

# CompTIA Cybersecurity Analyst (CySA+)






Kód kurzu: CTCA

Tento päťdňový kurz je určený administrátorom, najmä správcom sietí a bezpečnostným adminom, ktorí sú zodpovední za bezpečnosť alebo majú záujem vidieť pod povrch očami bezpečnostného analytika. Kurz je ideálny pre každého, kto pracuje ako analytik ohrození a rizík, bezpečnostný špecialista, člen SOC tímu. Kurz je zároveň určený každému, kto má záujem získať celosvetovo uznávanú certifikáciu CompTIA CySA+.

Pobočka	Dní	Katalógová cena	ITB
Praha	5	33 900 Kč	50
Brno	5	33 900 Kč	50
Bratislava	5	1 480 €	50

Všetky ceny sú uvedené bez DPH.

## Termíny kurzu

Dátum	Dní	Cena kurzu	Typ výučby	Jazyk výučby	Lokalita
 18.05.2026	5	1 480 €	Online	CZ/SK	Online
 18.05.2026	5	33 900 Kč	Online	CZ/SK	Online
 19.10.2026	5	1 480 €	Teleprezenčný	CZ/SK	GOPAS Bratislava
 19.10.2026	5	33 900 Kč	Teleprezenčný	CZ/SK	GOPAS Praha
 19.10.2026	5	33 900 Kč	Teleprezenčný	CZ/SK	GOPAS Brno

Všetky ceny sú uvedené bez DPH.

## Pre koho je kurz určený

Kurz je určený administrátorom, najmä správcom sietí a bezpečnostných adminom, ktorí sú zodpovední za bezpečnosť alebo majú záujem vidieť pod povrch očami bezpečnostného analytika. Kurz je ideálny pre každého, kto pracuje ako analytik ohrození a rizík, bezpečnostný špecialista, člen SOC tímu.

Kurz je zároveň určený každému, kto má záujem získať celosvetovo uznávanú certifikáciu CompTIA CySA+.

## Čo Vás naučíme

- Získať a využiť bezpečnostné informácie
- Identifikovať typy útočníkov a techniky útokov
- Vyhodnotiť bezpečnostné informácie a riziká
- Analyzovať dáta získané z logov a sieťových paketov
- Rozpoznať a identifikovať bezpečnostné incidenty pomocou forenzných nástrojov
- Implementovať manažment slabín
- Porozumieť významu rôznych bezpečnostných opatrení
- Vysvetliť bezpečnostné otázky z pohľadu architektúry sietí, cloudov a životného cyklu aplikácií

## Požadované vstupné znalosti

Na absolvovanie kurzu CySA+ sú vhodné znalosti na úrovni kurzov CompTIA Network+ a CompTIA Security+ alebo kurzy im zodpovedajúce.

## Študijné materiály

Študijné materiály spoločnosti Comptia

Účastníci školenia získajú prístup k študijným materiálom na obdobie 12 mesiacov, vrátane prístupu do virtuálneho prostredia, kde môžu opakovane prechádzať jednotlivé laby.

**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

# CompTIA Cybersecurity Analyst (CySA+)

## Osnova kurzu

### Význam bezpečnostných opatrení

- Identifikácia typov opatrení
- Význam dát a informácií

### Využitie dát a informácií

- Klasifikácia ohrození a typy útočníkov
- Použitie rámcov útokov a manažment indikátorov
- Použitie modelovania a vyhľadávacích metód

### Analýza dát

- Analýza sieťového monitoringu
- Analýza monitorovania bezpečnostných zariadení
- Analýza monitorovania koncových zariadení
- Analýza monitorovania mailovej komunikácie

### Zber a analýza dát

- Konfigurácia logov a použitie SIEM nástrojov
- Analýza a vyhľadávanie logov a dát v SIEM systémoch

### Využitie forenzných techník a analýza indikátorov

- Identifikácia forenzných techník
- Analýza sieťových indikátorov
- Analýza host indikátorov
- Analýza aplikačných indikátorov
- Analýza vedľajších indikátorov

### Aplikácia procesov reakcie na incident

- Procesy reakcie na incident
- Aplikácia detekčných a kontrolných opatrení
- Aplikácia opatrení obnovy a poincidenčných opatrení

### Znižovanie rizík

- Identifikácia rizík a prioritizovanie procesov
- Bezpečnostné rámce, politiky a procesy

### Manažment slabín

- Analýza výstupov z vyhľadávacích nástrojov
- Konfigurácia parametrov vyhľadávania slabín
- Analýza výstupov skenerov
- Odstraňovanie slabín

### Aplikovanie bezpečnostných riešení manažmentu infraštruktúry

- Identifikácia a manažment bezpečnostných riešení
- Sieťová architektúra a segmentácia bezpečnostných riešení
- Slabiny špeciálnych technológií

### Súkromie a ochrana dát

- Identifikácia netechnických dát a opatrenia na ich zabezpečenie
- Identifikácia technických dát a opatrenia na ich zabezpečenie

### Aplikovanie bezpečnostných riešení

- Mitigácia softvérových slabín a útokov
- Mitigácia webových slabín a útokov
- Analýza výstupov z aplikácií

### Aplikácia bezpečnostných riešení pre cloud a automatizácia

#### 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

# CompTIA Cybersecurity Analyst (CySA+)

- Identifikácia cloudových služieb a slabín
- Architektúra orientovaná na služby
- Analýza výstupov z cloudových nástrojov

## **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