



course : AI Cybersecurity: Attack and Defend

City : Kuala Lumpur
Start Date : 2025-11-24
Period : 1 Week

Hotel : Kuala Lumpur
End Date : 2025-11-28
Price : 3950 \$

HighPoint Training and Management Consultancy
هاي بوينت للتدريب والاستشارات الإدارية

info@highpointtc.com ✉
www.Highpointtc.com 🌐
UAE - Dubai 📍
+971 50 360 6133 📞

Course Overview

As artificial intelligence (AI) becomes increasingly integrated into digital systems, the cybersecurity landscape evolves with it. AI technologies introduce both new opportunities and unique vulnerabilities, making it essential for professionals to understand how AI systems can be exploited and how to defend them.

This AI Cybersecurity: Attack and Defend training course equips participants with the knowledge and practical skills needed to identify, simulate, and mitigate AI-driven cyber threats, covering areas such as adversarial attacks, AI system vulnerabilities, threat modeling, and defensive strategies. Through hands-on labs and real-world scenarios, participants will develop the expertise to safeguard AI-enabled systems in dynamic environments.

Course Objectives

By the end of this training course, participants will be able to:

- Understand AI architectures, models, and potential security risks
- Identify and simulate adversarial attacks against AI systems
- Analyze vulnerabilities in AI-enabled applications and networks
- Design and implement defensive AI strategies to mitigate attacks
- Apply AI-based cybersecurity tools for threat detection and response
- Evaluate and improve organizational AI security policies
- Conduct practical incident response exercises for AI security breaches

Target Audience

This course is ideal for professionals responsible for AI system security, IT infrastructure, and organizational cybersecurity, including:

- Cybersecurity analysts and engineers
- AI/ML developers and data scientists
- IT security managers and risk officers
- Incident response teams
- Network and system administrators
- Compliance and governance specialists

Methodology

The course combines:

- Instructor-led lectures and conceptual explanations
- Interactive discussions on emerging threats and mitigation strategies
- Hands-on labs simulating AI attacks and defensive techniques
- Case studies on real-world AI cybersecurity incidents
- Scenario-based group exercises to reinforce defensive planning and incident response

Course Outline

- Day 1 – Fundamentals of AI and Cybersecurity
 - Overview of AI systems, machine learning, and neural networks
 - Understanding AI vulnerabilities and threat surfaces
 - Introduction to cybersecurity principles for AI
 - Case studies of AI-related cyber incidents
- Day 2 – Adversarial Attacks on AI Systems
 - Types of adversarial attacks: evasion, poisoning, and model inversion
 - Techniques to simulate AI system attacks
 - AI threat modeling and risk assessment
 - Hands-on lab: launching controlled adversarial attacks
- Day 3 – AI Security and Defensive Strategies
 - Defensive AI models and anomaly detection
 - Implementing robust AI pipelines
 - Adversarial training and model hardening techniques
 - Hands-on lab: defending AI systems against attacks
- Day 4 – Monitoring, Detection, and Incident Response
 - AI-enabled cybersecurity monitoring tools
 - Detection of malicious AI activity and anomaly response
 - Incident response frameworks for AI security breaches
 - Workshop: simulated AI cybersecurity incidents and response
- Day 5 – AI Governance, Compliance, and Emerging Threats
 - Regulatory and compliance considerations for AI systems
 - Ethical and legal aspects of AI security
 - Emerging AI threats and trends
 - Capstone exercise: end-to-end attack and defend simulation

Course review and certification of completion

Certificates

On successful completion of this training course, HighPoint Certificate will be awarded to the delegates. Continuing Professional Education credits (CPE): In accordance with the standards of the National Registry of CPE Sponsors, one CPE credit is granted per 50 minutes of attendance.