IBM Security QRadar SIEM 7.2 Administration and Configuration

Information

Length:	3.0 Days
__Ref:	BQ121G-X
Delivery method:	ClassroomInstructor Led Online
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, topologies, and vulnerabilities. Suspected attacks and policy breaches are highlighted as offenses. In this course, you learn how to configure and administer QRadar SIEM, create Universal DSMs and Log Source Extensions, and create event, flow and anomaly rules. Using the skills taught in this course, you can maintain QRadar SIEM, work with log sources, analyze the offenses created by rules and if necessary fine-tune them. Hands-on exercises reinforce the skills learned.

Public

This course is for:

- Security analysts
- Security technical architects
- Offense managers
- Network administrators
- QRadar SIEM administrators
- Professional services

Prerequisits

You should have the following skills:

- IT infrastructure
- IT security fundamentals
- Linux
- Windows
- TCP/IP networking
- Log files and events
- QRadar SIEM user interface

- Successfully completed IBM Security QRadar SIEM Foundations

Objective

- Use tools on the Admin tab to manage administrative functions
- Build a network hierarchy
- Manage assets, reference sets, and the index
- Configure user accounts and authentication
- Use backups, recovery, and retention buckets to manage data
- Manage log and flow data sources
- Create customize log sources
- Use and create rules
- Identify and tune false positives

Topics

- Unit 1: Using administrative tools
- Unit 2: Creating the network hierarchy
- Unit 3: Updated administration tools
- Unit 4: Managing users
- Unit 5: Managing data
- Unit 6: Collecting log and flow records
- Unit 7: Collecting Windows log records
- Unit 8: Managing custom log sources
- Unit 9: Using rules
- Unit 10: Creating rules
- Unit 11: Managing false positives
- Unit 12: Using Refernce Maps in rules