CompTIA SecurityX

Kód kurzu: CTSX

Tento štvordňový kurz je prípravou na certifikačnú skúšku CompTIA SecurityX (CAS-005), určenú bezpečnostným architektom a senior security inžinierom. SecurityX sa venuje návrhu zabezpečenia podnikového prostredia, a to on-premises, v cloude aj v hybridnom modeli. Kurz preto stavia na scenároch a rozhodovaní: akú kontrolu zvoliť a ako ju zosúladiť s reguláciou a rizikami organizácie. Kurz pokrýva štyri domény skúšky: Governance, Risk, and Compliance; Security Architecture; Security Engineering a Security Operations. Osnova nižšie vychádza z modulov oficiálneho kurzu CompTIA, ktorých členenie sa od domén skúšky čiastočne líši.

Pobočka	Dní	Katalógová cena	ITB
Praha	4	37 300 Kč	40
Brno	4	37 300 Kč	40
Bratislava	4	1 680 €	40

Všetky ceny sú uvedené bez DPH.

Termíny kurzu

Dátum	Dní	Cena kurzu	Typ výučby	Jazyk výučby	Lokalita

Všetky ceny sú uvedené bez DPH.

Pre koho je kurz určený

Kurz je určený odborníkom, ktorí bezpečnosť navrhujú a zodpovedajú za ňu, nielen ju prevádzkujú.

- bezpečnostní architekti a senior security inžinieri
- security auditori, ktorí hodnotia účinnosť kontrol
- technickí lídri SOC a incident response tímov
- cloud a infraštruktúrni architekti, ktorí zodpovedajú za bezpečnosť hybridného prostredia
- špecialisti GRC, ktorí potrebujú technický základ pre rozhodovanie o rizikách

Čo Vás naučíme

Po absolvovaní kurzu budete vedieť v konkrétnom scenári:

- nastaviť governance bezpečnostného programu: politiky, frameworky, change management a pravidlá pre používanie AI v organizácii
- posúdiť dopad regulácie a štandardov na bezpečnostnú stratégiu
- riadiť riziká vrátane rizika tretích strán a AI a pripraviť organizáciu na krízovú situáciu a únik dát
- modelovať hrozby a určiť, ktoré z nich sa týkajú vašej útočnej plochy
- navrhnúť odolnú a bezpečnú architektúru pre on-premises, cloud aj hybrid a zapracovať do nej princípy Zero Trust
- zabezpečiť životný cyklus softvéru od požiadaviek cez CI/CD a supply chain až po vyradenie systému
- navrhnúť a diagnostikovať IAM: federation, conditional access, privileged access a PKI
- spevniť koncové body, siete a špecializované systémy, vrátane ICS/OT a legacy prostredí, využiť hardvérovú bezpečnosť (TPM, HSM, secure a measured boot) a vyriešiť zložité sieťové problémy
- zvoliť správnu kryptografiu pre daný prípad použitia a pripraviť sa na prechod na post-quantum algoritmy
- automatizovať bezpečnosť pomocou skriptov, SOAR a generatívnej AI
- analyzovať dáta z monitoringu, robiť threat hunting s využitím threat intelligence a odporučiť mitigácie zraniteľností

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

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

• viesť analýzu incidentu od detekcie cez forenznú analýzu a analýzu malvéru až po poučenie z incidentu

Požadované vstupné znalosti

Vhodným základom sú znalosti na úrovni Security+ a CySA+ alebo PenTest+, výhodou sú Network+ a Cloud+. Kurz nevysvetľuje základy (čo je firewall, PKI, SIEM) a pri každej téme prechádza rovno k návrhu a rozhodovaniu.

Študijné materiály

Účastníci obdržia oficiálne študijné materiály od CompTIA a prístup k lab cvičeniam – to všetko s prístupom 12 mesiacov.

