Training: Palo Alto Networks

Cortex XSIAM: Investigation and Analysis

TRAINING GOALS:

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.

This course is designed to enable you to:

- Investigate incidents, 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 incident analysis.

Objectives

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 incident handling, automation, and orchestrate cybersecurity excellence.

Target Audience

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.

CONSPECT:

- Introduction to Cortex XSIAM
- Endpoints
- XQL

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

- Alerting and Detection
- Threat Intel Management
- Automation
- Attack Surface Management
- Incident Handling
- Dashboards and Reports

REQUIREMENTS:

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

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by Palo Alto Networks (course completion).

This course also helps you prepare for the Palo Alto Networks Certified XSIAM Analyst certification exam. Palo Alto Networks certification exams are offered at Pearson Vue test centers worldwide https://home.pearsonvue.com/paloaltonetworks

More information about the Palo Alto Networks exams and certification program: https://www.paloaltonetworks.com/services/education/certification

TRAINER:

Palo Alto Networks Certified Security Platform Instructor (PCSPI)

ADDITIONAL INFORMATION:

The technical curriculum developed by Palo Alto Networks and delivered by Palo Alto Networks Authorized Training Partners helps provide the knowledge and expertise you need 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 and safely enable applications.

Authorized Courseware

Each attendee will receive a student guide and lab exercise guide in the form of a secure PDF. Students will access these materials by creating an account with a third party platform, Kortext,

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

hosted by fulfilment supplier.

Training Credit

Palo Alto Networks Training Credits allow you a single point of purchase for training for use throughout the year. Training credits are redeemable by all employees within an organization for any Palo Alto Networks open enrollment, private on-site, or online course offered by our Authorized Training Partners (ATPs). Compendium CE accept the Training Credits issued by Palo Alto Networks. To sign-up for a course and pay using training credits, please contact with our sales team: szkolenia@compendium.pl

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310