ExamsNest

Your Ultimate Exam Preparation Hub

Vendor: IBM

Code: C1000-162

Exam: IBM Certified Analyst - Security QRadar SIEM V7.5

https://www.examsnest.com/exam/c1000-162/

QUESTIONS & ANSWERS

DEMO VERSION

Version: 4.0

Question: 1

Offense chaining is based on which field that is specified in the rule?

A. Rule action field
B. Offense response field
C. Rule response field
D. Offense index field

Answer: D

Explanation:

Offense chaining in IBM Security QRadar SIEM V7.5 is based on the offense index field specified in the rule. This means that if a rule is configured to use a specific field, such as the source IP address, as the offense index field, there will only be one offense for that specific source IP address while the offense is active. This mechanism is crucial for tracking and managing offenses efficiently within the system.

Question: 2

What QRadar application can help you ensure that IBM GRadar is optimally configured to detect threats accurately throughout the attack chain?

A. Rules Reviewer
B. Log Source Manager
C. QRadar Deployment Intelligence
D. Use Case Manager

Answer: D

Explanation:

The IBM QRadar Use Case Manager application assists in tuning QRadar to ensure it is optimally configured for accurate threat detection throughout the attack chain. This application provides guided tips to help administrators adjust configurations, making QRadar more effective in identifying and mitigating security threats. The QRadar Use Case Manager plays a significant role in maintaining the effectiveness of the QRadar deployment.

Question: 3

How can an analyst search for all events that include the keyword "access"?

A. Go to the Network Activity tab and run a quick search with the "access" keyword.
B. Go to the Log Activity tab and run a quick search with the "access" keyword.
C. Go to the Offenses tab and run a quick search with the "access" keyword.
D. Go to the Log Activity tab and run this AOL: select * from events where eventname like 'access'.

Answer: B

Explanation:

In IBM Security QRadar SIEM V7.5, to search for all events containing a specific keyword such as "access", an analyst should navigate to the "Log Activity" tab. This section of the QRadar interface is dedicated to viewing and analyzing log data collected from various sources. By running a quick search with the "access" keyword in the Log Activity tab, the analyst can filter out events that contain this term in any part of the log data. This functionality is crucial for identifying specific activities or incidents within the vast amounts of log data QRadar processes, allowing analysts to quickly hone in on relevant information for further investigation or action.

Question: 4

What feature in QRadar uses existing asset profile data so administrators can define unknown server types and assign them to a server definition in building blocks and in the network hierarchy?

A. Server roles
B. Active servers
C. Server discovery
D. Server profiles

Answer: C

Explanation:

In IBM Security QRadar SIEM V7.5, the feature that utilizes existing asset profile data to define unknown server types and assign them to server definitions in building blocks and in the network hierarchy is known as "Server Discovery." This feature grants permission to discover servers, thereby enabling administrators to identify and classify various server types within their network infrastructure, enhancing the overall asset management and security posture.

Question: 5

QRadar analysts can download different types of content extensions from the IBM X-Force Exchange portal. Which two (2) types of content extensions are supported by QRadar?

A. Custom Functions
B. Events
C. Flows

D. FGroup
E. Offenses

Answer: A, E

Explanation:

QRadar supports different types of content extensions that can be downloaded from the IBM X-Force Exchange portal. Among the supported content extensions are "Custom Functions" and "Offenses." These extensions allow for enhanced functionality and customization within QRadar, providing users with the ability to tailor the system to specific security needs and requirements.

ExamsNest

Your Ultimate Exam Preparation Hub

Thank You for trying the PDF Demo

Vendor: IBM

Code: C1000-162

Exam: IBM Certified Analyst - Security QRadar SIEM V7.5

https://www.examsnest.com/exam/c1000-162/

Use Coupon “**SAVE15**” for extra 15% discount on the purchase of Practice Test Software. Test your Exam preparation with actual exam questions.

Start Your Preparation