BLACKBIRD FOR TRAINING

AI-Driven Threat Detection and Response

14 – 18 June 2027
Kuala Lumpur (Malaysia)

UK Traininig
PARTNER

www.blackbird-training.com

AI-Driven Threat Detection and Response

Ref: 3255274_336975 **Date:** 14 – 18 June 2027 **Location:** Kuala Lumpur (Malaysia) **Fees:** 4900 GBP

Introduction

In an era where cyber threats are advancing faster than traditional defense mechanisms, artificial intelligence AI has become a game-changer in cybersecurity. The integration of AI-Driven Threat Detection and Response has transformed how organizations detect, analyze, and mitigate digital risks. Rather than relying solely on reactive systems, AI enables predictive, adaptive, and automated security operations that can identify anomalies in real time and respond before damage occurs.

This course is designed to provide professionals with deep insights into how AI is reshaping cybersecurity strategy and operations. Participants will explore the technologies, models, and frameworks that drive AI-powered detection systems, learn how to integrate AI into their existing security infrastructure, and develop the skills needed to create a proactive and resilient defense posture.

Course Objectives

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

- Understand the fundamentals of artificial intelligence in cybersecurity applications.
- Analyze the limitations of traditional threat detection systems and how AI addresses them.
- Implement AI algorithms for anomaly detection, behavior analysis, and intrusion prevention.
- Integrate machine learning models within security information and event management SIEM systems.
- Design automated response strategies to mitigate cyberattacks effectively.
- Evaluate ethical considerations and governance in AI-based security systems.
- Apply AI solutions to enhance situational awareness and decision-making in cyber defense operations.

Course Outlines

Day 1: Introduction to AI in Cybersecurity

- Overview of AI's role in modern security ecosystems.
- Understanding machine learning and deep learning in threat detection.
- Comparison between rule-based and AI-driven approaches.
- Data as the foundation for AI-powered security intelligence.
- Challenges of integrating AI into legacy systems.

Day 2: Machine Learning Models for Threat Detection

- Types of machine learning models: supervised, unsupervised, and reinforcement learning.
- Training AI models to detect anomalies and malicious activities.
- Identifying false positives and improving model accuracy.
- Feature engineering for cybersecurity datasets.
- Case examples of successful AI-based threat detection deployments.

Day 3: Real-Time Threat Monitoring and Analysis

- Leveraging big data analytics for continuous threat monitoring.
- Correlating events from multiple data sources using AI.
- AI in intrusion detection and prevention systems IDPS.
- Detecting insider threats through behavioral analysis.
- Visualizing and interpreting AI-driven security insights.

Day 4: Automated Incident Response and Mitigation

- Building automated playbooks for incident response.
- AI-powered response orchestration across hybrid environments.
- Integrating AI with endpoint detection and response EDR tools.
- Adaptive defense strategies using predictive modeling.
- Reducing mean time to detect MTTD and mean time to respond MTTR.

Day 5: Implementation Strategy and Assessment

- Developing a roadmap for AI adoption in cybersecurity frameworks.
- Evaluating readiness and infrastructure maturity.
- Managing data privacy, ethics, and algorithmic transparency.
- Measuring performance and ROI of AI-based threat management systems.
- Final assessment: creating an AI-driven security model for a simulated enterprise environment.

Why Attend this Course: Wins & Losses!

- Gain in-depth knowledge of how AI transforms cybersecurity operations.
- Learn to design and implement AI-powered threat detection models.
- Develop the ability to predict and prevent cyberattacks using advanced analytics.
- Improve the speed and accuracy of incident response through automation.
- Understand how to manage risks associated with AI adoption and data ethics.
- Enhance decision-making using intelligent security insights and behavioral analytics.
- Strengthen your organization’s overall cyber resilience and adaptive defense strategy.
- Stay ahead of emerging threats with next-generation AI defense capabilities.

Conclusion

The rise of AI-Driven Threat Detection and Response marks a new era in cybersecurity—one where proactive intelligence and automation are key to staying secure in an increasingly hostile digital environment. By combining human expertise with machine learning capabilities, organizations can achieve faster detection, precise threat classification, and autonomous response actions that minimize risk and downtime.

This course equips professionals with the practical knowledge and strategic frameworks needed to integrate AI into their cybersecurity architecture effectively. As threats continue to evolve, leveraging AI will no longer be an option—it will be a fundamental requirement for maintaining trust, compliance, and operational resilience in the digital age.