EDUSUM

#1 Online Certification Guide

IBM C1000-162

IBM Security QRadar SIEM Analysis Certification Questions & Answers

Exam Summary – Syllabus –Questions

C1000-162

IBM Certified Analyst - Security QRadar SIEM V7.5

64 Questions Exam – 64% Cut Score – Duration of 90 minutes

Table of Contents:

Know Your C1000-162 Certification Well:

The C1000-162 is best suitable for candidates who want to gain knowledge in the IBM IBM Security - Not Applicable. Before you start your C1000-162 preparation you may struggle to get all the crucial Security QRadar SIEM Analysis materials like C1000-162 syllabus, sample questions, study guide.

But don't worry the C1000-162 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 C1000-162 syllabus?
- How many questions are there in the C1000-162 exam?
- Which Practice test would help me to pass the C1000-162 exam at the first attempt?

Passing the C1000-162 exam makes you IBM Certified Analyst - Security QRadar SIEM V7.5. Having the Security QRadar SIEM Analysis 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 C1000-162 Security QRadar SIEM Analysis Certification Details:

Exam Name	IBM Certified Analyst - Security QRadar SIEM V7.5
Exam Code	C1000-162
Exam Price	$200 (USD)
Duration	90 mins
Number of Questions	64
Passing Score	64%
Books / Training	**IBM Certified Analyst: Security QRadar SIEM V7.5 - Exam C1000-162 Preparation Guide** **QRadar SIEM Analyst learning plan**
Schedule Exam	**Pearson VUE**
Sample Questions	**IBM Security QRadar SIEM Analysis Sample Questions**
Practice Exam	**IBM C1000-162 Certification Practice Exam**

C1000-162 Syllabus:

Topic	Details	Weights
Offense Analysis	- QRadar uses rules to monitor the events and flows in your network to detect security threats. When the events and flows meet the test criteria that is defined in the rules, an offense is created to show that a security attack or policy breach is suspected. But knowing that an offense occurred is only the first step. Offense Analysis is all about initially identifying how it happened, where it happened, and who are the players involved in the offense. • Triage initial offense • Analyze fully matched and partially matched rules • Analyze an offense and associated IP addresses • Recognize MITRE threat groups and actors • Perform offense management • Describe the use of the magnitude within an offense • Identify Stored and Unknown events and their source • Outline simple offense naming mechanisms • Create customized searches	23%
Rules and Building Block Design	- QRadar rules are applied to all incoming events, flows, or offenses to search for or detect anomalies. If all the conditions of a test are met, the rule generates a response. A building block is a collection of tests that don't result in a response or an action. A building block groups commonly used tests to build complex logic so that it can be reused in	18%

Topic	Details	Weights
	rules. As an Analyst you need to fully understand how rules and building blocks are designed and used, and although you are not responsible for implementing new or tuning existing rules and building blocks, you can and should make recommendations on updating QRadar components that may improve rules and building block design based on your daily exposure to them. • Interpret rules that test for regular expressions • Create and manage reference sets and populate them with data • Identify the need for QRadar Content Packs • Analyze rules that use Event and Flow data • Analyze Building Blocks Host definition, category definition, Port definition • Review and understand the network hierarchy • Review and recommend updates to building blocks and rules • Describe the different types of rules, including behavioral, anomaly and threshold rules	
Threat Hunting	- After the initial Offense Analysis and based on technical skills in understanding QRadar rules and building block design, it is time to focus on the Analyst's main task of Threat Hunting. Starting with the results presented in an offense, the Analyst will investigate the evidence inside an offense, such as event and flow details, triggered rules, payloads, and more. Utilizing filters and advanced	24%

