Course Code: BQ650GW

Course Title: IBM Security QRadar v7.4.3 Deployment Professional

Description:

A QRadar Deployment specialist plans and installs QRadar SIEM and performs the initial configuration that allows an organization to begin using it. In this course, students will learn the various activities and responsibilities of a QRadar Deployment Professional. The course outline follows the same structure as the IBM Certified Deployment Professional - Security QRadar SIEM V7.4.3 (C1000-140) exam and helps the student prepare for the exam.

Objectives:

- Review the business needs of your organization and determine the QRadar apps and content value for your organization.
- Report the value of your QRadar deployment and what it provides to your organization.
- Describe the functional context and network flow analytics, extensible architecture, deployment models, components, resilience, licensing, and the flow of an event through the QRadar data pipeline.
- Explain installing QRadar, adding a license, adding certificates, configuring backup and restore, configuring the network hierarchy, and configuring user settings.
- Define and configure events and flows, log and flow sources, custom properties, and the flow data pipeline.
- Use and configure the QRadar Assistant app, configure and troubleshoot X-Force feeds, filter QRadar rules in the Use Case Manager app, view and expand your rules coverage with the MITRE ATT&CK interface, and import new assets.
- Update the QRadar network hierarchy, find Remote to Remote events, monitor the QRadar system health, understand QRadar system notifications, monitor system load and storage, Investigate QRadar logs, troubleshoot apps, and identify unknown events.
- Describe QRadar rules and offenses, offense indexing, use the rule response limiter when creating rules, perform server discovery, explain the role that building blocks play in searches, and use QRadar reference data in rules.
- Explain how to migrate data between consoles, prepare QRadar for upgrades, manage and migrate apps, back up data from one QRadar Console and restore it on another.
- Explain how multi-tenancy works in QRadar, explain overlapping IP addresses in multitenant environments, segment data between QRadar tenants, manage apps in multi-tenant environments, configure network hierarchy in multitenant environments, and configure Security Profiles in multitenant environments.

Prerequisites:

- TCP/IP networking
- Unix command line knowledge
- Basic security technologies (including PKI concepts
- Regex
- Enterprise logging
- Network monitoring using flows

Duration:

3.2 Hrs

Topics:

1. Deployment Objectives and Use Cases2. Architecture and Sizing3. Installation and Configuration4. Event and Flow Integration5. Environment and XFE Integration6. System Performance and Troubleshooting7. Initial Offense Tuning8. Migration and Upgrades9. Multi-Tenancy Considerations

Audience:

Users, Administrators, and Analysts interested in learning how to deploy a QRadar SIEM environment