CompTIA SecAI+

Course code: CTSAI

CompTIA SecAI+ is a modern certification focused on the secure deployment, management, and protection of systems using artificial intelligence. The course covers the fundamental principles of artificial intelligence, securing AI solutions, the use of AI in cybersecurity, and governance, risk management, and compliance requirements. Participants will learn to identify security risks associated with AI, implement appropriate security measures, and use AI to support security operations. The course is designed as preparation for the CompTIA SecAI+ (CY0-001) certification exam.

Affiliate	Duration	Course price	ITB
Praha	4	30 800 Kč	40
Brno	4	30 800 Kč	40
Bratislava	4	1 380 €	40

The prices are without VAT.

Course terms

Date	Duration	Course price	Type	Course language	Location

The prices are without VAT.

Who the course is intended for

The course is suitable especially for:

- Security analysts
- SOC analysts
- Cybersecurity specialists
- Security administrators
- Cloud Security specialists
- DevSecOps engineers
- Security architects
- AI Security specialists
- IT consultants
- Administrators of AI and ML platforms
- Candidates preparing for the CompTIA SecAI+ certification

Required prerequisite knowledge

Participants should have:

- basic knowledge of computer networks and operating systems,
- basic orientation in cybersecurity,
- knowledge at the level of CompTIA Security+, CySA+, or equivalent experience is recommended,
- approximately 2 years of experience in cybersecurity.

Course outline

- AI Fundamentals in Cybersecurity
- Artificial intelligence, machine learning, and deep learning
- Generative AI
- Large Language Models (LLM)
- Small Language Models (SLM)
- Natural Language Processing (NLP)
- Generative Adversarial Networks (GAN)
- Transformers

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

- Current trends of AI in cybersecurity
- Practical use of AI in enterprise environments
- Machine Learning and the AI Lifecycle
- Supervised Learning
- Unsupervised Learning
- Reinforcement Learning
- Model training
- Testing and validation of models
- Model fine-tuning
- Epochs, pruning, and quantization
- AI Development Lifecycle
- Model monitoring
- Human-in-the-loop
- Data Security and Prompt Engineering
- Types of data used for AI
- Data lineage
- Data provenance
- Data integrity
- Data quality management
- Prompt engineering
- Zero-shot prompting
- One-shot prompting
- Multi-shot prompting
- Prompt templates
- Prompt injection attacks
- Protection of generative AI systems
- AI Architecture and Components
- AI models
- AI agents
- AI services
- API interfaces
- Embeddings
- Retrieval-Augmented Generation (RAG)
- Vector databases
- Enterprise AI architectures
- Integrating AI into enterprise applications
- Securing AI Systems
- AI attack surface
- Secure AI architecture
- Identity and Access Management (IAM)
- Least privilege
- Segregation of duties
- API security
- Secrets management
- Data encryption
- Protection of training data
- Protection of models
- Protection of inference services

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

- AI Threats and Attacks
- Prompt injection
- Jailbreaking AI models
- Data poisoning
- Model poisoning
- Adversarial machine learning
- Membership inference attacks
- Model extraction
- Model theft
- Data leakage
- Hallucinations
- Supply chain attacks against AI solutions
- Secure AI Development and MLOps
- Secure SDLC
- DevSecOps for AI environments
- MLOps
- CI/CD pipeline for AI
- Model governance
- Security testing
- AI model validation
- Monitoring AI systems
- AI-Assisted Security Operations
- AI in the Security Operations Centre (SOC)
- AI for SIEM tools
- Correlation of security events
- Automation of security processes
- Threat hunting using AI
- Prioritization of security incidents
- AI-assisted security analytics
- AI for Incident Response
- AI-assisted triage
- Log analysis using AI
- Root Cause Analysis
- Automated incident investigation
- Malware analysis
- Forensic analysis
- Automation of incident response
- Vulnerability Management and Threat Intelligence
- Prioritization of vulnerabilities
- Risk scoring
- Exposure analysis
- Asset discovery
- Threat intelligence
- IOC analysis
- TTP correlation
- MITRE ATT&CK framework
- Predictive threat analysis
- AI Governance and Responsible AI

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

- Governance frameworks for AI
- Responsible AI
- Explainability
- Transparency
- Accountability
- AI Ethics
- Organizational policies
- AI lifecycle management
- AI Risk Management and Compliance
- Risk Assessment
- AI Risk Register
- Risk Treatment
- Business Impact Analysis
- Audit of AI solutions
- NIST AI Risk Management Framework
- ISO/IEC 42001
- GDPR and AI
- EU AI Act
- Compliance requirements for AI solutions
- Certification Exam Preparation
- Overview of certification domains
- Question types
- Performance-Based Questions (PBQ)
- Practical scenarios
- Practice tests
- Exam Tips &Tricks
- Final review

Hands-on exercises

The course includes lab exercises focused on:

- analyzing AI security risks,
- designing a secure AI architecture,ň
- protecting models and datasets,
- detecting and mitigating AI attacks,
- AI support for security operations,
- AI-assisted threat hunting,
- AI governance and risk assessment,
- solving scenarios similar to the certification exam.

Certification exam

The course prepares participants for the CompTIA SecAI+ (CY0-001) exam

Exam domains:

- Basic AI Concepts Related to Cybersecurity – 17 %
- Securing AI Systems – 40 %
- AI-Assisted Security – 24 %
- AI Governance, Risk and Compliance – 19 % [examsdigest.com], [onlc.com]

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk