Description:

A close-up of a button

AI-generated content may be incorrect.

If you are looking for the foremost AI cybersecurity course, then the **C)AICSO: Certified AI**

**Cybersecurity Officer** is for you. The course will prepare you with a broad range of

knowledge and skills for personal responsible for not only implementing AI but also securing.

The C)AICSO course not only teaches you how to protect your organization from AI — it's

about building resilience with AI. The C)AICSO guides managers on how AI can become a trusted, secure, and strategic enabler, not an existential liability. The C)AICSO will provide a battle-tested playbook for AI security, present a framework that articulates safe, resilient, and auditable AI ecosystems, and prepare the manager to lead AI governance programs and anticipate future threats.

The C)AICSO course will equip the AI manager with the following, **Progressive AI Risk Management Framework:** Tied to critical infrastructure; Policy-First Security Design: Treating GenAI as an Insider Threat Vector; Adversarial Use Case Mapping: Inspired by MITRE ATLAS and OWASP LLM Top 10; Quarterly Risk Reviews: What leaders should ask their AI teams; and **Red Teaming & Simulation Exercises**: For decision-makers (not coders).

Icon

Description automatically generated

Annual Salary Potential $148,662 AVG/year

Completion of Mile2 provided training and/or education is not required to achieve any Mile2 certification.

* IS Security Officers
* IS Managers
* Risk Managers
* Auditors
* Info Systems Owners
* IS Control Assessors
* System Managers
* AI Governance Officers
* Security Architects

