EDUSUM

#1 Online Certification Guide

IBM C1000-175

IBM Foundations of Security QRadar SIEM Certification Questions & Answers

Exam Summary – Syllabus –Questions

C1000-175

IBM Certified Associate - Security QRadar SIEM V7.5

62 Questions Exam – 66% Cut Score – Duration of 90 minutes

Table of Contents:

Know Your C1000-175 Certification Well: 2

IBM C1000-175 Foundations of Security QRadar SIEM Certification Details: 2

C1000-175 Syllabus: 3

IBM C1000-175 Sample Questions: 4

Study Guide to Crack IBM Foundations of Security QRadar SIEM C1000-175 Exam: 7

Know Your C1000-175 Certification Well:

The C1000-175 is best suitable for candidates who want to gain knowledge in the IBM Security - Not Applicable. Before you start your C1000-175 preparation you may struggle to get all the crucial Foundations of Security QRadar SIEM materials like C1000-175 syllabus, sample questions, study guide.

But don't worry the C1000-175 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 C1000-175 syllabus?
- How many questions are there in the C1000-175 exam?
- Which Practice test would help me to pass the C1000-175 exam at the first attempt?

Passing the C1000-175 exam makes you IBM Certified Associate - Security QRadar SIEM V7.5. Having the Foundations of Security QRadar SIEM 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 C1000-175 Foundations of Security QRadar SIEM Certification Details:

Exam Name	IBM Certified Associate - Security QRadar SIEM V7.5
Exam Code	C1000-175
Exam Price	$200 (USD)
Duration	90 mins
Number of Questions	62
Passing Score	66%
Books / Training	**IBM QRadar SIEM Foundations (BQ104G)** **IBM QRadar SIEM Foundations - Self-Paced Virtual Course (SPVC) (BQ104XG)** **IBM QRadar SIEM Foundation**
Schedule Exam	**Pearson VUE**
Sample Questions	**IBM Foundations of Security QRadar SIEM Sample Questions**
Practice Exam	**IBM C1000-175 Certification Practice Exam**

C1000-175 Syllabus:

Topic	Details	Weights
SIEM Concepts	- Log Management - Event Correlation and Analytics - Incident Monitoring and Security Alerts - Compliance Management and Reporting	10%
QRadar Architecture	- Understand the logical components of QRadar - Understand QRadar appliances - Understand how QRadar can be deployed in different environments	10%
User Interface	- Describe main portions of the QRadar SIEM GUI	5%
Extensions	- Illustrate the use of the IBM Security App Exchange - Understand the QRadar Assistant App - Describe the installed apps	5%
Flows	- Describe flows versus events - Manage flow sources - Explain the basic use case for QNI versus QIF - Understand that there are three inspection levels in QNI	6%
Rules and Building Blocks	- Create and configure rules - Understand the use of rule types - Understand rules tests - Understand rule responses - Create and manage building blocks - Describe Local versus Global correlation	10%
Working with Offenses	- Describe the basic offense lifecycle - Manage offenses	8%
Search, Filtering, and AQL	- Utilize different search types - Conduct search management - Use Filters	8%
Assets	- Explain how the asset database gets populated - Describe the value of the vulnerability information in the asset database - Demonstrate use of the asset database	5%
Reporting and Dashboards	- Generate, modify and interpret reports using QRadar templates	6%

Topic	Details	Weights
	- Interpret QRadar dashboards - Manage reports - Use the Report Wizard	
Events	- Describe the processes of data ingestion - Log source management - Event parsing - Custom properties - Describe the basic uses of the DSM editor	10%
Configuration and Tuning	- Understand network hierarchy - Explain the licensing model	6%
QRadar System Errors	- Monitor QRadar Notifications and error messages - Investigate common errors	6%
User and Role Management	- Understand user roles - Understand user authentication and authorization - Understand security profiles	5%

IBM C1000-175 Sample Questions:

Question: 1

Why is it important to define a parsing order for log sources that share a common Log Source Identifier in QRadar?

a) Ensure a specific order of parsing, prevent unnecessary parsing, and maintain system performance
b) Allow random parsing of log sources for performance optimization
c) Accommodate frequent changes to log source configuration
d) Prioritize low-level event sources for faster processing

Answer: a

Question: 2

Which QRadar application can delete, stop, or start other installed QRadar applications?

a) Pulse
b) QRadar Assistant
c) Use Case Manager
d) Threat Intelligence

Answer: b

Question: 3

From which IBM site can Content Packs including Custom Properties be downloaded?

a) IBM Support
b) IBM API Hub
c) IBM Fix Central
d) IBM App Exchange

Answer: d

Question: 4

A customer wants to implement QRadar Network Insights to detect suspicious traffic content using YARA rules. What is the minimum inspection level?

a) Basic
b) Advanced
c) Enriched
d) Advanced, but without SSL/TLS certificate inspection enabled

Answer: c

Question: 5

You need to use Ariel Query Language to select the default columns from events. Which is the correct query?

a) SELECT % FROM events
b) SELECT * FROM events
c) SELECT ALL FROM events
d) SELECT defaultcolumns from events

Answer: b

Question: 6

What happens to a rule when it is deleted from a group?

a) The rule remains in disabled state.
b) The rule is flushed from the system.
c) The rule remains available on the Rules page.
d) The rule is no longer available on the Rules page.

Answer: c

Question: 7

Who can edit the account of an administrative role user?

a) The user can edit their own administrative account
b) Only a user with Delegated Administration functions
c) Any user can edit the account of an administrative user
d) Another administrative user must make any account changes

Answer: d

Question: 8

Which two properties are the magnitude rating of an offense based on?

a) Severity
b) Priority
c) Credibility
d) Accuracy
e) Offense correlation

Answer: a, c

Question: 9

Which QRadar application supports building dashboards from custom AQL (Ariel Query Language) queries and QRadar offenses?

a) Pulse
b) Use Case Manager
c) Threat Intelligence
d) User Behavioral Analytics

Answer: a

Question: 10

QRadar SIEM ingests event data from a wide range of sources, including on-premises and cloud environments. Which SIEM functionality is described?

a) Log Management
b) Event Correlation and Analytics
c) Incident Monitoring and Security Alerts
d) Compliance Management and Reporting

Answer: a

Study Guide to Crack IBM Foundations of Security QRadar SIEM C1000-175 Exam:

- Getting details of the C1000-175 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 C1000-175 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 C1000-175 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 C1000-175 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 C1000-175 practice tests is must. Continuous practice will make you an expert in all syllabus areas.