IBM Security QRadar SIEM Administration

Information

Length:	2.0 Days
__Ref:	BQ150G-X
Delivery method:	ClassroomInstructor Led Online
Price:	EUR

Overview

IBM Security QRadar SIEM enables you to minimize the time gap between when suspicious activity occurs and when you detect it. There are a variety of administrative tools you can use to manage a QRadar SIEM deployment. This course covers system configuration, data source configuration, and remote networks and services configuration.

Public

This course is designed for QRadar SIEM administrators and professional services personnel managing QRadar SIEM deployments.

Prerequisits

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

- Basic knowledge of the purpose and use of a security intelligence platform
- Familiarity with the Linux command line interface and PuTTY
- Familiarity with custom rules
- Familiarity with the Ariel database and its purpose in QRadar SIEM
- Students should attend BQ102G, IBM Security QRadar Foundations or be able to navigate and use the QRadar SIEM Console

Objective

Learning objectives

- Install and manage automatic updates to QRadar SIEM assets
- Configure QRadar backup and restore policies
- Leverage QRadar administration tools to aggregate, review, and interpret metrics
- Use network hierarchy objects to manage QRadar SIEM objects and groups
- Manage QRadar hosts and licenses and deploy assets
- Monitor the health of assets in a QRadar deployment

- Configure system settings and asset profiles
- Configure reasons that QRadar administrators use to close offenses
- Create and manage reference sets
- Create the credentials used to perform authenticated scans
- Manage, route, and store event and flow data
- Use domains in QRadar SIEM to act as a filter for events, flows, scanners, assets, rules, offenses, and retention policies
- Configure user accounts including user profiles, authentication, and authorizations
- Manage custom properties for assets, events, and flows
- Manage QRadar log sources
- Manage QRadar flow sources
- Integrate Vulnerability Assessment Scanner results in QRadar SIEM
- Manage groups that monitor Internet networks and services

Topics

Unit 1: Auto Update
Unit 2: Backup and Recovery
Unit 3: Index and Aggregated Data Management
Unit 4: Network Hierarchy
Unit 5: System Management
Unit 6: License Management
Unit 7: Deployment Actions
Unit 8: High Availability management
Unit 9: System Health and Master Console
Unit 10: System Settings and Asset Profiler Configuration
Unit 11: Custom Offense Close Reasons
Unit 12: Store and Forward
Unit 13: Reference Set Management
Unit 14: Centralized Credentials
Unit 15: Forwarding Destinations
Unit 16: Routing Rules
Unit 17: Domain Management
Unit 18: Users, User Roles, and Security Profiles
Unit 19: Authentication
Unit 20: Authorized Services
Unit 21: Backup and Recovery
Unit 22: Custom Asset Properties
Unit 23: Log Sources
Unit 24: Log Soruce Groups
Unit 25: Log Source Extensions

Unit 26: Log Source Parsing Ordering
Unit 27: Custom Properties
Unit 28: Event and Flow Retention
Unit 29: Flow Sources
Unit 30: Flow Sources Aliases
Unit 31: VA Scanners
Unit 32: Remote Networks and Services