### Module 01: What is AI, Really?

### Module 02: AI Bus. Apps Across Sectors

### Module 03: Architecture of AI Systems

### Module 04: Ethical, Legal & Regulation

### Module 05: Threat Landscape AI Sys.

### Module 06: Supply Chain Risks

### Module 07: Securing GenAI Systems

### Module 08: Advanced Threat Scenarios

### Module 09: Sec AI-by-Design Principle

### Module 10: AI RM Frameworks

### Module 11: Identity, Access, Controls

### Module 12: Cloud-Native AI Security

### Module 13: AI Governance-Org

### Module 14: Auditing and Testing AI

### Module 15: AI-Centric Incident Resp.

### Module 16: Futureproofing & AI Res.

### Module 17: Exercises & Scenarios

### Module 18: Data Governance Updates

### Module 19: AI Policy Building Blocks

### Module 20: AI Security Program

**Live Class Duration:** 5 Days

**CEUs:** 40

**Language:** English

**Class Formats Available:**

• Instructor Led

• Self-Study

• Live Virtual Training

**Suggested Prerequisites:**

• Mile2’s C)SP

• Mile2’s C)ISSM

• 12 months of Information

Systems Management

Experience

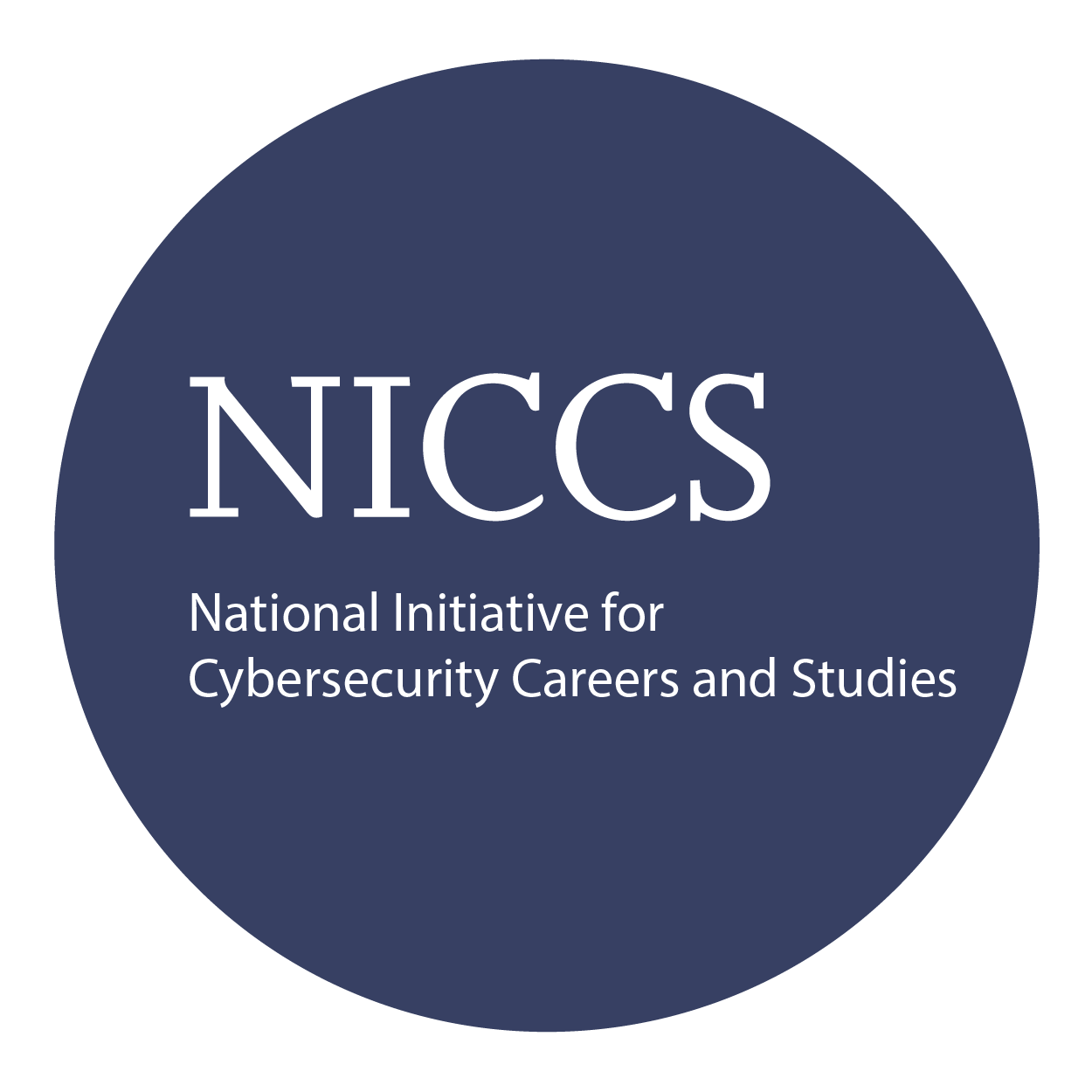
Who Should Attend

Modules/Lessons

Key Course Information

Key Course Information

Accreditations

Logo

Description automatically generatedA blue and gold badge with a red and white striped emblem

AI-generated content may be incorrect.A logo of a united states department of homeland security

AI-generated content may be incorrect.

Course FAQ’s

Exam Information

Upon Completion

**Question:** Do I have to purchase a course to buy a certification exam?

**Answer**: No

**Question:** Do all Mile2 courses map to a role-based career path?

**Answer**: Yes. You can find the career path and other courses associated with it at [www.mile2.com](http://www.mile2.com).

**Question:** Are all courses available as self-study courses?

**Answer**: Yes. There is however 1 exception. The Red Team vs Blue Team course is only available as a live class.

**Question:** Are Mile2 courses transferable/shareable?

**Answer**: No. The course materials, videos, and exams are not meant to be shared or transferred.

The Certified AI Cybersecurity Officer exam is taken online through Mile2’s Learning Management System and is accessible on you Mile2.com account. The exam will take approximately 2 hours and consist of 100 multiple choice questions.

A minimum grade of 70% is required for certification.

All Mile2 certifications will be awarded a 3-year expiration date.

There are two requirements to maintain Mile2 certification:

1. Pass the most current version of the exam for your respective existing certification
2. Earn and submit 20 CEUs per year in your Mile2 account.

Upon completion, Certified AI Cybersecurity Officer students will be able to establish industry-accepted cybersecurity and Information Systems management standards with current best practices. In addition, the following competencies will be achieved:

* A comprehensive framework for assessing and mitigating AI security risks
* How to red team and incident plan for LLM and GenAI systems
* How to apply NIST and ISO frameworks to real AI workflows
* How to securely integrate GenAI into enterprise environments
* Governance blueprints for multi-stakeholder coordination and oversight

