Administrator Security QRadar SIEM V7.5

Test Exam C1000-156

Certification overview, objectives, exam preparation and registration

Certification Overview

Prerequisite Knowledge:

Recommended Skills

- Basic security technologies, SIEM concepts, TCP/IP networking, IT security concepts, and IT skills
- Offense and log analysis
- Network monitoring using flows
- QRadar Network Insights, QRadar Incident Forensics

Key Areas of Competency

- QRadar troubleshooting
- Searching and reporting
- Rule and building block & reference data understanding
- Basic QRadar tuning and network hierarchy
- QRadar deployment and component architecture
- Understanding QRadar Event and Flow pipelines
- QRadar user management and data access control
- Basic concepts of multi-domain
- QRadar instances

Requirements

- This certification requires one exam.

Exam C1000-156: IBM Security QRadar SIEM V7.5 Administration

Exam Objectives

Test Details:

Number of Questions	Number of Questions to Pass	Time Allowed
62	38	90 Min

Course Content

IBM Certified Administrator - Security QRadar SIEM V7.5

System Configuration

- Understand license management
- Understand the managed hosts
- Understand AIO & distributed architecture
- Manage configuration and data backups
- Manage network hierarchy
- Use and manage reference data
- Manage automatic update
- Demonstrate the use of the asset database
- Install and configure apps

S e c t i o n – **1**

Topic covers

20 %

Of the Exam

Performance Optimization

- Construct identity exclusions
- Deal with resource restrictions
- Configuring, tuning and understanding rules
- Index management
- Search management
- Manage routing rules and event forwarding

S e c t i o n – **2**

Topic covers

13 %

Of the Exam

Data Source Configuration

- Manage flow sources
- Manage log sources
- Export event and flow data
- Manage custom event and flow properties
- Understand the custom log source

S e c t i o n – **3**

Topic covers

14 %

Of the Exam

Accuracy Tuning

- Understand and implement Anomaly Detection Engine rules
- Manage and use building blocks
- Manage content packs
- Distinguish native information sources
- Configure integrations

S e c t i o n – **4**

Topic covers

10 %

Of the Exam

User Management

- Manage users
- Create and update security profiles
- Create and update user roles
- Manage user authentication and authorization

S e c t i o n – **5**

Topic covers

06 %

Of the Exam

Reporting, Searching & Offense Management

- Manage reports
- Utilize different search types
- Manage offenses
- Sharing content among users

Section – **6**

Topic covers

13 %

Of the Exam

Troubleshooting

- Review and respond to system notifications
- Troubleshoot common documented issues
- Configure, manage and troubleshoot applications
- Perform health checks
- Basic GUI REST-API usage

Section – 7

Topic covers

16 %

Of the Exam


IBM