Cortex XSIAM: Investigation and Analysis

Course code: PAN-CXIA

XSIAM is the industry's most comprehensive security incident and asset management platform, offering extensive coverage for securing and managing infrastructure, workloads, and applications across multiple environments.Throughout this course, you will explore the key features of Cortex XSIAM.

Who is the course for

SOC/CERT/CSIRT/XSIAM analysts and managers, MSSPs and service delivery partners/system integrators, internal and external professional-services consultants and sales engineers, incident responders and threat hunters.

What we teach you

- The course is designed to enable cybersecurity professionals, particularly those in SOC/CERT/CSIRT and Security Analysts roles, to use XSIAM.
- The course reviews XSIAM intricacies, from fundamental components to advanced strategies and techniques, including skills needed to navigate case management, automation, and orchestrate cybersecurity excellence.

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.

Required skills

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

Related Certifications:

Palo Alto Networks Certified XSIAM Analyst

Course outline

- Introduction to Cortex XSIAM
- Endpoints
- XQL
- Alerting and Detection
- Threat Intel Management
- Automation
- Attack Surface Management
- Incident Handling
- Dashboards and Reports

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