IBM Certified Associate Administrator - IBM QRadar SIEM Training

Course Content

1. Implementing

- Plan and design QRadar deployment.
- Implement and install QRadar.
- Add Managed Hosts.

2. Migrating and upgrading

- Plan QRadar upgrade and migration.
- Review documentation and release notes.
- Perform QRadar updates, patches and upgrades.
- Perform migration (e.g., backup and restore, import and export content).

3. Configuring and administering tasks

- Configure event flow sources and custom properties.
- Maintain configuration and data backups.
- Create and administer users, user roles, and security profiles.
- Manage the license per allocation.
- Create, review and modify rules, building blocks and reference sets.
- Configure and manage retention policies (i.e., data and assets).
- Create and manage saved searches, index, global views, dashboards and reports.
- Deploy and manage applications and content packages.
- Configure global system notifications.
- Configure and apply network hierarchy.
- Configure and manage domain and tenants.
- Use the asset database.
- Schedule and run a VA scan.

4. Monitoring

- Monitor QRadar Notifications and error messages.
- Review and interpret system monitoring dashboards.
- Verify QRadar processes and services.
- Monitor QRadar performance.
- Use apps and tools for monitoring (e.g., QDI, assistant app, incident overview, DrQ).
- Check system maintenance and health of appliances.
- Monitor offenses and detect anomalies.

5. Troubleshooting

- Demonstrate knowledge of key commands to interpret QRadar services and processes.
- Explain error messages and notifications.
- Interpret the basic logs (e.g., qradar.error, qradar.log).
- Use embedded troubleshooting tools and scripts.