Szkolenie: Mile2
C)AICSO - Certified AI Cybersecurity Officer

Cel szkolenia:

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).

Upon completion

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

Each participant in an authorized Mile2 C)AICSO training held in Compendium CE will receive a free CAICSO Certified AI Cybersecurity Officer exam voucher.

Who Should Attend

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

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

Mile2® is:

ACCREDITED by the NSA CNSS 4011-4016 https://mile2.com/accreditations/

MAPPED to NIST / Homeland Security NICCS's Cyber Security Workforce Framework https://mile2.com/niccs/

APPROVED on the FBI Cyber Security Certification Requirement list (Tier 1-3)

Plan szkolenia:

- What is AI, Really?
  - AI, ML, DL, and LLMs Explained
  - Reinforcement Learning and Generative AI
  - AI System Examples: ChatGPT, Sora, Claude, Gemini, DALLÂ·E
  - The Capabilities and Limitations of Modern AI
- AI Business Applications Across Sectors
  - AI in Customer Service, Healthcare, HR, Fraud, Cyber
  - AI for Decision Augmentation vs Automation
  - Industry-Specific AI Use Cases (Critical Infrastructure, Finance, etc.)
  - Emerging Trends: Agenic AI & Autonomous Agents
- The Architecture of AI Systems
  - Data Pipelines: Ingestion, Cleaning, Feature Engineering
  - Models and Training vs Inference Workflows
  - APIs, Plugins, Cloud vs Edge Deployments
  - Cost, Performance & Scalability Trade-offs
- The Ethical, Legal & Regulatory Terrain
  - AI Bias, Fairness, and Explainability

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- EU AI Act, NIST AI RMF, ISO/IEC 42001, OECD
- Compliance in High-Risk Sectors
- Ethics of Autonomous Agents & Generative Models

- Threat Landscape for AI Systems
  - Prompt Injection, Jailbreaks, Adversarial Inputs
  - Model Inversion, Data Poisoning
  - Hallucinations, Misinformation, and Impersonation
  - Case Examples from 2023–2025
- Infrastructure and Model Supply Chain Risks
  - Insecure Training Environments & Data Lakes
  - Model Theft, Tampering, & Inference Abuse
  - API Abuse and Plugin Vulnerabilities
  - OSINT, Third-Party Risks, and GenAI Abuse
- Securing GenAI Systems
  - OWASP Top 10 for LLMs
  - MITRE ATLAS Threats to AI
  - Red Teaming and Adversarial Testing
  - Hallucination Mitigation Techniques
- Advanced Threat Scenarios
  - GPU Hijacking, Cloud Escalation
  - Synthetic Identity and Deepfake Exploits
  - Autonomous Offensive AI (Agenic AI Threats)
  - Coordinated AI-led Attacks on CI (Critical Infrastructure)
- Secure AI-by-Design Principles
  - Data Minimization and Privacy-Enhanced Learning
  - TEE, Federated Learning, Homomorphic Encryption
  - Threat Modeling for AI Workflows
- AI Risk Management Frameworks
  - NIST AI RMF Deep Dive
  - Implementing ISO/IEC 42001 in the Enterprise
  - Mapping AI Risks to Business Impact
- Identity, Access, and Control for AI Systems
  - Authentication for LLMs
  - RBAC/ABAC for AI APIs
  - Zero Trust Architectures for GenAI Systems
- Cloud-Native AI Security

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- AWS Bedrock, Azure OpenAI, Google Vertex AI
- Cloud Misconfigurations and Exfiltration Paths
- Logging, Threat Detection, and Response

- AI Governance in Complex Organizations
  - Who Owns AI Risk? (CISO/CIO/CTO Debate)
  - AI Ethics Committees, Governance Boards
  - Documentation and Transparency Best Practices
- Auditing and Testing AI
  - AI Red Teaming Methodologies
  - Bias Detection and Fairness Audits
  - Third-Party Evaluation Frameworks
- AI-Centric Incident Response
  - Detection and Containment of AI Exploits
  - Toxic Output and Privacy Leaks
  - Playbooks for Prompt Injection and GenAI Abuse
- Futureproofing and AI Resilience
  - Adaptive Threats: Autonomous and Multi-Modal AI
  - R&D: Simulating Rogue Agents
  - Building Post-AI-Compromise Resilience
- Strategic Exercises and Scenarios
  - Attack Simulation: Policy-Only Scenario Labs
  - Controls Mapping for Different AI Models
  - Designing Security Playbooks
- What Managers Must Ask Quarterly
  - Governance Checklists
  - Architecture Review Questions
  - Prompt Abuse Controls
  - Transparency & Data Governance Updates
- AI Policy Building Blocks
  - Writing a Safe AI Policy from Scratch
  - Mandatory Training and Awareness
  - Defining “High-Risk” and “Low-Risk” Systems
  - Board-Level AI Policy Templates
- Your AI Security Program – End to End
  - Maturity Models for AI Security
  - Role of the CISO, ISO, and Emerging Roles (CAIOs)

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Roadmap for the Next 18–24 Months
- Closing Thoughts & Final Reflection

Wymagania:

Suggested prerequisites:

- Participation in Mile2's C)SP - Certified Security Principles training
- Participation in Mile2's C)CSSM - Certified Cybersecurity Systems Manager training
- 12 months of Information Systems Management Experience

Poziom trudności



Certyfikaty:

The participants will obtain certificates signed by Mile2 (course completion).

This course will help prepare you for the Certified AI Cybersecurity Officer CAICSO exam, which is available through the on-line Mile2's Learning Management System, and is accessible on your 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.

Each participant in an authorized Mile2 C)AICSO training held in Compendium CE will receive a free CAICSO Certified AI Cybersecurity Officer exam voucher.

Prowadzący:

Certified Mile2 Instructor

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001