IBM QRadar SIEM Foundations (BQ103G)

Course ID #: 0370-103-BQ103G-W
Hours: 21

Course Content

Course Description:

IBM QRadar SIEM provides deep visibility into network, user, and application activity. It provides collection, normalization, correlation, and secure storage of events, flows, asset profiles, and vulnerabilities. QRadar SIEM classifies suspected attacks and policy violations as offenses.

Course Objectives:

After completing this course, you should be able to:

- Describe how QRadar SIEM collects data to detect suspicious activities
- Describe the QRadar SIEM component architecture and data flows
- Navigate the user interface
- Investigate suspected attacks and policy breaches
- Search, filter, group, and analyze security data
- Investigate the vulnerabilities and services of assets
- Use network hierarchies
- Locate custom rules and inspect actions and responses of rules
- Analyze offenses created by QRadar SIEM
- Use index management
- Navigate and customize the QRadar SIEM dashboard
- Use QRadar SIEM to create customized reports
- Use charts and filters
- Use AQL for advanced searches
- Analyze a real world scenario

Target Audience:

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

Prerequisites:

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

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

IBM QRadar SIEM Foundations (BQ103G)

Course ID #: 0370-103-BQ103G-W
Hours: 21

Topics:

- **Introduction to IBM QRadar**
- **IBM QRadar SIEM component architecture and data flows**
- **Using the QRadar SIEM User Interface**
- **Investigating an Offense Triggered by Events**
- **Investigating the Events of an Offense**
- **Using Asset Profiles to Investigate Offenses**
- **Investigating an Offense Triggered by Flows**
- **Using Rules**
- **Using the Network Hierarchy**
- **Index and Aggregated Data Management**
- **Using the QRadar SIEM Dashboard**
- **Creating Reports**
- **Using Filters**
- **Using the Ariel Query Language (AQL) for Advanced Searches**
- **Analyzing a Real-World Large-Scale Attack**
- **A real-world scenario introduction to IBM QRadar SIEM**
- **IBM QRadar architecture**