CYBERSECURITY FUNDAMENTALS FOR AI-DRIVEN FRAUD DETECTION



GENTEX®
TRAINING CENTER

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

Introduction

The Cybersecurity Fundamentals for AI-Driven Fraud Detection Training Course prepares fraud, risk, and security professionals to protect the systems and data that intelligent fraud detection depends on. AI detection models are only as trustworthy as the infrastructure around them. A poisoned dataset, a stolen credential, or an exposed API can turn a strong model into a liability. This course connects fraud analytics with cybersecurity fundamentals. It covers data protection, access control, secure pipelines, and threat modelling. Furthermore, it applies regulatory requirements and incident response practice. As a result, participants deploy AI detection that is effective and defensible.

Cybersecurity Fundamentals for AI-Driven Fraud Detection Course Objectives

- Explain cybersecurity fundamentals in the context of fraud detection systems.
- Apply the CIA triad and risk management principles to detection platforms.
- Identify threats and attack vectors targeting fraud analytics environments.
- Apply identity, access management, and least-privilege principles.
- Protect data in transit and at rest with encryption and tokenisation.
- Secure data pipelines, APIs, and model interfaces.
- Apply threat modelling methods to AI detection systems.
- Assess model integrity, data poisoning, and adversarial manipulation risks.
- Apply incident response, logging, and forensic readiness practices.
- Align detection security with GDPR, PCI DSS, and sector regulations.

Course Methodology

- Interactive lectures with real breach and fraud system case studies.

GENTEX® TRAINING CENTER

- Threat modelling and attack path mapping workshops.
- Access control and pipeline security design exercises.
- Incident response and forensic readiness simulations.
- Structured peer discussion with facilitator feedback on security design.

Who Should Take This Course

- Fraud and financial crime analytics teams.
- Information security and cybersecurity professionals.
- Data scientists and engineers building detection models.
- Risk and compliance officers in financial institutions.
- Internal auditors reviewing detection and security controls.
- Technology leaders responsible for analytics platforms.

Cybersecurity Fundamentals for AI-Driven Fraud Detection Course Outlines

Day 1: Cybersecurity Foundations for Detection Systems

- Cybersecurity fundamentals and the CIA triad applied to analytics.
- Risk management, threat landscape, and attacker motivation.
- Fraud detection system architecture and its attack surface.
- Common vulnerabilities in analytics and data platforms.
- Security governance, policy, and accountability structures.
- Regulatory landscape for security and data protection.

- Case study: a breach that compromised a detection capability.

Day 2: Identity, Access, and Privilege Management

- Identity and access management fundamentals.
- Authentication methods, multi-factor authentication, and federation.
- Role-based and attribute-based access control design.
- Least privilege, privileged access management, and just-in-time access.
- Segregation of duties in analytics and fraud operations.
- Insider threat and behaviour monitoring.
- Workshop: designing access control for a detection platform.

Day 3: Data Protection and Secure Pipelines

- Data classification and handling requirements.
- Encryption at rest and in transit, and key management basics.
- Tokenisation, masking, and pseudonymisation for fraud data.
- Secure data pipelines, transfer, and integration controls.
- API security, authentication, and rate limiting.
- Data leakage prevention and logging discipline.
- Workshop: securing a fraud data pipeline end to end.

Day 4: Threat Modelling and Model Integrity

- Threat modelling methods including STRIDE and attack trees.
- Adversarial attacks on detection systems and evasion techniques.
- Data poisoning and training integrity controls.
- Model theft, inversion, and extraction risks.

- Secure model deployment and interface hardening.
- Third-party, cloud, and supply chain security considerations.
- Workshop: threat modelling an AI fraud detection system.

Day 5: Detection, Response, and Compliance

- Security monitoring, SIEM, and detection engineering basics.
- Logging, audit trails, and forensic readiness.
- Incident response planning for analytics environments.
- Breach notification and regulatory reporting obligations.
- GDPR, PCI DSS, and sector-specific security requirements.
- Building a security roadmap for fraud detection systems.
- Course review, assessment, and action planning.

Conclusion

By successfully completing Cybersecurity Fundamentals for AI-Driven Fraud Detection, participants will gain a thorough understanding of cybersecurity fundamentals, identity and access control, data protection, secure pipelines, threat modelling, and incident response for detection systems. They will also acquire practical skills in access design, pipeline hardening, threat modelling, and compliance alignment. In addition, the course prepares them to deploy AI fraud detection that resists attack and satisfies regulators. Gentex Training Center delivers this programme with a strong focus on applied security practice and measurable resilience improvement.

LEARN BOLD. **LEAD BEYOND**
GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

FAQs for Cybersecurity Fundamentals for AI-Driven Fraud Detection course

Q1 What is the "Cybersecurity Fundamentals for AI-Driven Fraud Detection" course about?

It is a five-day programme on protecting the systems and data behind AI fraud detection. It covers cybersecurity fundamentals and architecture, identity and access control, data protection and secure pipelines, threat modelling and model integrity, security monitoring, incident response, and regulatory compliance.

Q2 What are the key benefits of the "Cybersecurity Fundamentals for AI-Driven Fraud Detection" course?

Participants gain a detection environment that resists attack rather than assuming it will not happen. The course reduces breach and data leakage exposure, strengthens access and privilege discipline, hardens pipelines and interfaces, protects model integrity from poisoning and evasion, improves forensic readiness, and supports regulatory compliance with credible evidence.

Q3 What skills will I gain from the "Cybersecurity Fundamentals for AI-Driven Fraud Detection" course?

Participants gain threat and attack surface assessment for analytics environments, identity, access and privilege control design, data protection and secure pipeline hardening, and threat modelling, model integrity protection and incident response alignment. These four skills cover the security foundation that AI detection requires.

GENTEX® TRAINING CENTER

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

Q4 What tools, methods, or standards are covered in the "Cybersecurity Fundamentals for AI-Driven Fraud Detection" course?

The course covers the CIA triad and risk management principles, fraud detection system architecture and attack surface mapping, identity and access management, multi-factor authentication and federation, role-based and attribute-based access control, least privilege and privileged access management, just-in-time access, segregation of duties, data classification and handling, encryption at rest and in transit, key management, tokenisation, masking and pseudonymisation, secure data pipeline and integration controls, API security and rate limiting, data leakage prevention, STRIDE threat modelling and attack trees, adversarial attack and evasion techniques, data poisoning controls, model theft and extraction risks, SIEM and detection engineering, logging and forensic readiness, incident response planning, breach notification obligations, and GDPR, PCI DSS and sector security requirements.

Q5 How is the "Cybersecurity Fundamentals for AI-Driven Fraud Detection" course applied in real-world practice?

Participants apply the methods to their own detection platforms. They map attack surfaces, design access and privilege models, harden data pipelines, threat model model deployments, define logging and audit requirements, and prepare incident response and breach notification procedures. Many leave with a threat model and a security control matrix ready for adoption.

GENTEX® TRAINING CENTER