

AI+ Security Expert

OEM: AI CERTs • Duration: 5 Days (40 hrs) • Code: AT-2102

COURSE MODULES & TOPICS

At a Glance: Course + Exam Overview

- Instructor-Led: 5 days (live or virtual)
- Self-Paced: 40 hours of content

Who Should Enroll?

- **Cybersecurity Professionals:** Professionals who want to stay updated on the latest AI-driven security tools, technologies, and techniques to strengthen cybersecurity practices.
- **IT Professionals and System Administrators:** Those who want to use AI capabilities to detect, analyze, and respond to security threats more effectively and efficiently.
- **Cloud Architects and Engineers:** Professionals who want to integrate AI-powered security solutions into cloud architectures and enhance the protection of cloud environments.
- **Risk Management Specialists:** Those who want to apply AI-driven approaches to identify, assess, and mitigate cybersecurity risks.
- **Business Leaders and Decision Makers:** Professionals who want to understand the role of AI in cybersecurity and make informed decisions about security investments and strategies.
- **Software Developers:** Developers who want to understand AI integration in security tools, applications, and secure software development practices.
- **Security Consultants and Advisors:** Professionals who want to gain advanced knowledge of AI technologies to provide strategic cybersecurity guidance and recommendations.

Skills You'll Gain

- AI-driven threat detection and cybersecurity analysis
- Machine learning applications in security operations
- Python-based security automation and tool development
- AI-powered malware and email threat detection
- Network anomaly detection and risk analysis
- AI-based authentication and security solutions
- Penetration testing using AI techniques
- Responsible AI, security governance, and compliance practices
- Designing AI-powered cybersecurity solutions through practical projects

What You'll Learn

- You will learn AI and cybersecurity fundamentals, AI-driven threat detection, vulnerability management, ethical considerations, regulatory requirements, and resilient security strategies.
- You will learn Python programming for security automation, data analysis, AI scripting, visualization, and developing cybersecurity tools.
- You will explore ML-based anomaly detection, behavior analysis, predictive threat identification, data protection, and advanced cybersecurity applications.
- You will learn AI-powered email security, phishing detection, deep learning models, automation techniques, and email threat response solutions.
- You will learn AI-based malware detection, neural networks, model development, real-time mitigation, and malware analysis techniques.
- You will explore AI-based network anomaly detection, model implementation, deployment strategies, and challenges in handling advanced threats.
- You will learn AI-driven authentication, biometric recognition, behavioral analysis, adaptive security controls, and emerging authentication trends.
- You will explore GAN applications in cybersecurity, including threat simulation, synthetic attack generation, vulnerability detection, and defense improvement.
- You will learn AI-enhanced penetration testing, cyberattack simulation, automated vulnerability identification, and improved security assessment techniques.
- You will apply AI cybersecurity concepts through real-world projects involving anomaly detection, email security, IoT protection, behavioral biometrics, and threat intelligence.

Prerequisites

- Interest in AI Technologies : Interest in learning about AI technologies such as ML, DL, and NLP.
- Tech Comfort : Basic knowledge about the fundamentals of computer science.
- Learning Mindset : Curiosity and openness to learn about new concepts and technologies.
- Ethical Awareness : Willingness to explore ethical considerations and legal frameworks surrounding the use of AI and data privacy.

Exam Blueprint:

- Introduction to Artificial Intelligence (AI) and Cyber Security - 8%
- Python Programming for AI and Cybersecurity Professionals - 10%
- Application of Machine Learning in Cybersecurity - 10%
- Detection of Email Threats with Artificial Intelligence (AI) - 11%
- Artificial Intelligence (AI) Algorithm for Malware Threat Detection - 11%
- Network Anomaly Detection using Artificial Intelligence (AI) Techniques - 11%
- User Authentication Security with Artificial Intelligence (AI) - 11%
- Generative Adversarial Network (GAN) for Cyber Security - 11%
- Penetration Testing with Artificial Intelligence - 11%
- Capstone Project - 6%

Choose the Format That Fits Your Schedule

- High-Quality Videos, E-book (PDF & Audio), and Podcasts
- AI Mentor for Personalized Guidance
- Quizzes, Assessments, and Course Resources
- Online Proctored Exam with One Free Retake
- Comprehensive Exam Study Guide

- 5 days of intensive training with live demos
- Real-time Q&A, peer collaboration, and hands-on labs
- Led by AI Certified Trainers and delivered through Authorized Training Partners
- ~40 hours of on-demand video lessons, e-book, podcasts, and interactive labs
- Learn anywhere, anytime, with modular quizzes to track progress