Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Vous pouvez nous joindre ici

.

Email: training.ecs.fr@arrow.com
Phone: 01 49 97 50 00

IBM QRadar SIEM Foundations

CODE:	DURÉE:	PRIX H.T.:
BQ104G	24 Hours (3 Jours)	€2,350.00

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 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 7.4 platform.

Objectifs

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

Audience

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

Prérequis

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

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

Programme

- Unit 0: IBM Security QRadar 7.4 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

Test et Certification

This is an IBM-issued and IBM-recognized badge that attests that its recipients have demonstrated their knowledge of various QRadar deployments' architecture and key concepts such as user management, domains and tenants, assets, network hierarchy, flows, events, rules, offenses, reference data, data obfuscation, and reporting.
In order to attempt and pass this test, students must have participated in either the ARROW ECS official training for IBM Security QRadar SIEM Foundations (BQ104G), or the self-paced virtual classroom for IBM Security QRadar SIEM Foundations (BQ104XG).
Note: The two hours time estimate on the front page of this course refers to the time it can take to complete the quiz.

Dates de session

Date	Lieu	Time Zone	Langue	Type	Garanti	PRIX H.T.
10 Jun 2024	Virtual Classroom	CEDT	English	Instructor Led Online		€2,350.00
16 Sep 2024	Virtual Classroom	CEDT	English	Instructor Led Online		€2,350.00
04 Nov 2024	Virtual Classroom	CET	English	Instructor Led Online		€2,350.00
09 Dec 2024	Virtual Classroom	CET	English	Instructor Led Online		€2,350.00

Informations Complémentaires

Cette formation est également disponible sous forme de formation sur site. Veuillez nous contacter pour en savoir plus.