Agentic Blast © Training

BILGINC
IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

Duration: **4 Day**

Overview

This immersive Agentic AI security risk simulation scenario equips participants with the skills to navigate the emerging risks of autonomous AI systems operating across organisational functions. As organisations adopt AI systems capable of acting independently, such as approving loans, verifying identities, managing employees, controlling access, and processing payments, traditional cybersecurity and governance frameworks become insufficient.

Participants assume the role of an AI Operations Supervisor at a mid-sized UK bank undergoing aggressive AI transformation. They will respond to a major fraud incident while managing the friction caused by multiple Agentic AI systems acting at cross purposes. The simulation combines real-world scenarios with regulatory guidance, including the EU AI Act, ISO/IEC 42001, and NCSC Cyber Assessment Framework, enabling participants to identify architectural vulnerabilities and implement effective AI oversight.

Prerequisites

There are no prerequisites for this simulation, it is LLM agnostic. It is suitable for participants across all levels seeking practical experience in managing AI and Agentic AI system risks.

Target audience

This simulation is designed for:

- Security, risk, assurance, and governance professionals
- Privacy specialists, and DPO's
- Security operations and IT leaders
- Software engineers, product and, data owners
- Business managers and decision-makers responsible for AI adoption

What You Will Learn

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

- Identify the difference between AI systems that recommend versus AI systems that act, and the associated risk implications
- Recognise circular trust vulnerabilities where human oversight depends on AI-generated reports
- Evaluate how multiple Agentic AI systems can work at cross purposes during crisis situations
- Apply regulatory frameworks, including EU AI Act Article 14, ISO/IEC 42001, and NCSC CAF, to NIST AI oversight design
- Assess biometric data collection risks and understand the permanent nature of biometric compromise
- Formulate appropriate responses when automated systems obstruct incident response
- Distinguish between attack vectors (how breaches occur) and root causes (architectural vulnerabilities)