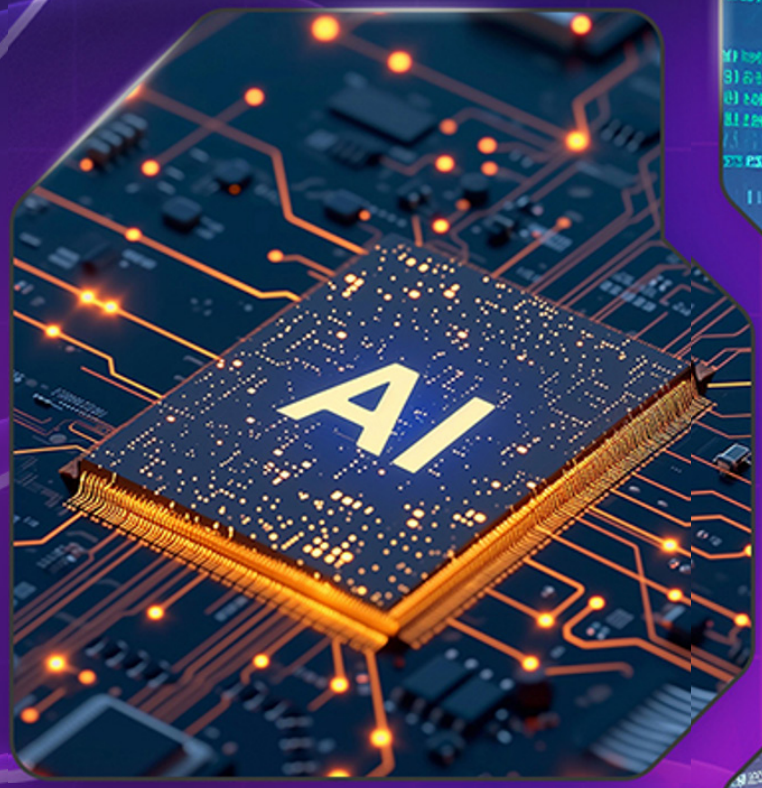
اتحاد المصارف العربية
Union of Arab Banks

Secure the Future:

WHERE CYBERSECURITY MEETS AI

2 - 4
NOVEMBER
2026





ONLINE

11:00 TO 14:00 BEIRUT TIME

Secure the Future:

WHERE CYBERSECURITY MEETS AI



Why AI in Cybersecurity?

Artificial intelligence (AI) is fundamentally transforming the cybersecurity landscape. Organizations across every sector are rapidly adopting AI to improve operational efficiency, automate decision-making, and enhance digital services. At the same time, cybercriminals are leveraging the same technologies to develop more sophisticated, adaptive, and scalable attacks.

While AI introduces new risks, it also provides powerful opportunities to strengthen cyber defenses. Security teams can now use AI to automate threat detection, accelerate incident response, identify anomalies in massive datasets, prioritize vulnerabilities, and improve security operations through intelligent analysis and decision support. These capabilities enable organizations to respond more quickly and effectively to increasingly complex cyber threats. However, successfully integrating AI into cybersecurity requires more than simply deploying AI-powered tools. Professionals must understand how these systems work, recognize their limitations, manage associated risks, and ensure they are implemented securely and responsibly.

In fact, as organizations deploy machine learning models and generative AI applications, these technologies become valuable targets for attackers. Threats such as prompt injection, data poisoning, model theft, adversarial attacks, insecure AI integrations, and unauthorized access to AI systems create new attack surfaces that demand specialized security knowledge. Protecting AI applications requires security practitioners to expand their expertise beyond conventional network, endpoint, and application security practices.

This comprehensive nine-hour training is designed to equip cybersecurity professionals with the knowledge and practical skills required to address these evolving challenges. Participants will explore both dimensions of modern AI security: securing AI systems against emerging threats and leveraging AI to strengthen cybersecurity operations. Through a combination of conceptual discussions, practical demonstrations and real-world case studies, the training bridges the gap between traditional cybersecurity practices and the rapidly evolving AI-driven security ecosystem.

By the end of the program, participants will have a solid understanding of the current AI threat landscape, the security implications of deploying AI technologies, and the practical application of AI-powered defensive capabilities. They will also gain insights into governance, risk management, ethical considerations, and financial sector best practices for securely adopting AI within their organizations.

Ultimately, this course is intended for those who want to move beyond traditional security tooling and develop the competencies that will define the next decade of cybersecurity. By mastering the principles of securing AI systems participants will be better positioned to protect their organizations against increasingly intelligent threats while harnessing the transformative potential of AI to build more resilient, proactive, and adaptive security operations

Secure the Future:

WHERE CYBERSECURITY MEETS AI



By the end of this course, you will be able to

- Explain foundational AI concepts as they apply to Cybersecurity
- Identify and defend against attacks on AI systems — data poisoning, prompt injection, model theft, and more
- Use AI-powered tools to strengthen threat detection, secure coding, penetration testing and incident response
- Apply AI governance, risk, and compliance principles in a business setting

Who Should Enroll

- IT and security professionals ready to up skill in AI-driven defense
- Software developers
- SOC analysts, penetration testers, and incident respondents
- Career-changers with a foundational technical background

Prerequisites

Basic networking and security fundamentals recommended. No prior AI/ML experience required.

What You'll Learn

DAY 1 (3 hrs)

Basic AI Concepts Related to Cybersecurity
ML, deep learning, Natural Language Processing, generative AI, prompting, RAG, the AI life-cycle, human oversight.

DAY 2 (3 hrs)

Securing AI Systems
Data poisoning, prompt injection, jail-breaking, model theft, guardrails, access controls, encryption, auditing.

DAY 3 (3 hrs)

AI-Assisted Security
AI-powered security tools, threat detection, secure coding, pen testing, and how attackers weaponize AI.

AI Governance, Risk & Compliance
Governance structures, corporate AI policy, third-party audits, data sovereignty.

Learning Format

- On-line presentation
- Real case discussions
- Lab demos and tools

Secure the Future:

WHERE CYBERSECURITY MEETS AI





SPEAKER:

JEAN-MICHEL KAWKABANI

CISA

ARCSHIELDS, DIRECTOR

Jean-Michel is the Director of ARCSHIELDS, a cybersecurity consulting firm serving clients across Europe, the Middle East, and Africa (EMEA). He previously served as Head of Information Security at Byblos Bank Group, where he also held leadership positions as Head of IT Audit and Head of Management Information Systems (MIS).

With over 27 years of experience in information systems, including more than 25 years specializing in cybersecurity, IT audit, and risk management within the financial sector, Jean-Michel is recognized for his expertise in enterprise security architecture, cybersecurity governance, risk assessment, incident response (CSIRT), digital forensics, IT auditing, and penetration testing.

Jean-Michel is a Certified Information Systems Auditor (CISA) accredited by ISACA and a Certified Security Analyst accredited by the EC-Council. He is an active lecturer at Saint Joseph University (ESIB) and the École Nationale d'Administration (ENA) in Lebanon. In addition, he serves as a cybersecurity trainer and Technical Committee member at the Union of Arab Banks, contributing to the advancement of cybersecurity awareness and best practices across the region.

