IBM QRadar SIEM Foundations

Duración: 3 Días Código del Curso: BQ105G Método de Impartición: Curso Remoto (Virtual)

Temario:

IBM Security QRadar enables deep visibility into network, endpoint, user, and application activity. It provides collection, normalization, correlation, and secure storage of events, flows, assets, and vulnerabilities. Suspected attacks and policy breaches are highlighted as offenses. In this course, you learn about the solution architecture, how to navigate the user interface, and how to investigate offenses. You search and analyze the information from which QRadar concluded a suspicious activity. Hands-on exercises reinforce the skills learned.

Curso Remoto (Abierto)

Nuestra solución de formación remota o virtual, combina tecnologías de alta calidad y la experiencia de nuestros formadores, contenidos, ejercicios e interacción entre compañeros que estén atendiendo la formación, para garantizar una sesión formativa superior, independiente de la ubicación de los alumnos.

Dirigido a:

This course is designed for security analysts, security technical architects, offense managers, network administrators, and system administrators using QRadar SIEM.

Objetivos:

- After completing this course, you should be able to perform the following tasks:
- 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

Prerequisitos:

Before taking this course, make sure that you have the following skills:

- IT infrastructure
- IT security fundamentals
- Linux
- Windows
- TCP/IP networking
- Syslog

Contenido:

Topics

- Unit 0: IBM Security QRadar 7.5 - Fundamentals
- Unit 1: QRadar Architecture
- Unit 2: QRadar UI - Overview
- Unit 3: QRadar - Log Source
- Unit 4: QRadar flows and QRadar Network Insights
- Unit 5: QRadar Custom Rule Engine (CRE)
- Unit 6: QRadar Use Case Manager app
- Unit 7: QRadar - Assets
- Unit 8: QRadar extensions
- Unit 9: Working with Offenses
- Unit 10: QRadar - Search, filtering, and AQL
- Unit 11: QRadar - Reporting and Dashboards
- Unit 12: QRadar - Admin Console

Extensive lab exercises are provided to allow learners an insight into the routine work of an IT Security Analyst operating the QRadar SIEM platform. The exercises cover the following topics:

- Architecture exercises
- UI Overview exercises
- Log Sources exercises
- Flows and QRadar Network Insights exercises
- Custom Rule Engine (CRE) exercises
- Use Case Manager app exercises
- Assets exercises
- App Framework exercises
- Working with Offenses exercises.
- Search, filtering, and AQL exercises
- Reporting and Dashboards exercises
- QRadar Admin tasks exercises

The lab environment for this course uses the IBM QRadar SIEM 7.5 platform.

Más información:

Para más información o para reservar tu plaza llámanos al (34) 91 425 06 60

info.cursos@globalknowledge.es

www.globalknowledge.com/es-es/

Global Knowledge Network Spain, C/ Retama 7, 6ª planta, 28045 Madrid