Osnova kurzu

Governance, Risk, and Compliance

- Governance komponenty – bezpečnostná dokumentácia a riadenie bezpečnostného programu, governance frameworky, change a configuration management, GRC nástroje, data governance v staging prostrediach, právne a privacy dopady používania AI
- Právny súlad (compliance) – odvetvové regulácie a štandardy, security a reporting frameworky, audit vs. assessment vs. certifikácia, ochrana súkromia (GDPR a ďalšie), súlad naprieč jurisdikciami
- Riadenie rizík – impact analysis, risk assessment a risk management, third-party risk, riziká dostupnosti, dôvernosti, integrity a súkromia, riziká používania AI, krízový manažment a reakcia na únik dát (breach response)

Architektúra a dizajn

- Bezpečnosť vývoja softvéru – bezpečnostné požiadavky, software a hardware assurance, CI/CD, supply chain risk management, end-of-life systémy
- Bezpečná architektúra – attack surface management, podpora detekcie a threat huntingu v návrhu, dizajn ochrany dát a DLP, hybridná infraštruktúra, integrácie tretích strán, účinnosť kontrol
- Prevádzková odolnosť – dostupnosť a integrita v návrhu, inšpekcia sieťovej prevádzky, NAC a VPN, proxy, špecializované komponenty
- Cloudová infraštruktúra – CASB a detekcia shadow IT, shared responsibility model, CI/CD pipeline, infrastructure as code a správa konfigurácie (Terraform, Ansible), bezpečnosť kontajnerov a orchestrácie, serverless, API security, ochrana dát v cloude, šifrovacie kľúče spravované poskytovateľom vs. zákazníkom, cloud control strategies, konektivita a integrácia cloudových služieb
- Zero Trust – kontinuálna autorizácia a kontextová reautentifikácia, sieťová architektúra, validácia API, identifikácia a atestácia aktív, bezpečnostné hranice a deperimeterizácia, vzťahy subject–object
- AAA a IAM – provisioning a deprovisioning, federation, conditional access, identity a service providers, policy decision a enforcement points, modely riadenia prístupu, PKI architektúra, biometria, secrets management, IAM politiky v cloude, privileged identity management, riešenie problémov s IAM

Security Engineering

- Bezpečnosť koncových bodov – EDR, endpoint privilege management, nástroje ochrany endpointov, MDM, TTPs útočníkov, špecializované, embedded a legacy systémy (ICS/OT) a ich odvetvové špecifiká
- Sieťová infraštruktúra – riešenie zložitých problémov: chybné konfigurácie siete, IDS/IPS, observability, bezpečnosť DNS, bezpečnosť e-mailu, kryptografické problémy, vyčerpanie zdrojov
- Hardvérová bezpečnosť a automatizácia – hardvérové bezpečnostné technológie a funkcie, útoky na hardvér a firmvér (firmware tampering, BIOS/UEFI, USB), skriptovanie, plánovanie a event triggers, generatívna AI v bezpečnosti, SOAR a workflow automatizácia
- Pokročilá kryptografia – post-quantum kryptografia, key stretching, key splitting a envelope encryption, homomorfné šifrovanie a secure multiparty computation, forward secrecy a AEAD, výkon vs. bezpečnosť, ochrana dát v rôznych stavoch, blockchain, integrita a pôvod softvéru

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

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

Security Operations a Incident Response

- Threat modeling – profilovanie hrozieb, štruktúrované hodnotenie hrozieb, určenie útočnej plochy, aplikovateľnosť hrozieb na organizáciu, hrozby pre AI modely (prompt injection, data poisoning, model theft a model inversion), útoky s podporou AI (deepfakes) a bezpečné nasadenie AI asistentov
- Bezpečnostný monitoring – zber a integrácia dát v SIEM, spracovanie dát a behaviorálny baseline, alerting, reporting a metriky
- Útoky a mitigácie – zraniteľnosti vstupu a výstupu, pamäte a vykonávania kódu, kryptografie, konfigurácie a supply chain, k nim zodpovedajúce mitigácie a secure coding
- Threat hunting a threat intelligence – interné a externé zdroje spravodajstva, counterintelligence a OPSEC, threat intelligence platformy, zdieľanie IoC, pravidlové jazyky (YARA, Sigma, Snort)
- Analýza a reakcia na incidenty – analýza malvéru, forenzná analýza, detekcia a prvotná analýza, prevencia a pripravenosť, kontinuálne zlepšovanie

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

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