CompTIA SecurityX

Kód kurzu: CTSX

Tento čtyřdenní kurz je přípravou na certifikační zkoušku CompTIA SecurityX (CAS-005), určenou bezpečnostním architektům a senior security inženýrům. SecurityX se věnuje návrhu zabezpečení podnikového prostředí, a to on-premises, v cloudu i v hybridním modelu. Kurz vychází z praktických situací, v nichž budete rozhodovat, jaké bezpečnostní opatření zvolit a jak ho sladit s regulatorními požadavky a riziky organizace. Kurz pokrývá čtyři oblasti zkoušky: Governance, Risk, and Compliance; Security Architecture; Security Engineering a Security Operations. Osnova níže vychází z modulů oficiálního kurzu CompTIA, jejichž členění se od jednotlivých sekcí zkoušky částečně liší.

Pro koho je kurz určen

Kurz je určen odborníkům, kteří bezpečnost navrhují a zodpovídají za ni, nejen ji provozují.

- bezpečnostní architekti a senior security inženýři
- security auditoři, kteří hodnotí účinnost kontrol
- techničtí lídři SOC a incident response týmů
- cloud a infrastrukturní architekti, kteří zodpovídají za bezpečnost hybridního prostředí
- specialisté GRC, kteří potřebují technický základ pro rozhodování o rizicích

Co Vás naučíme

Po absolvování kurzu budete umět v konkrétním scénáři:

- nastavit governance bezpečnostního programu: politiky, frameworky, change management a pravidla pro používání AI v organizaci
- posoudit dopad regulace a standardů na bezpečnostní strategii
- řídit rizika včetně rizik třetích stran a AI a připravit organizaci na krizovou situaci a únik dat
- modelovat hrozby a určit, které z nich se týkají vaší útočné plochy
- navrhnout odolnou a bezpečnou architekturu pro on-premises, cloud i hybrid a zapracovat do ní principy Zero Trust
- zabezpečit životní cyklus softwaru od požadavků přes CI/CD a supply chain až po vyřazení systému
- navrhnout a diagnostikovat IAM: federation, conditional access, privileged access a PKI
- provést hardening koncových bodů, sítí a specializovaných systémů, včetně ICS/OT a legacy prostředí, využít hardwarovou bezpečnost (TPM, HSM, secure a measured boot) a vyřešit složité síťové problémy
- zvolit správnou kryptografii pro daný případ použití a připravit se na přechod na post-quantum algoritmy
- automatizovat bezpečnost pomocí skriptů, SOAR a generativní AI
- analyzovat data z monitoringu, provádět threat hunting s využitím threat intelligence a doporučit mitigace zranitelností
- vést analýzu incidentu od detekce přes forenzní analýzu a analýzu malwaru až po poučení z incidentu

Požadované vstupní znalosti

Vhodným základem jsou znalosti na úrovni kurzů Security+ a CySA+ nebo PenTest+, výhodou Network+ a Cloud+. Kurz nevysvětluje základy (co je firewall, PKI, SIEM) a u každého tématu přechází rovnou k návrhu a rozhodování.

Studijní materiály

Účastníci obdrží oficiální studijní materiály od CompTIA a přístup k lab cvičením po dobu 12 měsíců.

Osnova kurzu

Governance, Risk, and Compliance

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

- Governance komponenty – bezpečnostní dokumentace a řízení bezpečnostního programu, governance frameworky, change a configuration management, GRC nástroje, data governance ve staging prostředích, právní a privacy dopady používání AI
- Právní soulad (compliance) – odvětvové regulace a standardy, security a reporting frameworky, audit vs. assessment vs. certifikace, ochrana soukromí (GDPR a další), soulad napříč jurisdikcemi
- Řízení rizik – impact analysis, risk assessment a risk management, third-party risk, rizika dostupnosti, důvěrnosti, integrity a soukromí, rizika používání AI, krizový management a reakce na únik dat (breach response)

Architektura a design

- Bezpečnost vývoje softwaru – bezpečnostní požadavky, software a hardware assurance, CI/CD, supply chain risk management, end-of-life systémy
- Bezpečná architektura – attack surface management, podpora detekce a threat huntingu v návrhu, design ochrany dat a DLP, hybridní infrastruktura, integrace třetích stran, účinnost kontrol
- Provozní odolnost – dostupnost a integrita v návrhu, inspekce síťového provozu, NAC a VPN, proxy, specializované komponenty
- Cloudová infrastruktura – CASB a detekce shadow IT, shared responsibility model, CI/CD pipeline, infrastructure as code a správa konfigurace (Terraform, Ansible), bezpečnost kontejnerů a orchestrace, serverless, API security, ochrana dat v cloudu, šifrovací klíče spravované poskytovatelem vs. zákazníkem, cloud control strategies, konektivita a integrace cloudových služeb
- Zero Trust – kontinuální autorizace a kontextová reautentizace, síťová architektura, validace API, identifikace a atestace aktiv, bezpečnostní hranice a deperimetrizace, vztahy subject–object
- AAA a IAM – provisioning a deprovisioning, federation, conditional access, identity a service providers, policy decision a enforcement points, modely řízení přístupu, architektura PKI, biometrie, secrets management, IAM politiky v cloudu, privileged identity management, řešení problémů s IAM

Security Engineering

- Bezpečnost koncových bodů – EDR, endpoint privilege management, nástroje ochrany endpointů, MDM, TTPs útočníků, specializované, embedded a legacy systémy (ICS/OT) a jejich odvětvová specifika
- Síťová infrastruktura – řešení složitých problémů: chybné konfigurace sítě, IDS/IPS, observability, bezpečnost DNS, bezpečnost e-mailu, kryptografické problémy, vyčerpání zdrojů
- Hardwarová bezpečnost a automatizace – hardwarové bezpečnostní technologie a funkce, útoky na hardware a firmware (firmware tampering, BIOS/UEFI, USB), skriptování, plánování a event triggers, generativní AI v bezpečnosti, SOAR a workflow automatizace
- Pokročilá kryptografie – post-quantum kryptografie, key stretching, key splitting a envelope encryption, homomorfní šifrování a secure multiparty computation, forward secrecy a AEAD, výkon vs. bezpečnost, ochrana dat v různých stavech, blockchain, integrita a původ softwaru

Security Operations a Incident Respons

- Threat modeling – profilování hrozeb, strukturované hodnocení hrozeb, určení útočné plochy, aplikovatelnost hrozeb na organizaci, hrozby pro AI modely (prompt injection, data poisoning, model theft a model inversion), útoky s podporou AI (deepfakes) a bezpečné nasazení AI asistentů
- Bezpečnostní monitoring – sběr a integrace dat v SIEM, zpracování dat a behaviorální baseline, alerting, reporting a metriky
- Útoky a mitigace – zranitelnosti vstupu a výstupu, paměti a provádění kódu, kryptografie, konfigurace a supply chain, odpovídající mitigace a secure coding
- Threat hunting a threat intelligence – interní a externí zdroje zpravodajství, counterintelligence a OPSEC, threat intelligence platformy, sdílení IoC, pravidlové jazyky (YARA, Sigma, Snort)
- Analýza a reakce na incidenty – analýza malwaru, forenzní analýza, detekce a prvotní analýza, prevence a připravenost, kontinuální zlepšování

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