Palo Alto Networks Cortex XSIAM: Investigation and Analysis

Palo Alto Networks Cortex XSIAM: Investigation and Analysis

XSIAM ist die branchenweit umfassendste Plattform für das Management von Sicherheitsvorfällen und Assets und bietet umfassende Funktionen für die Sicherung und Verwaltung von Infrastruktur, Workloads und Anwendungen in verschiedenen Umgebungen.

In diesem Training lernen Sie die wichtigsten Funktionen von Cortex XSIAM kennen. Der Kurs wurde entwickelt, um Cybersicherheitsexperten, insbesondere denen in SOC/CERT/CSIRT- und Security-Analysten-Rollen, die Nutzung von XSIAM zu ermöglichen. Das Training behandelt die Feinheiten von XSIAM, von den grundlegenden Komponenten bis hin zu fortgeschrittenen Strategien und Techniken, einschließlich der Fähigkeiten, die für die Bewältigung von Incidents, die Automatisierung und die Orchestrierung von Cybersicherheit erforderlich sind.

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

Sie haben Zugang zu Ihrem eigenen Labor für praktische Übungen. Das Labor besteht aus einer dedizierten Windows-VM, einer Next-Generation-Firewall und einer Broker-VM sowie Zugang zu einer gemeinsam genutzten Cortex XSIAM-Instanz. Das Labor ist während der Schulungswoche rund um die Uhr verfügbar, sodass Sie es auch nach dem Unterricht für zusätzliche Übungen nutzen können.

E-Book Sie erhalten englischsprachige Unterlagen von Palo Alto als E-Book.

Zielgruppe
SOC-/CERT-/CSIRT-/XSIAM-Analysten und -Manager, MSSPs und Service Delivery Partner/Systemintegratoren, interne und externe Berater für professionelle Dienstleistungen und Vertriebsingenieure, Incident Responder und Threat Hunter

Voraussetzungen
Die Teilnehmer sollten über grundlegende Kenntnisse der Prinzipien der Cybersicherheit sowie über Erfahrung in der Analyse von Vorfällen und der Verwendung von Sicherheitstools für Ermittlungen verfügen.

Kursziel
Dieses Training wird zur Vorbereitung auf die Zertifizierung Palo Alto Networks Certified XSIAM Analyst empfohlen.

- Untersuchen Sie Vorfälle, analysieren Sie wichtige Ressourcen und Artefakte und interpretieren Sie die Kausalkette.
- Fragen Sie Protokolle mit XQL ab und analysieren Sie sie, um aussagekräftige Erkenntnisse zu gewinnen.
- Nutzen Sie fortschrittliche Tools und Ressourcen für eine umfassende Vorfallanalyse.

Dieser Kurs im Web
Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/go/**PCXI**

Vormerkung
Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine
Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert
Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training	Preise zzgl. MwSt.
Termine in der Schweiz	**2 Tage**
Online Training	**2 Tage CHF 1.975,-**
Termin/Kursort	Kurssprache Englisch
13.11.-14.11.25 ONOnline	18.12.-19.12.25 ONOnline

Stand 24.09.2025

Palo Alto Networks

ExperTeach

Inhaltsverzeichnis

Palo Alto Networks Cortex XSIAM: Investigation and Analysis

ExperTeach AG
Kronenstrasse 11 · 8735 St. Gallenkappel · Telefon: +41 55 420 2591 · Fax: +41 55 420 2592 · info@experteach.ch · www.experteach.ch