Understanding Cisco Cybersecurity Operations Fundamentals

Kód kurzu: CBROPS

V kurzu Understanding Cisco Cybersecurity Operations Fundamentals jsou účastníci prováděni základními bezpečnostními koncepty, běžnými síťovými a aplikačními útoky a typy dat, které jsou nutné pro vyšetřování kybernetických bezpečnostních incidentů.Kurz vás naučí znalosti potřebné pro sledování bezpečnostních upozornění a průniků, dále pochopíte a dokážete následovat procedury, které vám umožní efektivně reagovat na bezpečnostní upozornění a efektivně převést relevantní informace k popisu incidentů. Kurz vám pomůže se připravit na certifikační zkoušku Cisco Certified CyberOps Associate a získat vědomosti pro práci jako cybersecurity operations analytika v týmu Security Operation Center (SOC).

Pobočka	Dnů	Cena kurzu	ITB
Praha	5	65 000 Kč	0
Brno	5	65 000 Kč	0
Bratislava	5	2 690 €	0

Uvedené ceny jsou bez DPH.

Termíny kurzu

Datum	Dnů	Cena kurzu	Typ výuky	Jazyk výuky	Lokalita

Uvedené ceny jsou bez DPH.

Formát školení

Standardně realizujeme kurz prezenční formou (onsite neboli ILT*) v ALEF Training centru. Po domluvě je možné zrealizovat kurz v prostorách klienta. Kurz je také možné realizovat formou on-line (vILT**) prostřednictvím videokonferenční platformy - Cisco Webex Meetings. Virtuální školení vedené instruktorem představuje kombinaci toho nejlepšího z tradičního kurzu v učebně a interaktivního školení bez nutnosti opouštět vlastní kancelář či pohodlí Vašeho domova. Přesvědčte se o špičkové kvalitě přenosu, videohovorů a efektivní týmové spolupráci.
Vysvětlivky: ILT - Instructor Led-Training - školení vedené instruktorem v učebně. ** vILT (Virtual Instructor-Led Training) - jde o formu distančního vzdělávání, kde instruktor vede školení z učebny prostřednictvím online platformy, na kterou se připojují studenti ze své kanceláře nebo pohodlí svého domova.

Požadované vstupní znalosti

- Základní znalost Ethernet a TCP/IP síťových protokolů
- Základní znalost práce s operačními systémy Windows a Linux
- Seznámení se základy konceptů síťové bezpečnosti

Studijní materiály

Účastníci obdrží přístup k elektronické verzi studijních materiálů.

Osnova kurzu

Po dokončení kurzu budete schopni:

- Vysvětlit, jak funguje Security Operations Center (SOC), a popsat různé typy služeb, které jsou poskytovány z pohledu Tier 1 SOC analytika.
- Popsat Network Security Monitoring (NSM) nástroje, které jsou analytikům k dispozici.
- Popsat data, která jsou analytikům k dispozici.
- Vysvětlit základní koncepty a užití kryptografie.
- Popsat bezpečnostní chyby v protokolu TCP/IP a způsob, jakým je lze využít k útoku na sítě a hostitele.

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

- Porozumět běžným technologiím zabezpečení koncových bodů.
- Porozumět modelu Kill Chain a Diamond modelu k vyšetřování bezpečnostních incidentů.
- Identifikace zdrojů potřebných pro Threat Hunting.
- Vysvětlit potřebu normalizace dat událostí a korelace událostí.
- Identifikovat běžné vektory útoků.
- Identifikovat škodlivé aktivity.
- Identifikovat vzorce podezřelého chování.
- Provádět vyšetřování kybernetických bezpečnostních incidentů.
- Vysvětlení používání typického playbooku v SOC.
- Vysvětlení metrik pro měření efektivity SOC týmu.
- Popsat typický plán reakce na kybernetické bezpečnostní incidenty a funkci týmu pro reakci na tyto incidenty (CSIRT)

Technické vybavení

Virtualizované LAB prostředí pro interaktivní studium a praktické procvičení získaných znalostí.

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