IBM

Exam 000-196

IBM Security QRadar SIEM V7.1 Implementation

Version: 9.0

[Total Questions: 122]

Question No : 1

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 : 2

What is the purpose of the offense index?

A. When the offense is created it will create indexes for other offenses.
B. It helps find the offenses faster when searching for offenses by a specific properly.
C. When the offense is created it will be added to any existing similar open offense with the same indexed value. If none exist, a new offense will be opened.
D. When the offense is created the magistrate will search for offenses with the same indexed value and add the offense to a list of offenses for the indexed value.

Answer: C

Question No : 3

What does the % of Searches Using Property column in the Index Management Page indicate?

A. The percentage of saved searches created by users that reference the index.
B. The total percentage of saved searches in the system that reference the index.
C. The percentage of executed searches in the selected time range that used the index.
D. The percentage of executed searches in the selected time range that successfully used the index.

Answer: C

Question No : 4

A network hierarchy consists of these objects:

- DMZ 192.168.0.0/16
- Webservers 192.168.1.0/24
- MailServers 192.168.2.0/24
- UserNetwork 10.0.0.0/8

Which object(s) does 192.168.1.5 fall into?

A. DMZ
B. Webservers
C. UserNetwork
D. DMZ and Webservers

Answer: B

Question No : 5

How does the order of rule tests affect the ORE performance?

A. Itdoesnotaffecttheperformance.
B. All tests in a rule are evaluated individually. Tests that have counters affect the ORE performance and not the order of tests.
C. When analyzing the rules in pairs from top to bottom, the test at the top should always be the one most likely to fail because if it fails then ORE will not evaluate the following tests.
D. When analyzing the rules in pairs going from top to bottom, the test at the bottom should always be the test that is most likely to fail. This ensures that the rule evaluation is optimized.

Answer: C

Question No : 6

What are two ways an asset can be added to asset profiles? (Choose two.)

A. by flow data
B. by offense data

C. by anomaly rule
D. by search queries
E. by a vulnerability assessment or active network scan

Answer: A,E

Question No : 7

When scheduling a vulnerability scan which factor would be controlled by the Concurrency Mask?

A. The level of detail of the scan data based on the number of hosts involved in a particular run.
B. The load placed on each host that is being scanned during the time that the scan is underway.
C. The potential risk to the subnet being scanned due to the number and frequency of operations performed during the scan.
D. The load placed on the network, scanner, and/or IBM Security QRadar SIEM V7.1 due to the number of scans being performed during a scanner run.

Answer: D

Question No : 8

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 specifythe 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 : 9

If an IBM Security QRadar 1790 virtual appliance is added to a configuration, which

capability becomes available?

A. additional storage capacity for event data
Badditional Web interface for user browsing
B. additional storage capacity for OFlow data
C. internal storage capacity for event and QFlow data

Answer: C

Question No : 10

What is the last step to add a protocol based log source?

A. on the Admin tab click Deploy Changes
B. from Log Sources, select Log Source Type, and click Save
C. from Log Sources, select Log Source Identifier, and click Save
D. on the Admin tab, select Actions and click Deploy Pull Configuration

Answer: A

Question No : 11

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 : 12

How are values mapped in a LSXto parse data from a payload for a UDSM?

A. quotes (‘’)
B. backtics(‘)
C. regular expressions
D. comma separated (,)

Answer: C

Question No : 13

Which two flow sources provide layer 7 payload? (Choose two.)

A. JFlow
B. SFlow
C. NetFlow
D. Packeteer
E. Network Interface

Answer: B,E

Question No : 14

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 : 15

How is a new high level or low level event category added to IBM SecurityQRadar SIEM V7.1?

A. usetheAdmintab
B. usetheMapEventscreen
C. use the qidmap_cli.sh utility
D. a new event category cannot be added

Answer: D

Question No : 16

To overwrite an IBM SecurityQRadar 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 : 17

Which tuning template is available in IBM Security QRadar SIEM V7.1?

A. Custom
B. Common
C. Enterprise
D. Small Business Edition

Answer: C

Question No : 18

What is the default password to access the Integrated Management Module remote access controller for an IBM Security QRadar appliance?

A. calvin
B. default

C. passw0rd
D. PASSWORD

Answer: C

Question No : 19

Which family of analysis methods are commonly used with a time series?

A. deep packet intrusion detection
B. packet content protocol detection
C. network behavior anomaly detection
D. N-gram based behavior attack detection

Answer: C

Question No : 20

What must be provided when utilizing kickstart disks to install IBM Security QRadar SIEM V7.1 software on customer supplied hardware?

A. access using the serial port
B. support for a kickstart file is not supported
C. access to the file share where the kickstart file is located
D. a USB hard drive with enough room to support the kickstart file

Answer: B

Question No : 21

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.