An Intensive 3-day Training Course

AI Powered Risk & Fraud Detection

Securing Your Organization's Future: Mastering AI for Advanced Threat Detection and Prevention

Classroom sessions

Date	Venue	Fees
18-20 June 2025	Online	R 8,999

INTRODUCTION

This training course equips senior risk, compliance, and security professionals with advanced knowledge of AI-powered detection systems, their limitations, and potential vulnerabilities. In an era where digital threats evolve at unprecedented speeds, artificial intelligence has become a critical tool in risk management and fraud detection.

Participants will learn to balance the powerful capabilities of AI in detecting threats with an understanding of its potential weaknesses and exploitation points.

The training course provides a dual perspective: leveraging AI's strengths in identifying patterns and anomalies while remaining vigilant about emerging AI-enabled threats and attack vectors. This training course provides a comprehensive approach to both defensive and offensive considerations in AI security. Participants will learn not only how to implement AI for detection but also understand how adversaries might attempt to manipulate or bypass these systems.

This **Luthando Skills** AI Powered Risk & Fraud Detection training course will highlight:

- Balancing technical and strategic elements
- Addresses both opportunities and threats
- AI risk management
- AI compliance requirements

TRAINING OBJECTIVES

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

- Understand how to manage AI-based risk and fraud detection systems
- Identify and protect against AI-enabled threats
- Develop comprehensive security strategies incorporating AI
- Ensure compliance while maintaining effective detection capabilities
- Build resilient and adaptable security within organisations

TRAINING METHODOLOGY

The training course utilizes a comprehensive, multi-faceted learning approach to ensure effective knowledge acquisition. It combines expert-led instruction with interactive small-group exercises that encourage collaboration and deeper understanding. Learning is further reinforced through the use of engaging videos that illustrate key concepts and real-world case analysis, allowing participants to apply what they've learned to practical scenarios.

Organisational Impact

Organisations implementing the strategies and systems covered in this program can expect to significantly enhance their risk management and fraud detection capabilities. The training course provides frameworks for building robust, adaptable security that leverage AI while maintaining critical human oversight and intervention capabilities.

Key Impact Areas:

- Enhanced early warning systems for emerging threats and fraud patterns
- Reduced false positives in fraud detection, leading to operational efficiency
- Improved regulatory compliance through advanced monitoring capabilities
- Strengthened defence against AI-powered attacks and social engineering
- Decreased financial losses from fraud through proactive detection

Personal Impact

Participants will develop a unique skill set that combines technical understanding of AI systems with strategic risk management capabilities. Beyond technical skills, the training course develops critical thinking about AI system vulnerabilities and the ability to balance automation with human oversight.

- Increased knowledge AI risk management technologies
- Improve strategic capability to protect against evolving AI-enabled threats
- Enhanced crisis management and response capabilities
- Specialized knowledge in an increasingly critical business function
- Recognition as a thought leader in AI security implementation

WHO SHOULD ATTEND?

This **Luthando Skills** AI Powered Risk & Fraud Detection training course is specifically designed for:

- Risk and Compliance Officers
- Security Directors and Managers
- Financial Crime Specialists
- IT Security Leaders
- Business Leaders

- Those looking to progress in this field

Day 1

Foundations of AI in Risk and Fraud Detection:

- AI and Machine Learning Fundamentals for Security

    - Core concepts and algorithms relevant to risk detection
    - Types of AI models in security applications
    - Limitations and blind spots of AI systems
    - Real-world applications and failure cases

- Understanding the Threat Landscape

    - Traditional vs AI-powered threats
    - Evolution of fraud techniques
    - Social engineering and AI
    - Threat modelling with AI considerations

Implementation and Integration:

- Building AI Detection Systems

    - Data requirements and quality
    - Model selection and training
    - Integration with existing security infrastructure
    - Performance monitoring and metrics

- System Vulnerabilities and Protections

    - Common attack vectors against AI systems
    - Model poisoning and data manipulation
    - Defence strategies and best practices

Day 2

Advanced Detection Techniques:

- Pattern Recognition and Anomaly Detection

    - Behavioural analytics
    - Network traffic analysis
    - Transaction monitoring
    - Feature engineering for fraud detection

- Emerging Threats and Countermeasures

    - Deepfake detection
    - AI-powered social engineering
    - Cryptocurrency fraud
    - Case Studies: Advanced attack scenarios

Governance and Compliance:

- Regulatory Framework

    - Global compliance requirements
    - AI system auditing
    - Documentation and reporting
    - Legal considerations and liability

- Ethics and Privacy

    - Balancing security with privacy
    - Bias in AI systems
    - Transparency and explainability
    - Developing ethical guidelines

Day 3

Future-Proofing and Strategic Planning:

- Emerging Technologies and Threats

    - Quantum computing implications
    - Advanced persistent threats
    - Future of AI in security
    - Preparing for new attack vectors

- Strategic Implementation Workshop

    - Risk assessment framework
      development
    - Resource allocation planning
    - Training and awareness
      programs
    - Creating a security roadmap