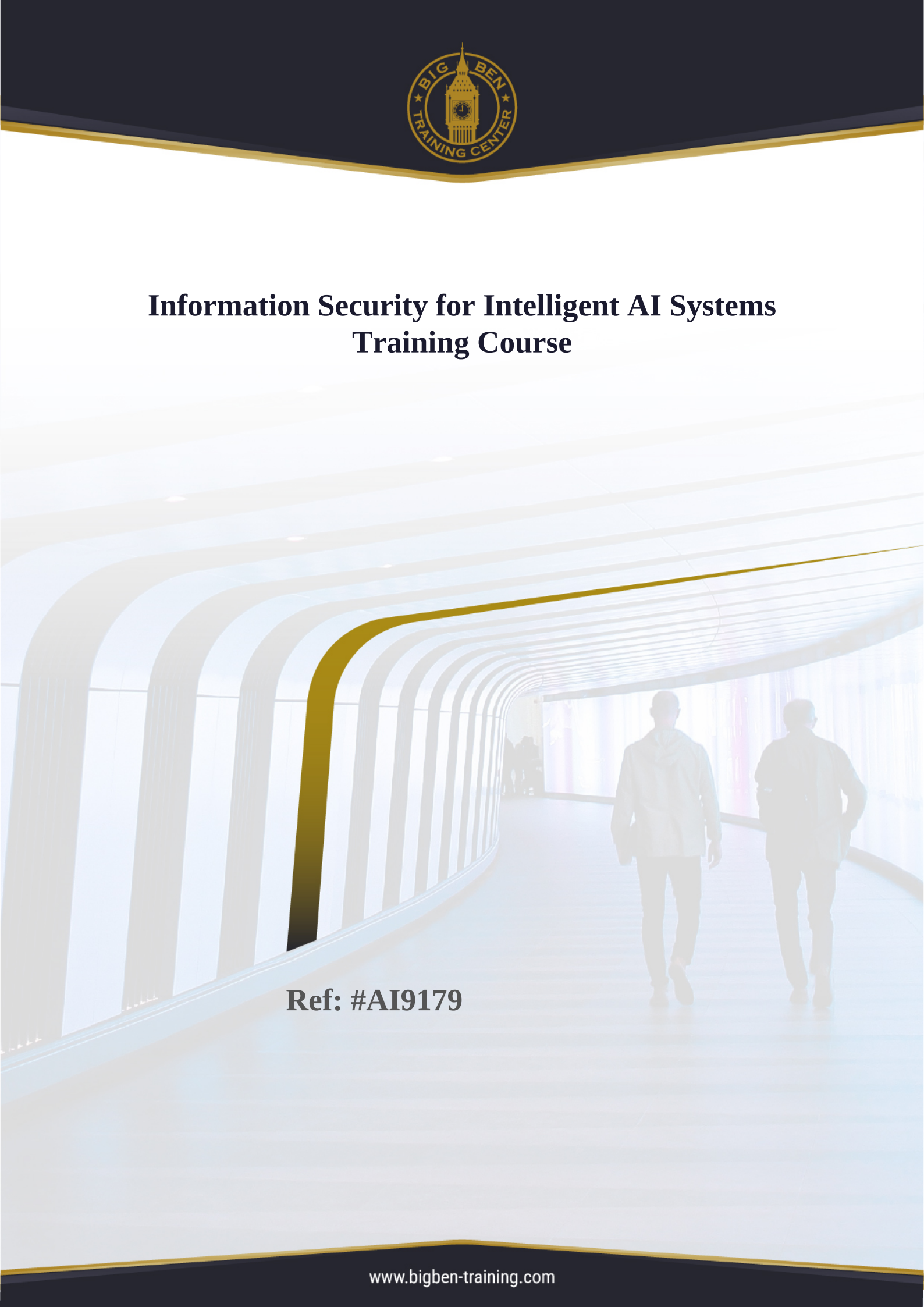
Information Security for Intelligent AI Systems Training Course



Ref: #AI9179

Course Introduction / Overview:

This training course is designed to provide a comprehensive understanding of the unique security challenges presented by artificial intelligence and intelligent systems. As organizations increasingly rely on AI for critical functions, the need to protect these systems from cyberattacks, data breaches, and adversarial threats has become a top priority. This program goes beyond traditional cybersecurity concepts to focus specifically on the vulnerabilities and risks that are unique to AI models and data pipelines. Drawing on the work of academics like Robert L. P. T. and C. N. K. from their book "Security and Privacy in Intelligent Systems," the course explores topics such as adversarial machine learning, data poisoning, and model theft. Participants will learn how to design and implement security frameworks that protect AI systems from end to end, from data collection and training to deployment. BIG BEN Training Center has developed this curriculum with a strong focus on practical, real-world applications and hands-on projects. It gives participants the skills to identify potential threats, harden their AI systems, and ensure the integrity and trustworthiness of their intelligent applications. This course is a vital resource for any professional looking to secure their organization's AI investments and protect against emerging cyber threats.

