Enterprise AI Security

Secure AI usage, data protection, and threat awareness

Format	Duration	Audience	Deployment	LMS/SSO	PO
On-Demand	Scoped runtime	Security, IT, risk, compliance	Enterprise licensing	Optional	Supported

Executive Overview

Enterprise AI Security is an enterprise training program that addresses AI-specific security risks across tools, data flows, and integrations. It explains how data handling, access control, secure configuration, logging, and misuse awareness should be applied to AI-enabled work in a way that supports oversight, internal control alignment, and audit review. The program is designed to reduce AI-related security exposure while producing structured, reviewable evidence suitable for governance and internal audit workflows.

Program Outcome

Reduce AI-related security exposure across tools, data flows, and integrations.

Why This Matters

Organizations need more than general security awareness when AI tools and integrations are introduced into daily work. A practical AI security baseline helps teams apply consistent safeguards, reduce data exposure, strengthen control expectations, and show that AI-related risk has been addressed in a structured, reviewable way.

Enterprise Risk Exposure Addressed

- Prompt injection and data exfiltration risks
- Sensitive data exposure through AI workflows
- Insufficient logging/monitoring of AI usage
- Unreviewed integrations increasing attack surface

What the Organization Receives

- AI Security Control Checklist: Access, logging, data protection, and secure usage requirements.
- Threat Scenario Library: Prompt injection, data exfiltration, and misuse patterns.
- Security Review Workflow: When security review is required and what evidence is needed.
- Secure Tooling Guidance: Approved tool configuration, identity, and monitoring recommendations.
- Templates, Workbook, and Governance-Oriented Guidance: Practical materials that support documented oversight and internal control alignment.