IBM Certified Deployment Professional — QRadar SIEM V7.5

OEM: IBM • Duration: 5 Days (40 hrs) • Code: C1000-163

COURSE MODULES & TOPICS

Section 1: Deployment Objectives and Use Cases (10%)

- Review business needs
- Determine useful QRadar Apps and Extension Packs
- Define QRadar value reporting

Section 2: Architecture and Sizing (16%)

- Determine scope and size requirements for deployment
- Plan for placement of appliances
- Determine requirements for data retention
- Determine QRadar deployment components
- Identify the need for HA and DR
- Determine licensing requirements
- Windows collection architecture

Section 3: Installation and Configuration (16%)

- Install QRadar SIEM
- Apply and update licensing
- Apply QRadar system Certificates
- Backup, recovery, and data retention
- Conduct initial configuration
- Configure authentication and access control

Section 4: Event and Flow Integration (13%)

- Define log sources
- Define and configure flow sources
- Define custom properties
- Install content extensions based on requirements
- Identify event parsing requirements

Section 5: Environment and X-Force Integration (6%)

- Configure Assistant App and manage apps
- Establish X-Force intelligence data integration levels
- Configure Use Case Manager
- Populate and use the Asset database

Section 6: System Performance and Troubleshooting (13%)

- Monitor system performance
- Check QRadar audit and self-monitoring events
- Check and restart Apps as necessary
- Identify event drops and events going to storage

Section 7: Initial Offense Tuning (10%)

- Tune noisy rules and CRE events
- Identify expensive rules and properties
- Utilize Server Discovery
- Update building blocks
- Manage and use reference data

Section 8: Migration and Upgrades (10%)

- Migrate Data
- Review upgrade prerequisites
- Determine content migration strategy
- Review App Framework considerations (UBI)
- Restoring a backup
- Performing QRadar SIEM hardware migration

Section 9: Multi-Tenancy Considerations (6%)

- Define domains and tenants requirements
- Configure items which involve Multi-tenancy