Certified AI Security Practitioner (CAISP) v2.0 Training

Deep Dive into AI/ML Cybersecurity Training

Batch : Asia & Middle East
Date: 10-13 November 2025
Timing: 6:00 AM – 10:00 AM GMT
Mode of training: Online

Batch : Americas & Europe
Date: 10 -13 November 2025
Timing: 1:00 PM – 5:00 PM GMT
Mode of training: Online

Course Fee: USD 199 **For ISACA/ISC2 members: USD 159** **For Client/Returning participants: USD 129**

CAISP v2.0 Training

Introduction

- Artificial Intelligence (AI) and Machine Learning (ML) are transforming cybersecurity, enabling advanced threat detection, faster response, and automation at scale. These technologies allow organizations to process vast data, derive real-time insights, and strengthen security without proportional increases in resources.

- However, AI/ML adoption also introduces new risks such as data poisoning, adversarial attacks, and vulnerabilities in large language models (LLMs). Addressing these challenges requires robust governance, security testing, and alignment with global standards like ISO/IEC 42001 and NIST AI RMF.

- This training equips participants with the knowledge and practical skills to secure AI/ML systems through hands-on labs, case studies, and best practices in secure MLOps. By the end, attendees will be ready to design, secure, and govern AI/ML systems that advance business goals while mitigating evolving cyber threats.

Why Attend?

- Expert-led sessions
- Hands-on labs & simulations
- Real-world case studies
- Actionable skills & takeaways

CAISP v2.0 Training

Objective Of CAISP v2.0

- Grasp the fundamentals of AI and ML, and understand how they are reshaping cybersecurity
- Explore real-world uses of LLMs in threat intelligence, malware detection, and SOC operations
- Learn practical methods to integrate AI/ML models into existing security workflows
- Recognize challenges and risks, including ethical considerations when applying AI/LLMs in security
- Gain confidence through practice, with case studies and hands-on demonstrations that connect concepts to real scenarios

Course Contents

Foundations of AI/ML Risks and Cybersecurity

Welcome and Introduction
- Training objectives and agenda
- Icebreaker: AI/ML in your organization

AI/ML in Cybersecurity: Theoretical Foundations
- AI/ML in AppSec, SOC, GRC
- Risk foundations of AI/ML systems
- Standards: ISO 42001, NIST AI RMF, OWASP LLM Top 10

Emerging Cyber Risks in AI/ML
- Data leakage, adversarial attacks, model poisoning, supply chain risks
- Case studies: Ransomware on AI-powered claims, vendor data exfiltration
- Group exercise: Mapping risks in participant organizations

Threat Modeling and Adversarial Testing
- Threat modeling for AI/ML systems
- Adversarial examples & robustness testing
- Lab: Adversarial Testing and Threat Modeling

Practical Prompt Engineering and LLM Usage
- Basics of prompt engineering
- Identifying and mitigating hallucinations
- Introduction to Retrieval-Augmented Generation (RAG)
- Lab: Prompt Engineering and Hallucination Mitigation

Course Contents

Security Testing and Secure MLOps

Security Testing Techniques for AI Models
- AI-specific pentesting methodologies
- Vulnerability assessment and scanning tools
- Lab: OWASP LLM Top 10 Vulnerabilities

Secure MLOps and DevSecOps
- Security controls in CI/CD pipelines
- Vulnerability management and monitoring
- Lab: Secure MLOps and DevSecOps

Agentic AI and MCP (Multi-Context Processing)
- Introduction to MCP and agentic AI
- vCISO use case
- Lab: Building and Securing MCP

Jailbreak Ideas and Securing Agentic AI
- Common jailbreak techniques
- Mitigation best practices
- Mapping to OWASP LLM Top 10 and ISO 42001

Course Contents

Advanced Topics and Practical Applications

LLM-Specific Vulnerabilities and Mitigation

- Deep dive: OWASP LLM Top 10
- Threat modeling for LLMs
- Case study: Insurance chatbot exploitation
- Group exercise: Identifying risks in participant systems

Cyber Risk Audit Methodologies and Tools

- MLSecOps, ISO/IEC 42001, NIST AI RMF
- Risk audit planning, execution, and reporting
- Mock audit and incident simulation

Hands-On: NotebookLM and Cybersecurity Projects

- NotebookLM introduction and use cases
- Lab: NotebookLM for Cybersecurity Projects

Creative Applications of LLMs

- Synthetic data, video, and image generation
- Open exploration of innovative AI security applications
- Lab: Creative Applications of LLMs

Wrap-Up and Q&A

- Summary of key takeaways
- Open discussion
- Next steps and resources

Trainer profile

Swapnil Khandekar,

Trainer and Cybersecurity Specialist,
Network Intelligence

Swapnil currently serves as a Senior Cybersecurity Analyst at NII and Senior trainer at IIS. His work mainly focuses on Security training, Vulnerability Assessment, and Penetration Testing for NII. His technical abilities span SOC, Networks, Web Apps, Databases, Digital Forensics, Cloud Security, Red teaming, and ISO Compliance. He has 6+ years of overall experience in the field of Information security and training on relevant topics.

Registration link: https://forms.office.com/r/rKzC7N9eWP