

# CORTEX XDR : Investigation and Analysis

Kód kurzu: EDU-262

This 2-day course is an XDR training course that's focused on the role of the XDR Analyst. This is an update and replacement for the previous Investigation and Response, specifically intended for a wide range of security professionals, including SOC, CERT, CSIRT, and XDR analysts, managers, incident responders, and threat hunters.

Pobočka	Dnů	Cena kurzu	ITB
Praha	2	24 900 Kč	0
Brno	2	24 900 Kč	0
Bratislava	2	1 030 €	0

Uvedené ceny jsou bez DPH.

## Termíny kurzu

Datum	Dnů	Cena kurzu	Typ výuky	Jazyk výuky	Lokalita
11.05.2026	2	24 900 Kč	Online	CZ/SK	TD SYNEX Czech - Online
11.05.2026	2	24 900 Kč	Prezenční	CZ/SK	TD SYNEX Czech

Uvedené ceny jsou bez DPH.

## Pro koho je kurz určen

This course is for a wide range of security professionals, including SOC, CERT, CSIRT, and XDR analysts, managers, incident responders, and threat hunters. It is also well-suited for professional-services consultants, sales engineers, and service delivery partners.

## Co Vás naučíme

The course is designed to enable cybersecurity professionals, particularly those in SOC/CERT/CSIRT and engineering roles, to use XDR.

The course reviews XDR intricacies, from fundamental components to advanced strategies and techniques, including skills needed to configure security integrations, develop workflows, manage indicators, and optimize dashboards for enhanced security operations.

## This course is designed to enable you to:

- Investigate cases, analyze key assets and artifacts, and interpret the causality chain.
- Query and analyze logs using XQL to extract meaningful insights.
- Utilize advanced tools and resources for comprehensive case analysis.
- The course reviews XDR intricacies, from fundamental components to advanced strategies and techniques, including skills needed to navigate case management, platform automation, and orchestrate cybersecurity excellence.

## Požadované vstupní znalosti

Participants should have a foundational understanding of cybersecurity principles and experience with analyzing incidents and using security tools for investigation.

GOPAS Praha  
Kodaňská 1441/46  
101 00 Praha 10  
Tel.: +420 234 064 900-3  
[info@gopas.cz](mailto:info@gopas.cz)

GOPAS Brno  
Nové sady 996/25  
602 00 Brno  
Tel.: +420 542 422 111  
[info@gopas.cz](mailto:info@gopas.cz)

GOPAS Bratislava  
Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 248 282 701-2  
[info@gopas.sk](mailto:info@gopas.sk)



Copyright © 2020 GOPAS, a.s.,  
All rights reserved

# CORTEX XDR : Investigation and Analysis

## Poznámka: This course replaces Cortex XDR: Investigation and Response

### Osnova kurzu

- Introduction to Cortex XDR
- Endpoints
- XQL
- Alerting and Detection
- Vulnerability & Forensics
- Platform Automation
- Case Management
- Dashboards & Reports

### Palo Alto Networks Education

The technical curriculum developed and authorized by Palo Alto Networks and delivered by Palo Alto Networks Authorized Training Partners helps provide the knowledge and expertise that prepare you to protect our digital way of life. Our trusted certifications validate your knowledge of the Palo Alto Networks product portfolio and your ability to help prevent successful cyberattacks, safely enable applications, and automate effective responses to security events.

**GOPAS Praha**  
Kodaňská 1441/46  
101 00 Praha 10  
Tel.: +420 234 064 900-3  
[info@gopas.cz](mailto:info@gopas.cz)

**GOPAS Brno**  
Nové sady 996/25  
602 00 Brno  
Tel.: +420 542 422 111  
[info@gopas.cz](mailto:info@gopas.cz)

**GOPAS Bratislava**  
Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 248 282 701-2  
[info@gopas.sk](mailto:info@gopas.sk)



Copyright © 2020 GOPAS, a.s.,  
All rights reserved