AI in Cybersecurity

1 – 5 March 2027
Kuala Lumpur (Malaysia)

UK Traininig
PARTNER



www.blackbird-training.com

AI in Cybersecurity

Ref: 3255157_189656 **Date:** 1 – 5 March 2027 **Location:** Kuala Lumpur (Malaysia) **Fees:** 4900 GBP

Introduction

This course explores the integration of Artificial Intelligence AI and Machine Learning ML in cybersecurity, focusing on how AI can be leveraged to predict, detect, and respond to cyber threats effectively. Participants will gain essential knowledge of AI-driven security systems, including Deep Learning, predictive analytics, and real-world applications in cyber defense.

Course Objectives

- Understand the fundamentals of AI, ML, and Deep Learning in the context of cybersecurity.
- Identify the role of AI in threat detection, prevention, and incident response.
- Apply AI models to real-world cybersecurity problems.
- Evaluate the strengths and limitations of AI in combating cybercrime.
- Develop strategies to integrate AI tools into existing cybersecurity frameworks.

Course Outlines

Day One: Fundamentals of AI & Cybersecurity

- Cybersecurity landscape and challenges.
- Basics of Artificial Intelligence, Machine Learning, and Deep Learning.
- Role of AI in modern cybersecurity.
- Types of cyber threats addressed by AI.
- Case studies of AI applications in cyber defense.

Day Two: AI Techniques in Threat Detection

- Machine Learning models for Intrusion Detection Systems IDS.
- Anomaly detection vs. signature-based detection.
- Using AI for malware and phishing detection.
- Natural Language Processing NLP in email security.
- Hands-on lab: training a simple ML model for threat detection.



Day Three: AI in Incident Response & Prevention

- AI for automated threat hunting.
- Predictive analytics in cybersecurity.
- Real-time incident response with AI.
- AI-driven risk assessment models.
- Hands-on lab: building an automated response workflow.

Day Four: Advanced Applications of AI in Cybersecurity

- Deep Learning for network traffic analysis.
- AI in cloud security and IoT protection.
- AI-powered fraud detection systems.
- Ethical hacking with AI tools.
- Hands-on lab: detecting anomalies in network logs.

Day Five: Future Trends, Challenges & Implementation

- Limitations and risks of AI in cybersecurity bias, adversarial attacks.
- Legal, ethical, and regulatory considerations.
- Integrating AI into existing cybersecurity frameworks.
- Future trends: Generative AI, Zero-Trust, and autonomous defense.
- Capstone exercise: designing an AI-based cybersecurity strategy.

Why Attend this Course: Wins & Losses!

- Gain advanced knowledge of AI, ML, and Deep Learning in cybersecurity.
- Learn to use predictive analytics and AI-driven tools for advanced threat detection.
- Build hands-on experience in malware detection, phishing defense, and automated incident response.
- Understand future innovations such as Generative AI, Zero-Trust, and autonomous defense.

Conclusion

Artificial Intelligence is transforming the future of cybersecurity by enabling early threat detection, automated response, and more resilient defense systems. Through this course, participants will gain the knowledge, tools, and strategies to design and implement innovative AI-based cybersecurity solutions. This is your opportunity to lead the way in protecting digital assets and combating cyber threats with the power of AI.