Target Audience / This training course is suitable for:

- Cybersecurity professionals and analysts.
- AI and machine learning engineers.
- Data scientists.
- IT security managers.
- Privacy officers and compliance specialists.
- Cloud security engineers.
- R&D and innovation managers.

Target Sectors and Industries:

- Technology and software development.
- Financial services.
- Defense and government agencies.
- Telecommunications.
- Healthcare and pharmaceuticals.
- Automotive and manufacturing.
- Research and development.

Target Organizations Departments:

- Information security.
- AI and data science.
- Research and development.
- IT and network security.
- Risk management.
- Product development.
- Compliance and governance.

Course Offerings:

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

- Identify and mitigate unique security vulnerabilities in AI and machine learning systems.
- Defend against adversarial attacks, including data poisoning and model evasion.
- Design secure data pipelines and model deployment strategies.
- Implement robust access control and privacy-preserving techniques for AI data.
- Assess the risks associated with AI models and platforms.
- Develop a comprehensive security framework for intelligent systems.
- Use AI-powered tools to enhance traditional cybersecurity defenses.

Course Methodology:

The training course at BIG BEN Training Center is built on a practical, hands-on methodology that addresses the complex security challenges posed by AI. We believe that securing AI systems requires a deep understanding of how they work and how they can be exploited. The course features case studies of real-world security breaches involving AI, allowing participants to analyze the vulnerabilities and learn how to prevent similar attacks. We use interactive workshops and simulations where participants get to act as both a defender and an attacker, building and then trying to break a simple AI system. These exercises give participants tangible experience in identifying and mitigating threats. The training also includes group discussions and expert-led Q&A sessions to ensure a comprehensive and collaborative learning environment. This approach ensures that participants leave with a clear understanding of how to protect their organization's intelligent systems and build trust in their AI applications.

Course Agenda (Course Units):

Unit One:? Fundamentals of AI Security

- Introduction to AI security and its importance.
- Key security concepts for machine learning.
- Understanding the AI attack surface.
- Adversarial machine learning attacks.
- Data privacy in AI systems.
- The human element in AI security.
- Case studies of AI security breaches.

Unit Two:? Securing the AI Data Pipeline

- Data collection and integrity issues.
- Data poisoning attacks and mitigation.
- Securing training data and models.
- Privacy-preserving techniques.
- Secure data storage and access control.
- Anomaly detection for data pipelines.
- Practical project on data security.

Unit Three:? Model Security and Integrity

- Protecting AI models from theft and exfiltration.
- Model evasion and black-box attacks.
- Robustness testing and model hardening.
- Securing model APIs and deployment.
- Model traceability and version control.
- AI for threat intelligence.
- Practical project on model security.

Unit Four:? Defensive AI and System Hardening

- Using AI to detect cyberattacks.
- AI for fraud detection and network anomaly detection.
- Implementing an AI security framework.
- Threat modeling for intelligent systems.
- Post-deployment monitoring and maintenance.
- Building a security-first AI development culture.
- Practical project on defensive AI.

Unit Five:? Governance, Ethics, and the Future of AI Security

- The ethical implications of AI security.
- Data governance and regulatory compliance.
- Developing a security-focused AI governance policy.
- The future of adversarial AI.
- Emerging threats and solutions.
- Building a long-term AI security strategy.
- Final capstone project presentation.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

How can organizations balance the need for transparent, explainable AI with the need to protect their proprietary models from adversarial attacks and intellectual property theft?

What unique qualities does this course offer compared to other courses?

This training course is specifically designed to address the critical intersection of information security and artificial intelligence, setting it apart from more generic cybersecurity or AI programs. While other courses may touch on security as a single topic, this curriculum focuses entirely on the unique and evolving threats that target intelligent systems. It provides a complete framework for protecting AI, from securing data pipelines and models to defending against sophisticated adversarial attacks. The program's practical, hands-on approach is a key differentiator. Participants won't just learn about threats in theory; they will engage in simulations that show how attacks happen and how to defend against them. This immersive learning style gives participants the tangible skills needed to build robust, secure AI systems. We also address the strategic and ethical aspects of AI security, which are crucial for long-term organizational success. This focused, in-depth approach is what makes this program an indispensable resource for any professional looking to secure their organization's future in the age of AI.