EDUSUM

#1 Online Certification Guide

IBM C1000-140

IBM QRadar SIEM V7.4.3 Deployment Certification Questions & Answers

Exam Summary – Syllabus –Questions

C1000-140

IBM Certified Deployment Professional - Security QRadar SIEM V7.4.3

61 Questions Exam – 65% Cut Score – Duration of 90 minutes

Table of Contents:

Know Your C1000-140 Certification Well: 2

IBM C1000-140 QRadar SIEM V7.4.3 Deployment Certification Details: 2

C1000-140 Syllabus: 3

IBM C1000-140 Sample Questions: 4

Study Guide to Crack IBM QRadar SIEM V7.4.3 Deployment C1000-140 Exam: 7

Know Your C1000-140 Certification Well:

The C1000-140 is best suitable for candidates who want to gain knowledge in the IBM Security. Before you start your C1000-140 preparation you may struggle to get all the crucial QRadar SIEM V7.4.3 Deployment materials like C1000-140 syllabus, sample questions, study guide.

But don't worry the C1000-140 PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the C1000-140 syllabus?
- How many questions are there in the C1000-140 exam?
- Which Practice test would help me to pass the C1000-140 exam at the first attempt?

Passing the C1000-140 exam makes you IBM Certified Deployment Professional - Security QRadar SIEM V7.4.3. Having the QRadar SIEM V7.4.3 Deployment certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

IBM C1000-140 QRadar SIEM V7.4.3 Deployment Certification Details:

Exam Name	IBM Certified Deployment Professional - Security QRadar SIEM V7.4.3
Exam Code	C1000-140
Exam Price	$200 (USD)
Duration	90 mins
Number of Questions	61
Passing Score	65%
Books / Training	**Roadmap: QRadar SIEM Administrator**
Schedule Exam	**Pearson VUE**
Sample Questions	**IBM QRadar SIEM V7.4.3 Deployment Sample Questions**
Practice Exam	**IBM C1000-140 Certification Practice Exam**

C1000-140 Syllabus:

Topic	Details	Weights
Deployment Objectives and Use Cases	- Review business needs - Determine QRadar apps and content value - Define QRadar value reporting	5%
Architecture and Sizing	- 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	18%
Installation and Configuration	- Install QRadar SIEM - Apply and update licensing - Apply QRadar system Certificates - Backup, recovery, and data retention - Conduct initial configuration - Configure authentication and access control	16%
Event and Flow Integration	- Define log sources - Define and configure flow sources - Define custom properties - Install content extensions based on requirements - Identify event parsing requirements	12%
Environment and XFE Integration	- Configure Assistant App and use it to manage the apps - Establish X-Force intelligence data integration levels - Configure Use Case Manager - Populate and Use Asset database	8%
System Performance and Troubleshooting	- Look for R2R events - Monitor system performance - Check SIM audit events and logs - Check and restart Apps as necessary - Identify event drops, events going to storage and unknown events	13%
Initial Offense Tuning	- Tune noisy offenses and CRE events - Identify expensive rules and properties - Utilize Server Discovery	8%

Topic	Details	Weights
	- Update building blocks - Manage and use reference data	
Migration and Upgrades	- Migrate Data - Upgrade prerequisites - Determine content migration strategy - Review App Framework considerations (UBI) - Restoring a backup - Performing system migration	13%
Multi-Tenancy Considerations	- Define domains and tenants requirements - Configure items which involve Multi-tenancy	7%

IBM C1000-140 Sample Questions:

Question: 1

There are frequent network interruptions from a particular network zone called “Underground” to the network where QRadar components are installed.

Some important applications, though not time critical, are running in the “Underground” network zone. The log data from these applications needs to be sent to QRadar Event Processor for compliance.

How can QRadar receive the logs from the applications in the "Underground" network zone?

a) Using an App Host
b) Installing an Event Processor secondary node in the “Underground” network
c) Using Data Node installed in the “Underground” network
d) Using Disconnected Log Collector configured with TLS

Answer: d

Question: 2

An organization wants QRadar to have rules, dashboards, and reports to detect and report on cryptocurrency mining activity. What can be installed in QRadar to meet this requirement?

a) Content extension from IBM Security App Exchange
b) Latest MITRE content from IBM Security Fix Central
c) Latest autoupdates from IBM Security Fix Central
d) User Behavior Analytics from IBM Security App Exchange

Answer: a

Question: 3

What is the default data retention period for a retention bucket?

a) 7 days
b) 14 days
c) 1 month
d) 1 year

Answer: c

Question: 4

On a Console migration, after the config backup restoration, what is required to ensure that the required configuration is migrated to the new appliance?

a) Restore Data Backup
b) Deploy Full Configuration
c) Recreate users and roles
d) Restore application data

Answer: b

Question: 5

How are extensions added to a QRadar deployment?

a) Import extensions by CSV file
b) Use the Extensions Management tool
c) Use Import Extensions under Admin tab
d) Download extensions from IBM X-Force App Exchange

Answer: b

Question: 6

In the Backup Recovery Configuration section, what is the default retention period?

a) 1 day
b) 4 days
c) 7 days
d) 15 days

Answer: c

Question: 7

A QRadar deployment professional is asked to plan a hardware migration for an Event Processor in HA. Two new appliances are ready to be used, and they use the same IP addresses. Which approach can be used to migrate the systems?

a) Use the QRadar config backup and restore process to transfer all configurations.
b) Use rsync to transfer the contents of the /store/postgres partition to the new system.
c) Remove HA on the EPs, migrate to the new primary, then add the new secondary back in.
d) Ensure both systems are built as appliance type 500 and add them into the deployment as replacements.

Answer: c

Question: 8

Where do you select a custom property in an event?

a) Event payload
b) Event protocol
c) Log source test output
d) Use Case Manager app

Answer: a

Question: 9

Where are audit logs located?

a) /var/audit
b) /var/log/audit
c) /opt/audit/logs
d) /opt/var/log/audit

Answer: b

Question: 10

Which is a sign that the QRadar Network Hierarchy requires tuning?

a) MITRE tactics are blue.
b) Dashboards are not updating.
c) The Use Case Manager does not load.
d) There are many Remote-to-Remote events.

Answer: d

Study Guide to Crack IBM QRadar SIEM V7.4.3 Deployment C1000-140 Exam:

- Getting details of the C1000-140 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the C1000-140 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the IBM provided training for C1000-140 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the C1000-140 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on C1000-140 practice tests is must. Continuous practice will make you an expert in all syllabus areas.