

Information Security, Cyber Security & AI Mastery Course

26 October – 6 November 2026
Cape Town (South Africa)

UK Training

PARTNER



Information Security, Cyber Security & AI Mastery Course

Ref: 321817_147542 **Date:** 26 October – 6 November 2026 **Location:** Cape Town (South Africa) **Fees:** 7600 GBP

Why This Course

In an era of rapidly evolving digital threats, organizations need professionals who can bridge traditional cybersecurity practices with cutting-edge AI solutions. This 10-day intensive course equips participants with the skills to detect, prevent, and respond to cyber threats using both conventional and AI-powered security strategies. Through a combination of theoretical insights and hands-on exercises, attendees will be prepared to tackle modern security challenges effectively.

What You'll Learn and Practice

Participants will explore:

- Core principles of information and cyber security
- Threat detection and risk mitigation techniques
- AI and machine learning applications for enhanced security operations
- Integration of AI into security policies and organizational infrastructure
- Ethical and privacy considerations in AI-powered cybersecurity

By participating in this course, you will:

- Develop practical expertise in AI-driven threat detection and response
- Strengthen your organization's cybersecurity posture using advanced tools
- Implement AI-powered solutions for malware prevention, network protection, and SIEM
- Apply ethical AI practices to ensure responsible and transparent security operations
- Design a comprehensive AI-enhanced security solution through a capstone project

Program Flow

Day 1: Foundations of Information Security

- Introduction to information security concepts
- CIA triad: Confidentiality, Integrity, and Availability
- Security policies and standards
- Risk management fundamentals

UK Training

PARTNER

A graphic of a chessboard with several chess pieces. A gold king piece is prominent in the foreground, with a silver pawn and a silver knight behind it. The board is checkered, and there are concentric circles in the background.

Day 2: Cyber Security Essentials

- Cyber threat landscape overview
- Network security principles
- Endpoint security and access control
- Incident response basics

Day 3: Cryptography and Data Protection

- Encryption algorithms and protocols
- Public Key Infrastructure PKI
- Data classification and handling
- Privacy regulations and compliance

Day 4: Artificial Intelligence Fundamentals

- Introduction to AI and machine learning
- Supervised and unsupervised learning
- Neural networks and deep learning
- AI applications in cybersecurity

Day 5: AI-Powered Threat Detection

- Anomaly detection using machine learning
- Behavioral analytics and user profiling
- AI-driven intrusion detection systems
- Threat intelligence and AI

Day 6: Security Information and Event Management SIEM

- SIEM architecture and components
- Log collection and normalization
- Correlation rules and alerts
- AI-enhanced SIEM capabilities

Day 7: AI in Malware Analysis and Prevention

- Machine learning for malware classification
- Automated malware analysis techniques
- AI-powered antivirus solutions
- Zero-day threat detection using AI

UK Training

PARTNER

A graphic of a chessboard with several chess pieces (a king, a queen, and a pawn) positioned on it. The board is checkered, and the pieces are gold and silver. The text 'UK Training PARTNER' is overlaid on the board.

Day 8: AI-Driven Network Security

- Network traffic analysis using AI
- DDoS mitigation with machine learning
- AI-based firewall and IPS systems
- Software-defined networking and AI

Day 9: Ethical AI and Security

- Bias and fairness in AI security systems
- Explainable AI for security decisions
- Privacy-preserving machine learning
- Ethical considerations in AI-powered surveillance

Day 10: Future Trends and Capstone Project

- Emerging AI technologies in cybersecurity
- Quantum computing and post-quantum cryptography
- AI-human collaboration in security operations
- Capstone project: Designing an AI-enhanced security solution

Training Methodology

- Interactive lectures and expert-led discussions
- Hands-on labs for AI, threat detection, and SIEM tools
- Case studies and real-world cybersecurity scenarios
- Group exercises and capstone project for applied learning

Beyond the Course

Participants will leave with:

- The ability to implement AI-driven threat detection systems
- Skills to enhance existing security infrastructure with AI capabilities
- Knowledge to evaluate and select appropriate AI security solutions
- Strategies to integrate AI into organizational security policies and procedures
- A completed capstone project demonstrating practical AI-enhanced security solutions

A graphic of a chessboard with several pawns and a king piece. The text 'UK Training' is above 'PARTNER' which is in large, bold, black letters.

UK Training
PARTNER