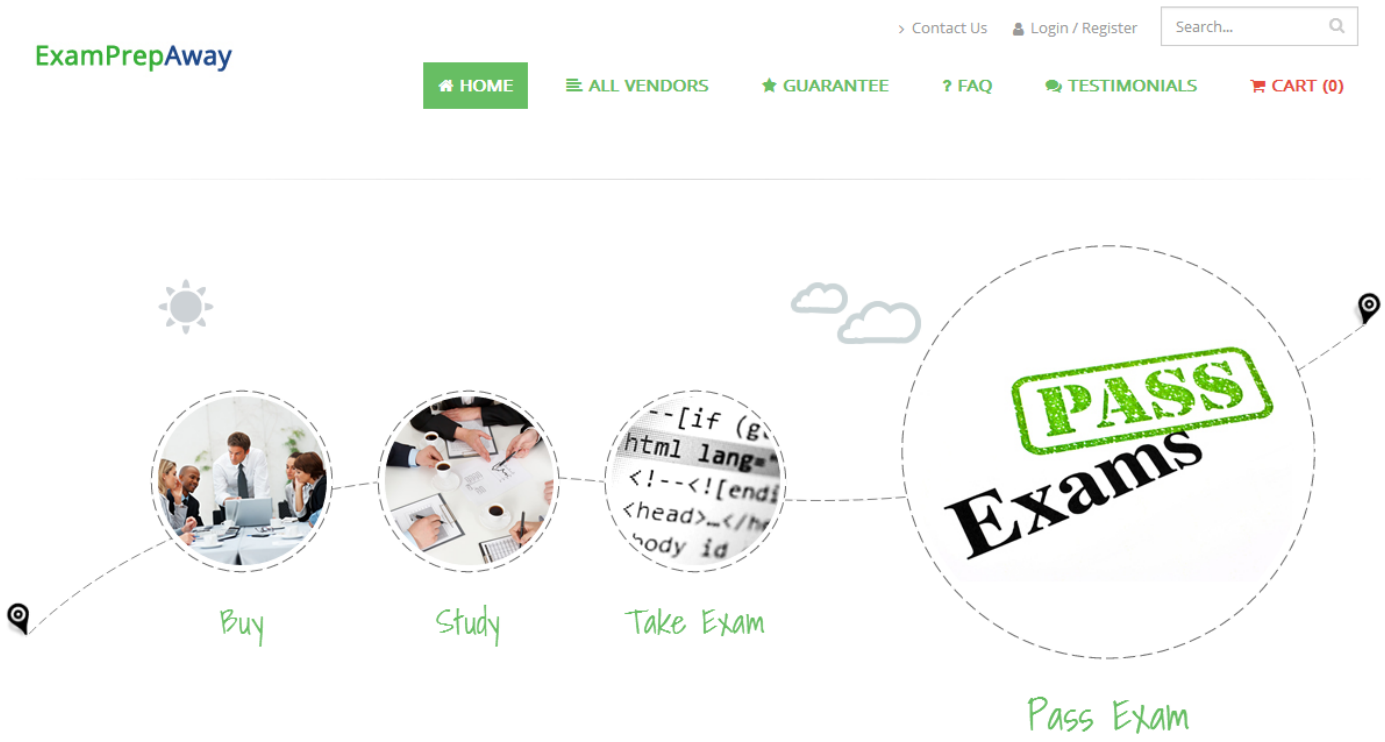
ExamPrepAway



Try **Online Engine** before you buy

We're not the only ones **happy** about ExamPrepAway Practice Material ...

56295+ customers in 100+ countries use ExamPrepAway Test Engine. Meet our customers.

GetCustom JET ORANGE iCompany Paradoxx iMessenger VOREED

http://www.examprepaway.com/

Latest Exam Guide & Learning Materials

Exam : **C1000-156**

Title : IBM Security QRadar SIEM V7.5 Administration

Vendor : IBM

Version : DEMO

NO.1 How many vulnerability processors can you have in your deployment?
A. 5
B. 3
C. 10
D. 1
Answer: D
Explanation:
In QRadar SIEM V7.5, the number of vulnerability processors is limited to 1.
These vulnerability processors are responsible for handling and processing vulnerability data within the system.
Having multiple vulnerability processors is not supported in this version of QRadar.
Reference:
IBM QRadar SIEM V7.5 Administration documentation.