Topic	Details	Weights
	searches the Analyst will be able to distinguish real threats from false positives. • Investigate Event and Flow parameters • Perform AQL query • Search & filter logs • Configure a search to utilize time series • Analyze potential IoCs • Break down triggered rules to identify the reason for the offense • Distinguish potential threats from probable false positives • Add a reference set based filter in log analysis • Investigate the payload for additional details on the offense • Recommend adding new custom properties based on payload data • Perform "right-click Investigations" on offense data	
Dashboard Management	- Use the QRadar Dashboard tab to focus on specific areas of your network security. The workspace supports multiple dashboards on which you can display your views of network security, activity, or data that is collected. You can use the QRadar Pulse app for an enhanced dashboard experience. • Use the default QRadar dashboard to create, view, and maintain a dashboard based on common searches • Use Pulse to create, view, and maintain a dashboard based on	14%

Topic	Details	Weights
	common searches	
Searching and Reporting	- Effectively utilizing QRadar's search capability represents one of the foundational skills for an Analyst. These capabilities include filtering event, flow, and asset related data as well as creating quick and advanced searches, including the Ariel Query Language. Filters and searches can be used in various parts of the QRadar UI. - The Analyst can create, edit, distribute, and manage reports, including flexible options to satisfy your organization's various regulatory standards, such as PCI compliance, and offense and threat related reports. • Explain the different uses and benefits for each Ariel search type • Explain the different uses of each search type • Perform an advanced search • Filter search results • Build threat reports • Perform a quick search • View the most commonly triggered rules • Report events correlated in the offense • Export Search results in CSV or XML • Create reports and advanced reports out of offenses • Share reports with users • Search using indexed and non-indexed properties • Create and generate scheduled and manual reports	21%

IBM C1000-162 Sample Questions:

Question: 1

What are events called when they are classified in the proper log source?

a) Stored events
b) Parsed events
c) Payload events
d) Unknown events

Answer: b

Question: 2

Which report can you run to find rules or building blocks that use performance-intensive tests that are not at the end of the test list?

a) CRE report
b) R2R report
c) Active Rules report
d) Tuning Finding report

Answer: d

Question: 3

What are the key elements used by the Report wizard in QRadar to create a report?

a) Font, color, and size
b) Content, style, and design
c) Layout, container, and content
d) Schedule, generate, and export

Answer: c

Question: 4

Based on which factors will the magistrate prioritize the offenses and assign the magnitude values?

a) Relevance, severity, and risk
b) Severity, relevance, and credibility
c) Risk, severity, and number of events
d) Credibility, priority, and number of events

Answer: b

Question: 5

Offense chaining is possible based on which parameter?

a) Rule type
b) Rule response
c) Offense index field
d) Rule response limiter

Answer: c

Question: 6

How can a QRadar analyst identify the gap between the rules deployed on QRadar and rules needed to cover the security use cases?

a) Use the QRadar Assistant app
b) Use the Offense tab to add new rules
c) Use the IBM X-Force Exchange portal
d) Use the content extension filters on Use Case Manager app

Answer: d

Question: 7

When a QRadar QFlow Collector is combined with QRadar and flow processors, what is the highest OSI layer visible in Network Activity?

a) Layer 7
b) Layer 5
c) Layer 4
d) Layer 1

Answer: a

Question: 8

In QRadar, where is a list of offenses displaying associated source IP addresses?

a) Offense Summary > By Source IP
b) Offense Summary > New Search > Advanced Search
c) Log Activity > Offense Source Summary > Offenses
d) Log Activity > Add Filter > Source IP > offense_assigned

Answer: a

Question: 9

Which two (2) of these categories can be used for Ariel Query Language?

a) Assets
b) Widget
c) Network
d) Keyword
e) Database

Answer: d, e

Question: 10

An analyst is investigating rules that are deployed in the QRadar deployment. Where does the analyst determine which rules are most active in generating offenses?

a) In the Offenses tab, on the All Offenses menu, checking the Flows column
b) In the Offenses tab, on the My Offenses menu, checking the Events column
c) In the Offenses tab, on the Rules menu, checking the Offense Count column
d) In the Offenses tab, on the Rules menu, checking the Events/Flow Count column

Answer: c

Study Guide to Crack IBM Security QRadar SIEM Analysis C1000-162 Exam:

- Getting details of the C1000-162 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 C1000-162 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 C1000-162 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 C1000-162 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 C1000-162 practice tests is must. Continuous practice will make you an expert in all syllabus areas.