Certified Information Security & AI Professional (CISAIP) Workshop

Course Duration: 5 days

Course Overview

Transform your CISSP expertise with AI-driven security strategies. Gain the documents, frameworks, and best practices needed to elevate your cybersecurity skills into the AI era.
This 3-day intensive program focuses on bridging AI concepts into each of the eight CISSP domains.

Target Audience

- CISSP-Certified Professionals looking to integrate AI into their existing security framework.
- Cybersecurity Managers and Team Leads who oversee risk management, network security, or IAM.
- IT Governance Professionals aiming to align AI strategies with corporate compliance.
- Security Architects and Engineers exploring AI for threat modeling, detection, and response.

What You Will Learn

- AI Integration for Each CISSP Domain: Adapt your foundational knowledge with AI-driven solutions and documentation.
- Strategic Document Creation: Develop governance policies, risk assessment frameworks, and compliance checklists that incorporate AI considerations.
- Real-World Application: Discover how to immediately deploy these tools and templates for faster, more effective security management.

Why Should you attend the course

- Future-Proof Your Skillset: Stay relevant by evolving your current CISSP knowledge to include AI advancements.
- Practical Output: Walk away with ready-to-use documents and frameworks—no abstract theory, just actionable deliverables.
- Certification Advantage: Earn the CISAIP credential, demonstrating your AI-readiness to employers and peers.

Course Focus Areas

- **AI Fundamentals for Cybersecurity**
  Explore core AI concepts (ML, NLP, Deep Learning) and how they apply to risk detection and threat intelligence.
- **Risk Management & Compliance Upgrades**
  Adapt traditional risk frameworks like NIST SP 800-30 with AI-based tools for predictive analysis.
- **Documenting AI-Infused Architecture & Engineering**
  Use curated templates to incorporate AI into network designs, hardware configurations, and secure system lifecycles.
- **AI-Driven IAM & Access Control**
  Build policies for biometric authentication, anomaly detection, and zero-trust frameworks augmented by AI.
- **Security Assessment & Testing Tools**
  Compile checklists for AI-driven penetration testing, vulnerability scanning, and continuous compliance.
- **Incident Response & Security Operations**
  Leverage AI to enhance incident response playbooks, streamline log analysis, and automate threat hunting.
- **Governance, Ethics, and Regulatory Considerations**
  Account for ethical AI deployment, data privacy, and evolving legal frameworks.
- **AI in Software Development Security**
  Develop guidelines for integrating AI-powered static code analysis and secure DevOps pipelines.

Prerequisites

- Active CISSP Certification (or equivalent professional experience).
- Anyone with a Basic understanding of cybersecurity fundamentals, including risk management, network security, and IAM concepts.

Course Agenda

Course Modules & Topics (Focuses on the CISSP’s domains)

Module #	Module Topic	Description
00	**Overview**	• Course Introduction • Certificate Introduction & Exam Details.
Module 01	**Security and Risk Management (Domain 1)**	• AI-Driven Governance and Policy: How to update existing security policies with AI considerations, including ethical AI guidelines. • AI in Risk Assessment: Leveraging predictive analytics for threat forecasting and prioritization. • Compliance and Regulatory Requirements: Incorporating evolving AI regulations into standard compliance checklists (e.g., GDPR, ISO 27001)
Module 02	**Asset Security (Domain 2)**	• Data Classification with AI: Automating classification processes using machine learning. • AI-Enabled Asset Discovery: Identifying unknown or untracked assets through anomaly detection. • Information Lifecycle Management: Managing data retention and destruction policies with AI-driven audits.
Module 03	**Security Architecture and Engineering (Domain 3)**	• AI-Augmented System Design: Integrating machine learning models into secure-by-design principles. • Hardware and Firmware Considerations: Evaluating AI accelerators, edge devices, and their security implications. • Emerging Technologies: Quantum-resistant cryptography and how AI aids in designing future-proof architectures.

Module 04	**Communication and Network Security (Domain 4)**	• AI in Network Segmentation: Automating segmentation policies based on real-time traffic analytics. • Intelligent Threat Detection: Machine learning for anomaly detection, intrusion prevention, and traffic flow analysis. • Secure Protocols and Encryption: Assessing AI's role in identifying vulnerabilities in encryption algorithms and protocols.
Module 05	**Identity and Access Management (Domain 5)**	• Biometric Authentication with AI: Facial recognition, voice authentication, and continuous monitoring for identity assurance. • Adaptive Access Control: Using AI to determine dynamic access privileges based on user behavior patterns. • Zero Trust Models: Leveraging AI to enforce just-in-time access decisions and micro-segmentation.
Module 06	**Security Assessment and Testing (Domain 6)**	• Automated Vulnerability Scanning: Enhancing traditional tools with AI to reduce false positives and streamline reporting. • Penetration Testing with AI: Scripted AI bots to discover complex attack paths and misconfigurations. • AI-Driven Compliance Testing: Crafting checklists to validate adherence to regulations and internal policies.
Module 07	**Security Operations (Domain 7)**	• AI in Security Operations Centers (SOCs): Implementing ML-based event correlation, automated alert triaging, and real-time threat hunting. • Incident Response Automation: Leveraging AI to detect attacks faster and orchestrate response playbooks. • Behaviour Analytics & Insider Threats: Using AI to profile normal behaviors and flag suspicious deviations.

Module 08	**Software Development Security (Domain 8)**	• AI-Enhanced Code Review: Tools and approaches for automatically identifying security flaws during development. • Secure DevOps Pipelines: Integrating AI-based vulnerability scanning into CI/CD workflows. • AI for Threat Modeling: Generating risk scenarios and countermeasures early in the software lifecycle.

Exam Details

Exam Details	**Exam Code: MBC-400**
MCQs	**100 randomized out of 150 total**
Duration	**120 Minutes**
Test Format	**Multiple choice and advanced innovative items**
Test Delivery	**Pearson VUE, either at authorized testing centers or online, depending on your preference and location.**
Passing Score	**70% or greater**
Practice Exam	**No**
Validity	**1 year**