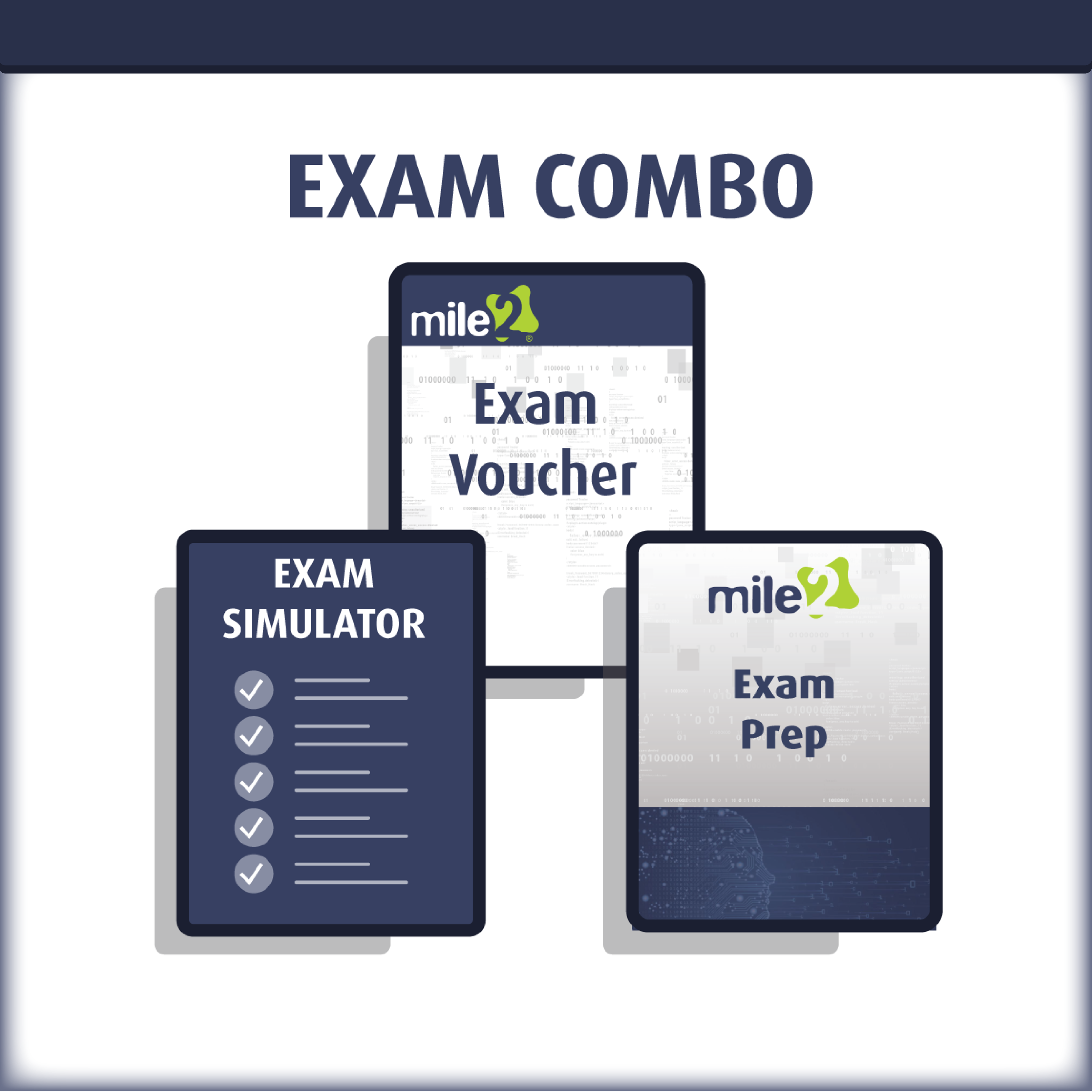
Re-Certification Requirements

Course and Certification Learning Options

Graphical user interface, application

Description automatically generated





Detailed Outline:

**Module 01: What is AI, Really?**

01.1 AI, ML, DL, and LLMs Explained

01.2 Reinforcement Learning and Generative AI

01.3 AI System Examples: ChatGPT, Sora, Claude, Gemini, DALLÂ·E

01.4 The Capabilities and Limitations of Modern AI

### Module 02: AI Business Applications Across Sectors

02.1 AI in Customer Service, Healthcare, HR, Fraud, Cyber

02.2 AI for Decision Augmentation vs Automation

02.3 Industry-Specific AI Use Cases (Critical Infrastructure, Finance, etc.)

02.4 Emerging Trends: Agenic AI & Autonomous Agents

### Module 03: The Architecture of AI Systems

03.1 Data Pipelines: Ingestion, Cleaning, Feature Engineering

03.2 Models and Training vs Inference Workflows

03.3 APIs, Plugins, Cloud vs Edge Deployments

03.4 Cost, Performance & Scalability Trade-offs

### Module 04: The Ethical, Legal & Regulatory Terrain

04.1 AI Bias, Fairness, and Explainability

04.2 EU AI Act, NIST AI RMF, ISO/IEC 42001, OECD

04.3 Compliance in High-Risk Sectors

04.4 Ethics of Autonomous Agents & Generative Models

## **PART II – AI-SPECIFIC THREATS AND RISKS**

### Module 05: Threat Landscape for AI Systems

05.1 Prompt Injection, Jailbreaks, Adversarial Inputs

05.2 Model Inversion, Data Poisoning

05.3 Hallucinations, Misinformation, and Impersonation

05.4 Case Examples from 2023–2025

### Module 06: Infrastructure and Model Supply Chain Risks

06.1 Insecure Training Environments & Data Lakes

06.2 Model Theft, Tampering, & Inference Abuse

06.3 API Abuse and Plugin Vulnerabilities

06.4 OSINT, Third-Party Risks, and GenAI Abuse

### Module 07: Securing GenAI Systems

07.1 OWASP Top 10 for LLMs

07.2 MITRE ATLAS Threats to AI

07.3 Red Teaming and Adversarial Testing

07.4 Hallucination Mitigation Techniques

### Module 08: Advanced Threat Scenarios

08.1 GPU Hijacking, Cloud Escalation

08.2 Synthetic Identity and Deepfake Exploits

08.3 Autonomous Offensive AI (Agenic AI Threats)

08.4 Coordinated AI-led Attacks on CI (Critical Infrastructure)

## **PART III – DEFENSE & RISK MANAGEMENT**

### Module 09: Secure AI-by-Design Principles

09.1 Data Minimization and Privacy-Enhanced Learning

09.2 TEE, Federated Learning, Homomorphic Encryption

09.3 Threat Modeling for AI Workflows

### Module 10: AI Risk Management Frameworks

10.1 NIST AI RMF Deep Dive

10.2 Implementing ISO/IEC 42001 in the Enterprise

10.3 Mapping AI Risks to Business Impact

### Module 11: Identity, Access, and Control for AI Systems

11.1 Authentication for LLMs

11.2 RBAC/ABAC for AI APIs

11.3 Zero Trust Architectures for GenAI Systems

### Module 12: Cloud-Native AI Security

12.1 AWS Bedrock, Azure OpenAI, Google Vertex AI

12.2 Cloud Misconfigurations and Exfiltration Paths

12.3 Logging, Threat Detection, and Response

## 

## **PART IV – GOVERNANCE, INCIDENT RESPONSE & RESILIENCE**

### Module 13: AI Governance in Complex Organizations

13.1 Who Owns AI Risk? (CISO/CIO/CTO Debate)

13.2 AI Ethics Committees, Governance Boards

13.3 Documentation and Transparency Best Practices

### Module 14: Auditing and Testing AI

14.1 AI Red Teaming Methodologies

14.2 Bias Detection and Fairness Audits

14.3 Third-Party Evaluation Frameworks

### Module 15: AI-Centric Incident Response

15.1 Detection and Containment of AI Exploits

15.2 Toxic Output and Privacy Leaks

15.3 Playbooks for Prompt Injection and GenAI Abuse

### Module 16: Futureproofing and AI Resilience

16.1 Adaptive Threats: Autonomous and Multi-Modal AI

16.2 R&D: Simulating Rogue Agents

16.3 Building Post-AI-Compromise Resilience

## **PART V – PRACTICALS, STRATEGY & ACTION**

### Module 17: Strategic Exercises and Scenarios

17.1 Attack Simulation: Policy-Only Scenario Labs

17.2 Controls Mapping for Different AI Models

17.3 Designing Security Playbooks

### Module 18: What Managers Must Ask Quarterly

18.1 Governance Checklists

18.2 Architecture Review Questions

18.3 Prompt Abuse Controls

18.4 Transparency & Data Governance Updates

### Module 19: AI Policy Building Blocks

19.1 Writing a Safe AI Policy from Scratch

19.2 Mandatory Training and Awareness

19.3 Defining “High-Risk” and “Low-Risk” Systems

19.4 Board-Level AI Policy Templates

### Module 20: Your AI Security Program – End to End

20.1 Maturity Models for AI Security

20.2 Role of the CISO, ISO, and Emerging Roles (CAIOs)

20.3 Roadmap for the Next 18–24 Months

20.4 Closing Thoughts & Final Reflection

## 

## **APPENDICES**

* Glossary of AI + Cyber Terms
* AI Attack & Threat Matrix (Custom)
* Quarterly Review Template for Managers
* Policy Draft Template
* Dataset Checklist for Secure Training