

Kód kurzu: CTSAI

CompTIA SecAI+ je moderná certifikácia zameraná na bezpečné nasadenie, správu a ochranu systémov využívajúcich umelú inteligenciu. Kurz pokrýva základné princípy umelej inteligencie, zabezpečenie AI riešení, využitie AI v kybernetickej bezpečnosti a požiadavky na governance, risk management a compliance. Účastníci sa naučia identifikovať bezpečnostné riziká spojené s AI, implementovať vhodné bezpečnostné opatrenia a využívať AI na podporu bezpečnostných operácií. Kurz je určený ako príprava na certifikačnú skúšku CompTIA SecAI+ (CY0-001).

## Pre koho je kurz určený

Kurz je vhodný najmä pre:

- Security analytikov
- SOC analytikov
- Cybersecurity špecialistov
- Security administrátorov
- Cloud Security špecialistov
- DevSecOps inžinierov
- Security architektov
- AI Security špecialistov
- IT konzultantov
- Administrátorov AI a ML platforiem
- Kandidátov pripravujúcich sa na certifikáciu CompTIA SecAI+

## Požadované vstupné znalosti

Účastník by mal mať:

- základné znalosti počítačových sietí a operačných systémov,
- základnú orientáciu v kybernetickej bezpečnosti,
- odporúča sa znalosť na úrovni CompTIA Security+, CySA+ alebo ekvivalentná prax,
- približne 2 roky skúseností v oblasti kybernetickej bezpečnosti.

## Osnova kurzu

- Základy AI v kybernetickej bezpečnosti
- Umelá inteligencia, strojové učenie a deep learning
- Generatívna AI
- Large Language Models (LLM)
- Small Language Models (SLM)
- Natural Language Processing (NLP)
- Generative Adversarial Networks (GAN)
- Transformer
- Súčasné trendy AI v kybernetickej bezpečnosti
- Praktické využitie AI v podnikových prostrediach
- Machine Learning a životný cyklus AI
- Supervised Learning
- Unsupervised Learning
- Reinforcement Learning
- Tréning modelov
- Testovanie a validácia modelov
- Fine-tuning modelov
- Epochs, pruning a quantization
- AI Development Lifecycle

### GOPAS Praha

Na Strži 2097/63  
140 00 Praha 4 - Krč  
Tel.: +420 226 201 390  
[info@gopas.cz](mailto:info@gopas.cz)

### GOPAS Brno

Nové sady 996/25  
602 00 Brno  
Tel.: +420 530 513 590  
[info@gopas.cz](mailto:info@gopas.cz)

### GOPAS Bratislava

Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 902 903 132  
[info@gopas.sk](mailto:info@gopas.sk)



Copyright © 2026 GOPAS, a.s.,  
All rights reserved

- Monitoring modelov
- Human-in-the-loop
- Bezpečnosť dát a Prompt Engineering
- Typy dát používaných pre 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 útoky
- Ochrana generatívnych AI systémov
- AI architektúra a komponenty
- AI modely
- AI agenti
- AI služby
- API rozhrania
- Embeddings
- Retrieval-Augmented Generation (RAG)
- Vector databases
- Enterprise AI architektúry
- Integrácia AI do podnikových aplikácií
- Zabezpečenie AI systémov
- AI attack surface
- Secure AI architecture
- Identity and Access Management (IAM)
- Least privilege
- Segregation of duties
- API security
- Secrets management
- Šifrovanie dát
- Ochrana tréningových dát
- Ochrana modelov
- Ochrana inferenčných služieb
- AI hrozby a útoky
- Prompt injection
- Jailbreaking AI modelov
- Data poisoning
- Model poisoning
- Adversarial machine learning
- Membership inference attacks
- Model extraction
- Model theft
- Data leakage
- Hallucinations

**GOPAS Praha**

Na Strži 2097/63  
140 00 Praha 4 - Krč  
Tel.: +420 226 201 390  
[info@gopas.cz](mailto:info@gopas.cz)

