

IBM

Exam C2150-196

IBM Security QRadar SIEM V7.1 Implementation

Version: 9.0

[Total Questions: 121]

Question No : 1

What is the result of modifying a saved search?

- A. The original search criteria is not changed.
- B. The user will be prompted to save the new search criteria as a new saved search.
- C. The original search criteria is automatically saved and updated with the new criteria.
- D. The user will be prompted to update the search criteria to that of the modified criteria.

Answer: A

Question No : 2

To overwrite an IBM Security QRadar SIEM V7.1 system, what must be typed in when prompted during the re-imaging process?

- A. OK
- B. FLATTEN
- C. REFRESH
- D. REINSTALL

Answer: B

Question No : 3

Where does IBM Security QRadar SIEM V7.1 get the severity of an event?

- A. from the QIDmap
- B. from the event payload
- C. from the Tomcat server
- D. from the user's definition

Answer: A

Question No : 4

IBM Security QRadar SIEM V7.1 can be forced to run an instant backup by selecting which

option?

- A. Backup Now
- B. On Demand Backup
- C. Launch On Demand Backup
- D. Configure On Demand Backup

Answer: B

Question No : 5

An IBM Security QRadar SIEM V7.1 (QRadar) ALE agent should be installed on which system to collect Windows logs?

- A. the QRadar Console
- B. a QRadar Event Processor
- C. any Windows 2000 or newer server
- D. any Linux server with SMB installed

Answer: C

Question No : 6

Which statement best describes the supported external storage options in IBM Security QRadar SIEM V7.1(QRadar)?

- A. While QRadar supports NES for external storage, NES is recommended for backups, not for storing active data
- B. QRadar data is located in the /store file system. An off board storage solution can be used to migrate the entire /store file system to an external system for faster performance.
- C. The /store/ariel directory is the most commonly off boarded file system. Subsequently, collected event logs and flow records data can be relocated to external storage using protocols such as SMB.
- D. Any subdirectory in the /store file system can be used as a mount point for external storage device. By creating multiple volumes and mounting /store/ariel/logs and /store/ariel/qflow, storage capabilities can be extended past the 64TB file system limit currently supported by QRadar

Answer: A

Question No : 7

By default how often are events forwarded from an event collector to an event processor?

- A. every hour
- B. continuously
- C. every 2 hours
- D. it does not forward until the forwarding schedule is set

Answer: B

Question No : 8

What is required to configure users for successful external authentication?

- A. A configured External Authentication type
- B. Users with no account on the IBM Security QRadar SIEM V7.1 (QRadar) appliance
- C. Users with existing accounts on QRadar and a configured External Authentication type
- D. Select which users require external authentication and select the correct authentication type

Answer: C

Question No : 9

What are the main functions of the Report wizard within IBM Security QRadar SIEM V7.1?

- A. to enable branding of reports with a customer's logo or local identification information
- B. to specify the schedule, layout, report content, output format, and distribution channels
- C. to create new report groups which are placed in the existing hierarchy of reporting groups
- D. to select from compliance, executive, log source, network management, and security reports

Answer: B

Question No : 10

Where is the optimal location for IBM Security QRadar QFlow appliances to monitor Internet traffic?

- A. in the datacenter
- B. at the workstation switches
- C. at the wireless access points
- D. at an ingress/egress point in the network

Answer: D

Question No : 11

How is the WinCollect agent enabled to communicate with the IBM Security QRadar SIEM V7.1 (QRadar) console?

- A. Configure the WinCollect agent to forward syslog events to the QRadar Event Collector.
- B. Supply credentials to connect to the WinCollect agent when creating the Windows log source.
- C. Apply the token created for the WinCollect agent during the WinCollect software installation on the target.
- D. WinCollect log sources collect using the QRadar console as host so the WinCollect agent directly accesses the console.

Answer: C

Question No : 12

In which section can event or flow hashing be enabled/disabled in IBM Security QRadar SIEM V7.1?

- A. Console
- B. Security
- C. System Settings
- D. Deployment Editor

Answer: C

Question No : 13

What action(s) can be taken from the Log and Network Activity tab?

- A. close an offense based on existing anomaly rules
- B. create and edit rules and building blocks, and add log sources and flow sources
- C. open offenses based on users in the organization performing unauthorized activity
- D. create and edit searches, filter on specific details, sort, and right-click and filter on specific details

Answer: D

Question No : 14

Which user account is used to log in when installing the activation key?

- A. root
- B. admin
- C. qradar
- D. default

Answer: A

Question No : 15

What are three types of rules that can be created using the Rule Wizard? (Choose three.)

- A. Flow Rule
- B. Event Rule
- C. Offense Rule
- D. Anomaly Rule
- E. Threshold Rule
- F. Behavioral Rule

Answer: A,B,C

Question No : 16

What is an IBM Security QRadar network object?

- A. An asset definition
- B. Avulnerability scanner
- C. A collection of CIDR addresses
- D. A device sending logs to a QRadar

Answer: C

Question No : 17

Where is a LSX uploaded to IBM Security QRadar SIEM V7.1 to be used by a UDSM in the Admin Section?

- A. Log Source Extensions> Add
- B. Log Sources> Add > Extensions
- C. System Settings> Extensions > Add
- D. Systems and License Management> Add > Extensions

Answer: A

Question No : 18

When creating a behavioral rule in Automated Anomaly Analysis, which three components are weighted to determine the rule?

- A. autoregressive pattern, fit to underlying curve, and moving average
- B. seasonal or cyclical behavior, underlying trend, and random fluctuation
- C. previous period value, current observation, and average of residuals for future observations
- D. length of the seasonal component, date range for the trend, and time window during the day

Answer: B

Question No : 19

Which statement best describes the advantages of implementing NetFlow monitoring?

- A.** If antivirus software signatures fail to detect malware infection, NetFlow monitoring can help identify malware propagation by using its own signatures.
- B.** NetFlow provides the ability to detect suspicious log activity. Each log contains the number of bytes and packets transferred by both the SRC and DST allowing for volume-based reporting of network traffic.
- C.** NetFlow provides deep packet inspection, from layers three to seven of the OSI model, increasing visibility into applications; whereas, traditional flow monitoring only provides visibility at layers three and four.
- D.** NetFlow provides the ability to detect suspicious network activity, e.g. identify a potential botnet when Local to Remote traffic is matched to an IP address configured in a corresponding Remote Network group.

Answer: D

Question No : 20

How are user permissions applied using Log Source groups?

- A.** using user roles
- B.** applied to individual users
- C.** applied to network objects
- D.** applied to authorized services

Answer: A

Question No : 21

This command provides what information when run from an IBM Security QRadar QFlow 1202 appliance: `grep 'Sent.\ + flows' /var/log/qradar.log?`

- A.** total number of flows per minute sent to the Event Collector
- B.** total number of flows per minute sent to the Event Processor
- C.** total number of flows being sent since the system was restarted
- D.** total number of flows per second sent to the Flow Collector or console

Answer: A