Enterprise Computing Solutions - Education Services

OFERTA FORMATIVA

Detalles de contacto

Avda Europa 21, 28108 Alcobendas

Email: formacion.ecs.es@arrow.com
Phone: +34 91 761 21 51

IBM QRadar SIEM Foundations

CÓDIGO:	DURACIÓN:	Precio:
bq104g	24 Hours (3 días)	€1,700.00

Description

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.
In this 3-day instructor-led course, you learn how 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

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

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

The lab environment for this course uses the IBM QRadar SIEM 7.4 platform.

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

Público

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

Requisitos Previos

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

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

Programa

- Unit 0: IBM Security QRadar 7.4 ﷺ Fundamentals
- Unit 1: QRadar Architecture
- Unit 2: QRadar UI ﷺ Overview
- Unit 3: QRadar ﷺ 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 ﷺ Assets
- Unit 8: QRadar extensions
- Unit 9: Working with Offenses
- Unit 10: QRadar ﷺ Search, filtering, and AQL
- Unit 11: QRadar ﷺ Reporting and Dashboards
- Unit 12: QRadar ﷺ Admin Console

Fechas Programadas

A petición. Gracias por contactarnos.

Información Adicional

Esta formación también está disponible en modalidad presencial. Por favor contáctenos para más información.