**GOPAS Brno**

Nové sady 996/25  
602 00 Brno  
Tel.: +420 530 513 590  
[info@gopas.cz](mailto:info@gopas.cz)

**GOPAS Bratislava**

Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 902 903 132  
[info@gopas.sk](mailto:info@gopas.sk)



Copyright © 2026 GOPAS, a.s.,  
All rights reserved

- Supply chain útoky proti AI riešeniam
- Secure AI Development a MLOps
- Secure SDLC
- DevSecOps pre AI prostredia
- MLOps
- CI/CD pipeline pre AI
- Model governance
- Security testing
- Validácia AI modelov
- Monitoring AI systémov
- AI-Assisted Security Operations
- AI v Security Operations Centre (SOC)
- AI pre SIEM nástroje
- Korelácia bezpečnostných udalostí
- Automatizácia bezpečnostných procesov
- Threat hunting pomocou AI
- Prioritizácia bezpečnostných incidentov
- AI-assisted security analytics
- AI pre Incident Response
- AI-assisted triage
- Analýza logov pomocou AI
- Root Cause Analysis
- Automatizované vyšetřovanie incidentov
- Malware analysis
- Forenzná analýza
- Automatizácia reakcie na incident
- Vulnerability Management a Threat Intelligence
- Prioritizácia zraniteľností
- Risk scoring
- Exposure analysis
- Asset discovery
- Threat intelligence
- IOC analýza
- TTP korelácia
- MITRE ATT&CK framework
- Prediktívna analýza hrozieb
- AI Governance a Responsible AI
- Governance rámce pre AI
- Responsible AI
- Explainability
- Transparency
- Accountability
- AI Ethics
- Organizačné politiky
- Riadenie životného cyklu AI
- AI Risk Management a Compliance
- Risk Assessment
- AI Risk Register

**GOPAS Praha**

Na Strži 2097/63  
140 00 Praha 4 - Krč  
Tel.: +420 226 201 390  
[info@gopas.cz](mailto:info@gopas.cz)

**GOPAS Brno**

Nové sady 996/25  
602 00 Brno  
Tel.: +420 530 513 590  
[info@gopas.cz](mailto:info@gopas.cz)

**GOPAS Bratislava**

Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 902 903 132  
[info@gopas.sk](mailto:info@gopas.sk)



Copyright © 2026 GOPAS, a.s.,  
All rights reserved

- Risk Treatment
- Business Impact Analysis
- Audit AI riešení
- NIST AI Risk Management Framework
- ISO/IEC 42001
- GDPR a AI
- EU AI Act
- Compliance požiadavky pre AI riešenia
- Príprava na certifikačnú skúšku
- Prehľad certifikačných domén
- Typy otázok
- Performance-Based Questions (PBQ)
- Praktické scenáre
- Skúšobné testy
- Exam Tips & Tricks
- Záverečné opakovanie

## Praktické cvičenia

Súčasťou kurzu sú laboratórne cvičenia zamerané na:

- analýzu AI bezpečnostných rizík,
- návrh bezpečnej AI architektúry,
- ochranu modelov a dátových súborov,
- detekciu a mitigáciu AI útokov,
- AI podporu bezpečnostných operácií,
- AI-assisted threat hunting,
- AI governance a risk assessment,
- riešenie scenárov podobných certifikačnej skúške.

## Certifikačná skúška

Kurz pripravuje na skúšku CompTIA SecAI+ (CY0-001)

Domény skúšky:

- 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](mailto:info@gopas.cz)

### GOPAS Brno

Nové sady 996/25  
602 00 Brno  
Tel.: +420 530 513 590  
[info@gopas.cz](mailto:info@gopas.cz)

### GOPAS Bratislava

Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 902 903 132  
[info@gopas.sk](mailto:info@gopas.sk)



Copyright © 2026 GOPAS, a.s.,  
All rights reserved