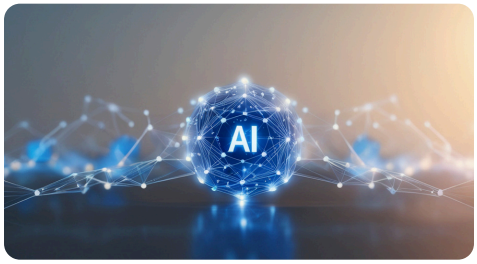
ed-watch
Your online resource partner

CPD MEMBER
The CPD Certification Service

Generative AI Security (Beyond Basic Deepfakes)

Securing Tomorrow's Intelligence: Defensive Strategies for a Generative World !



Program Overview

The Generative AI Security (Beyond Basic Deepfakes) program is designed to equip professionals and decision-makers with an in-depth understanding of security risks, threats, and controls related to Generative AI technologies. Moving beyond basic deepfake awareness, the program explores advanced attack vectors, misuse scenarios, and defense strategies for large language models, generative systems, and AI-driven automation.

Participants gain practical knowledge to secure AI systems, manage AI-related risks, and implement robust governance frameworks that protect organizations from emerging cyber, data, and reputational threats.

PROGRAM AT A GLANCE

- 2nd To 4th August 2026
- 8:00 AM - 2:30 PM (GMT+3)
- 18 CPD Hours
- In Person Public Program In Jeddah

Key Learning Outcomes

- ✓ Understand evolving Generative AI threats and risks.
- ✓ Assess AI vulnerabilities and implement mitigation controls.
- ✓ Establish governance, policies, and secure AI frameworks.
- ✓ Align AI security strategies with compliance requirements.

COURSE COVERAGE

Module 1: Foundations of Generative AI & Security Risks

- Overview of Generative AI technologies (LLMs, diffusion models, multimodal AI)
- How Generative AI systems work: data, models, and deployment
- Threat landscape introduced by Generative AI
- Limitations and security blind spots of current AI systems

Module 2: Beyond Deepfakes – Advanced Generative AI Threats

- Prompt injection and model manipulation attacks
- Data poisoning and training data compromise
- Model theft, inversion, and extraction attacks
- AI-generated malware, phishing, and social engineering

Module 3: Securing Generative AI Models & Infrastructure

- Securing AI development pipelines and MLOps environments
- Model access controls, monitoring, and validation
- Data security, integrity, and privacy considerations
- Securing APIs and AI-enabled applications

Module 4: Generative AI, Cybersecurity & Fraud Risks

- AI-powered cyberattacks and automation risks
- Identity fraud, impersonation, and synthetic identities
- Financial crime, misinformation, and reputational threats
- Case studies of real-world AI-driven incidents

Module 5: Governance, Risk & Compliance for Generative AI

- AI risk management frameworks and standards
- Regulatory considerations and emerging AI laws
- AI policies, acceptable use, and internal controls
- Role of leadership in AI security oversight

Module 6: Responsible & Secure Use of Generative AI

- Ethical AI principles and bias mitigation
- Human-in-the-loop controls and accountability
- Transparency, explainability, and auditability
- Balancing innovation with security and trust

Module 7: Building a Generative AI Security Roadmap

- Identifying critical AI risks and priority controls
- Integrating AI security into enterprise risk management
- Measuring effectiveness and continuous monitoring
- Practical roadmap development exercise

INSTRUCTOR

Adam Elshimi

Adam Elshimi is a Senior Solutions Architect at NVIDIA with 15+ years designing agentic systems and high-performance computing architectures. He focuses on deploying accelerated computing for telecom, integrating GPU and DPU technologies to build AI-native, virtualized networks. Previously, as CEO of SensAi, he advanced multi-agent systems for enterprise automation and holds a patent for Graph Neural Network-driven energy optimization in telecom. With a Master's in Data Science and research in AI/ML cybersecurity, Adam bridges research and real-world deployment. He also advises and educates global partners on AI frameworks and networking technologies.

PROFESSIONAL ASSOCIATIONS & AFFILIATIONS

AREAS OF EXPERTISE

Agentic AI | Telecom AI | Edge Computing | Generative AI | Multi-Agent Systems

Registration & Contact

PROGRAM DETAILS

- 2nd To 4th August 2026
- Timing 8:00 AM - 2:30 PM (GMT+3)
- 18 credit hours spread over three days.

Who Should Attend?

- Information Security Leaders
- Cybersecurity & SOC Professionals
- AI / ML Engineers
- Technology Risk & GRC Professionals
- Legal, Privacy & Compliance Officers
- Senior Executives & Decision-Makers

PAY NOW

Scan to pay

To proceed with company registration.

CLICK HERE

For any information, contact us at below given details.

Email Us:

shahzad@ed-watch.org
javaria@ed-watch.org

Call or WhatsApp Us

+1 (917) 893-4606
+1 (929) 361-2818

Why Ed Watch?

Ed-Watch is a dynamic learning platform offering professional development in sustainability, ESG, digital transformation, digital skills, data analytics, leadership, and finance. Gain practical expertise, earn certifications, and empower yourself to excel in today's fast-evolving workplace.

Ready to Transform?
Contact our support team today.

contact@ed-watch.org
www.ed-watch.org

ed-watch
Your online resource partner

Complete the nomination form and send it via email to shahzad@ed-watch.org or javaria@ed-watch.org.

Nomination Form

S.No.	Participant Full Name	Job ID	Email ID	Contact No.	Function/ Department	Education Level	Years of Experience
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							

Note: Please complete the details below if your nomination is through a company.

HR Contact Person Details

Name:	Email ID:	Contact No:
Designation:	Company:	
Company Address:		

Invoicing Contact Person Details

Name:	Email ID:
Designation:	Contact No:
Any Remarks:	

OFFICE

KSA: 4218,RIYADH, 6706, 13322 KSA

US: 20 Hallo St, Edison, NJ 08837, USA