ Data Governance for AI Systems

Module 5: AI Model Security and Protection

- ✓ Protecting AI Algorithms and Models
- ✓ Model Hardening Techniques
- ✓ Secure Model Deployment Practices
- ✓ Access Control and Authentication for AI Systems
- ✓ AI Model Monitoring and Threat Detection
- ✓ Preventing Model Manipulation and Exploitation

Module 6: Risk Management and Governance in AI Security

- ✓ AI Risk Assessment and Threat Modeling
- ✓ Security Policies for AI Systems
- ✓ Compliance and Regulatory Considerations
- ✓ Ethical AI and Responsible AI Practices
- ✓ Governance Frameworks for AI Security
- ✓ Security Auditing and Reporting

Module 7: AI Security Operations and Incident Response

- ✓ Monitoring AI Systems for Security Threats
- ✓ Detecting Anomalies in AI Environments
- ✓ Incident Response Strategies for AI Attacks
- ✓ Threat Intelligence for AI Security
- ✓ Managing AI Security Breaches
- ✓ Recovery and Remediation Techniques

Module 8: Integrating AI Security with Enterprise Cybersecurity

- ✓ AI Security in Cloud Environments
- ✓ DevSecOps for AI Applications
- ✓ Integration with Security Operations Centers (SOC)
- ✓ Automation and AI-driven Security Tools
- ✓ Best Practices for Enterprise AI Security

Module 9: Case Studies and Real-world AI Security Scenarios

- ✓ Analysis of AI Security Breaches
- ✓ Real-world Adversarial Attack Examples
- ✓ Risk Mitigation Strategies
- ✓ AI Security Implementation Case Studies