CORTEX XDR : Investigation and Analysis

Course code: 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.

Affiliate	Duration	Course price	ITB
Praha	2	24 900 Kč	0
Brno	2	24 900 Kč	0
Bratislava	2	1 030 €	0

The prices are without VAT.

Course terms

Date	Duration	Course price	Type	Course language	Location
11.05.2026	2	24 900 Kč	Online	CZ/SK	TD SYNNEX Czech - Online
11.05.2026	2	24 900 Kč	Presence	CZ/SK	TD SYNNEX Czech

The prices are without VAT.

Who is the course for

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.

What we teach you

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.

Required skills

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

Note: This course replaces Cortex XDR: Investigation and Response

Course outline
- Introduction to Cortex XDR

GOPAS®

- Endpoints
- XQL
- Alerting and Detection
- Vulnerability &Forensics
- Platform Automation
- Case Management
- Dashboards &Reports

GOPAS®

16.03.2026 00:00:14