IBM Security QRadar SIEM Foundations

Information

Length:	2.0 Days
__Ref:	BQ102G-X
Delivery method:	ClassroomInstructor Led OnlineSelf-paced Virtual Training
Price:	EUR

Overview

QRadar SIEM provides deep visibility into network, 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 to navigate the user interface and how to investigate offenses. You search and analyze the information from which QRadar SIEM concluded a suspicious activity. Hands-on exercises reinforce the skills learned.

Public

This basic course is suitable for security analysts, security technical architects, offense managers, network administrators, and system administrators.

Prerequisits

You must have:

- Basic TCP/IP networking skills
- System administration knowledge
- Basic information security skills

Objective

- Describe the purpose and capabilities of the QRadar SIEM licensed program
- Describe how QRadar SIEM collects data and performs vulnerability assessment
- Learn how to navigate and customize the dashboard tab
- Learn how to investigate the information contained in an offense and respond to an offense
- Learn how to find, filter, and group events in order to gain critical insights about the offense
- Learn how to create and edit a search that monitors the events of suspicious hosts
- Learn how asset profiles are created and updated, and how to use them as part of an offense investigation
- Learn how to investigate the flows that contribute to an offense, create and tune false positives, and

investigate superflows
- Learn how to find custom rules in the QRadar SIEM console, assign actions and responses to the rule, and how to configure rules
- Learn how to use charts and apply advanced filters to examine specific activities in your environment

Topics

- Unit 1: Introduction to IBM Security QRadar SIEM
- Unit 2: How QRadar SIEM collects security data
- Unit 3: Using the QRadar SIEM Dashboard
- Unit 4: Investigating an offense that is triggered by events
- Unit 5: Investigating the events of an offense
- Unit 6: Using asset profiles to investigate offenses
- Unit 7: Investigating an offense that is triggered by flows
- Unit 8: Using rules and building blocks
- Unit 9: Creating QRadar SIEM reports
- Unit 10: Performing advanced filtering