BQ105G

IBM QRadar SIEM Foundations

IBM Security QRadar ermöglicht einen umfassenden Einblick in Netzwerk-, Endpunkt-, Benutzer- und Anwendungsaktivitäten. Es ermöglicht die Sammlung, Normalisierung, Korrelation und sichere Speicherung von Ereignissen, Flüssen, Assets und Schwachstellen. Verdächtige Angriffe und Richtlinienverstöße werden als Verstöße markiert. In diesem Kurs lernen Sie die Architektur der Lösung kennen, wie Sie sich auf der Benutzeroberfläche bewegen und wie Sie Angriffe untersuchen. Sie suchen und analysieren die Informationen, aus denen QRadar auf eine verdächtige Aktivität geschlossen hat. Praktische Übungen festigen die erlernten Fähigkeiten.

Kursinhalt

- Describe how QRadar collects data to detect suspicious activities
- Describe the QRadar architecture and data flows
- Navigate the user interface
- Define log sources, protocols, and event details
- Discover how QRadar collects and analyzes network flow information
- Describe the QRadar Custom Rule Engine
- Utilize the Use Case Manager app
- Discover and manage asset information
- Learn about a variety of QRadar apps, content extensions, and the App Framework
- Analyze offenses by using the QRadar UI and the Analyst Workflow app
- Search, filter, group, and analyze security data
- Use AQL for advanced searches
- Use QRadar to create customized reports
- Explore aggregated data management
- Define sophisticated reporting using Pulse Dashboards
- Discover QRadar administrative tasks

In diesem Kurs erhält jeder Teilnehmer die englischsprachigen Original-Unterlagen von IBM.

Zielgruppe

Dieser Kurs richtet sich an Sicherheitsanalysten, technische Sicherheitsarchitekten, Offensivmanager, Netzwerkadministratoren und Systemadministratoren, die QRadar SIEM verwenden.

Voraussetzungen

Bevor Sie an diesem Kurs teilnehmen, sollten Sie sich vergewissern, dass Sie über die folgenden Kenntnisse verfügen:

- IT-Infrastruktur
- Grundlagen der IT-Sicherheit
- Linux
- Windows
- TCP/IP-Netzwerke
- Syslog

Kursziel

Nach Abschluss dieses Kurses sollten Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Beschreiben, wie QRadar Daten sammelt, um verdächtige Aktivitäten zu erkennen
- Beschreiben der QRadar-Architektur und der Datenflüsse
- Navigieren durch die Benutzeroberfläche
- Definieren von Protokollquellen, Protokollen und Ereignisdetails
- Entdecken, wie QRadar Netzwerkflussinformationen sammelt und analysiert
- Beschreiben der QRadar Custom Rule Engine
- Nutzen der Use Case Manager-App
- Erkennen und Verwalten von Asset-Informationen
- Kennenlernen einer Vielzahl von QRadar-Apps, Inhaltserweiterungen und des App Frameworks
- Analysieren von Verstößen mithilfe der QRadar-Benutzeroberfläche und der Analysten-Workflow-App
- Suchen, Filtern, Gruppieren und Analysieren von Sicherheitsdaten
- Verwenden von AQL für erweiterte Suchen
- Verwenden von QRadar, um benutzerdefinierte Berichte zu erstellen
- Erforschen der Verwaltung aggregierter Daten
- Definieren von anspruchsvollen Berichten mit Pulse Dashboards
- QRadar-Verwaltungsaufgaben entdecken

Dieser Kurs im Web

Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.at/go/**BQ3G**

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 Deutschland	**3 Tage**	**€ 2.595,-**
Online Training	**3 Tage**	**€ 2.595,-**

Termin/Kursort — Kurssprache Deutsch

07.07.-09.07.25	München	06.10.-08.10.25	Leinfelden
07.07.-09.07.25	ONOnline	06.10.-08.10.25	ONOnline
07.07.-09.07.25	ONOnline		

Termin/Kursort — Kurssprache Englisch

06.10.-08.10.25	ONOnline

Stand 25.04.2025

BQ105G

IBM

ExperTeach

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 Training & Consulting GmbH
Handelskai 94-96 · 1200 Wien · Telefon: +43 1 2350 383-0 · Fax: +43 1 2350 383-19 · info@experteach.at · www.experteach.at