NO.2 A user reports that some data points are missing from a generated report. The logs show these notifications, which are determined to be the root cause of the problem:
The accumulator was unable to aggregate all events/flows for this interval.
In what timeframe does this system need to complete data aggregation for it to be deemed successful?
A. 30 seconds
B. 5 seconds
C. 120 seconds
D. 60 seconds
Answer: D
Explanation:
In IBM QRadar SIEM V7.5, the accumulator process must complete data aggregation within a specific timeframe to be deemed successful:
Timeframe: 60 seconds
Aggregation Process: The accumulator aggregates events and flows for reporting and analysis. If it cannot complete this task within 60 seconds, it is considered unsuccessful.
Impact: Failure to aggregate within the specified timeframe can result in missing data points in reports and dashboards, affecting the accuracy and completeness of the information presented.
Reference
The QRadar SIEM administration guides detail the accumulator process and the importance of completing data aggregation within 60 seconds to ensure accurate reporting.

NO.3 Domain assignments lake precedence over the settings of which other elements from a security profile?
A. Security profiles, Networks, and Log Sources tabs
B. Security profiles. Networks, and Domains
C. Permission Precedence, and Log Sources tabs
D. Permission Precedence. Networks, and Log Sources tabs
Answer: D
Explanation:

In IBM QRadar SIEM, domain assignments take precedence over the settings of other elements from a security profile, specifically Permission Precedence, Networks, and Log Sources tabs. This hierarchical precedence ensures that the domain settings are enforced across different security configurations. The domain settings effectively override other configurations to maintain consistency and security across the environment. This structure helps in managing access and permissions more effectively by ensuring that the domain-level policies are the primary controlling factor.
Reference
QRadar SIEM V7.5 Administration Guide - Chapter on Domain Management and Security Profiles

NO.4 Which event advanced search query will check an IP address against the Spam X-Force category with a confidence greater than 3?
A. select * from events where XFORCE_IP_CONFIDENCE('Spam', sourceip>>3
B. select * from flows where XFORCE_IP_CONFIDENCE{'Spam', sourceip)<3
C. select * from flows where XF0RCE_iP_C0NFiDEKCE{*Malware',sourceip)-3
D. select * from events where XF0RCE_IP_C0NFIDENCE('Malware',sourceip)>3
Answer: D
Explanation:
To check an IP address against the Spam X-Force category with a confidence greater than 3 using an advanced search query in QRadar, the correct query format is:
Query Structure: select * from events where XF0RCE_IP_C0NFIDENCE('Malware',sourceip)>3
Components:
select * from events: This part of the query selects all events from the QRadar events database.
where XF0RCE_IP_C0NFIDENCE('Malware',sourceip)>3: This filter checks if the source IP address has a confidence level greater than 3 for being associated with malware according to the X-Force category.
This query is designed to filter out and display events where the source IP is identified with high confidence as being associated with malicious activity.
Reference
The syntax and usage of advanced search queries are detailed in the IBM QRadar SIEM search and analytics guides, providing specific examples for utilizing X-Force threat intelligence data.

NO.5 An administrator receives a file with all the vital assets in the company and wants to import this file into QRadar. How must this import file be formatted?
A. CSV file in the format: IP address. Name, Weight. Description
B. JSON file in the format: IP address. Name, Weight, Domain
C. XML file in the format: IP address. Name, Weight, Domain
D. XLS file in the format: IP address, Name. Weight, Description
Answer: A
Explanation:
When importing vital asset information into IBM QRadar SIEM V7.5, the import file must be formatted as a CSV file with the following structure:
Format: CSV (Comma-Separated Values)
Fields: The required fields are IP address, Name, Weight, and Description.
IP address: The IP address of the asset.
Name: The name of the asset.

Weight: A numerical value representing the importance or criticality of the asset.
Description: A brief description of the asset.
This format ensures that QRadar can correctly parse and import the asset information, integrating it into its asset database for further analysis and correlation.
Reference
IBM QRadar SIEM documentation provides guidelines on the required CSV format for importing asset information, detailing the necessary fields and their order.

NO.6 Which user role is defined by default in QRadar?
A. Event and Logs
B. QRadar Users
C. WinCollect
D. QRadar Managers
Answer: B
Explanation:
The default user role defined in QRadar is "QRadar Users". Here's a detailed explanation:
User Roles in QRadar: QRadar has a role-based access control system to manage user permissions and access levels. This ensures that users can only access and perform actions within their assigned roles.
Default Role - QRadar Users: The "QRadar Users" role is the default role assigned to new users. This role typically includes basic permissions needed to access and use QRadar features without administrative privileges.
Permissions: Users with the "QRadar Users" role can view and analyze security data, but they might have limited access to configuration settings and administrative functions.
Assigning default roles helps streamline user management and ensures that new users have the necessary access to perform their tasks.
Reference
IBM Security QRadar SIEM and IBM Security QRadar EDR integration.pdf