

## Palo Alto Networks EDU-262 Cortex XDR: Investigation and Response for Cortex XDR

In diesem Kurs lernen Sie, wie Sie die Meldungen der Cortex XDR-Verwaltungskonsole verwenden, um Angriffe zu untersuchen. Es werden Kausalitätsketten, Detektoren in der Analytics Engine, Alarime im Vergleich zu Protokollen, Log Stitching und die Konzepte von Kausalität und Analytik erklärt.

Sie lernen, wie Sie Alarime mit Hilfe der Kausalitäts- und Zeitleistenansichten analysieren und wie Sie fortschrittliche Reaktionsmaßnahmen wie Abhilfeschläge, den EDL-Dienst und die Remote-Skriptausführung nutzen. Mehrere Module konzentrieren sich darauf, wie die gesammelten Daten genutzt werden können. Sie erstellen einfache Suchabfragen in einem Modul und XDR-Regeln in einem anderen. Der Kurs demonstriert die Verwendung spezieller Untersuchungsansichten zur Visualisierung artefaktbezogener Daten, wie z. B. IP- und Hash-Views. Darüber hinaus bietet er eine Einführung in die XDR Query Language (XQL). Der Kurs schließt mit den Fähigkeiten von Cortex XDR zur Sammlung externer Daten, einschließlich der Verwendung der Cortex XDR API zum Empfang externer Warnmeldungen.

### Kursinhalt

- Cortex XDR Incidents
- Causality and Analytics Concepts
- Causality Analysis of Alerts
- Advanced Response Actions
- Building Search Queries
- Building XDR Rules
- Investigation Views
- Introduction to XQL
- External Data Collection

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

### Zielgruppe

Cybersecurity-Analysten und -Ingenieure sowie Spezialisten für Security Operations.

### Voraussetzungen

Die Teilnehmer müssen den Kurs EDU-260 (Cortex XDR: Prevention and Deployment) besucht haben.

### Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: [www.experteach.de/go/P262](http://www.experteach.de/go/P262)

### 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.	
<b>Termine in Deutschland</b>	<b>2 Tage</b>	<b>€ 1.795,-</b>	
<b>Online Training</b>	<b>2 Tage</b>	<b>€ 1.795,-</b>	
<b>Termin/Kursort</b>	<b>Kurssprache Deutsch </b>		
06.06.-07.06.24	05.12.-06.12.24		
06.06.-07.06.24	05.12.-06.12.24		

Stand 17.12.2023



## Unser Trainingsangebot für Sie:



### Classroom Training

Das Live-Trainingserlebnis in unseren Training Centern oder bei Ihnen vor Ort.



### Online Training

Nehmen Sie online am Kurs teil – ohne Reise- und Hotelaufwände.



### Hybrid Training

Classroom & online in einem Kurs – Sie wählen, wie Sie teilnehmen möchten.



### Inhouse-Schulungen

Für Ihr Projekt erstellen wir genau passende Trainingskonzepte.



### Garantierte Kurstermine

Die ExperTeach Garantietermine geben Ihnen Sicherheit für Ihre Planung.

## Auszeichnungen für ExperTeach



ExperTeach Gesellschaft für Netzwerkkompetenz mbH

Waldstr. 94 · 63128 Dietzenbach · Telefon: +49 6074 4868-0 · Fax: +49 6074 4868-109 · info@exper teach.de · www.exper teach.de