IBM

Exam C2150-400

IBM Security Qradar SIEM Implementation v 7.2.1

Version: 8.0

[Total Questions: 175]

Question No : 1

A QRadar SIEM administrator wants to report when a local system connects to the internet on more than 100 destination ports over a 2 hour period. The administrator created an anomaly rule to capture this scenario.

Which type of rule should be selected in the rule creation wizard in this situation?

A. Flow Tule
B. Event Rule
C. Offense Rule
D. Common rule

Answer: B

Question No : 2

Which two types of charts are available on QRadar SIEM Report editor? (Choose two.)

A. Top Events
B. Top Source IPs
C. Top Login Failures
D. Top Destination IPs
E. Top Access Failures

Answer: B,D

Explanation:

References:

Question No : 3

How many IP addresses are required if the customer is planning to do high availability installation of one 31xx, two 16xx, and one 171xx appliances?

A. 8
B. 10
C. 12
D. 15

Answer: C

Question No : 4

Which two IP Addresses are required to setup NATed environment? (Choose two.)

A. Public IP Address
B. Private IP Address
C. Remote IP Address
D. Secondary IP Address
E. Destination IP Address

Answer: D,E

Question No : 5

What is used to define the server types in the server discovery screen?

A. Ports
B. Hostname
C. Mac address
D. IP addresses

Answer: A
Explanation:

The Server Discovery function is based on server-type building blocks. Ports are used to define the server type so that the server-type building block essentially functions as a port-based filter when searching the Asset Profile database.

Question No : 6

In which two ways can an administrator view all the events that are related to an offense from the Offense

Details screen? (Choose two.)

A. Top 5 Source IPs section
B. Click on Display > Sources
C. Click on Display > Destinations
D. Click on Event/Flow Count field's Events link
E. Click on Events button in Last 10 Events section

Answer: B,D

Question No : 7

There is a requirement at the customer site to double the default QFlow Maximum Content Capture size.

What would be the resulting packet size?

A. 64 bytes
B. 128 bytes
C. 256 bytes
D. 1024 bytes

Answer: B

Question No : 8

Which scanners report vulnerabilities on all ports? (Choose two.)

A. Axis
B. NMap
C. Qualys
D. tcpdump
E. nCircle IP360

Answer: B,C

Question No : 9

Which line color inside the deployment editor signals that encrypted communication has been selected for the managed hosts in a distributed environment?

A. Red
B. Blue
C. Black
D. Green

Answer: D

Question No : 10

What should the format of a CSV file be while importing assets on the QRadar console?

A. ip,portweight,description
B. ip,name,weightmagnitude
C. ip.name.weight.description
D. ip.name.severity.description

Answer: C

Explanation:

References:

Question No : 11

Which two options need to be set when adding host inside deployment editor? (Choose two.)

A. Netmask
B. IP Address
C. Root password
D. QRadar version
E. Gateway IP Address

Answer: B,E

Explanation:

References:

Question No : 12

Which Permission Precedence should be applied in the Security Profile so the users can see events from the "Windows Servers" log source group and from other log sources that match the destination or source network "Windows"?

A. No Restrictions
B. Log Sources Only
C. Networks OR Log Sources
D. Networks AND Log Sources

Answer: B

Question No : 13

What are the two expected Host Statuses after HA setup if the initial synchronization is complete? (Choose two.)

A. Primary: Active
B. Primary: Offline
C. Secondary: Failed
D. Secondary: Active
E. Secondary: Standby
F. Primary: Synchronizing

Answer: A,E

Question No : 14

Which two primary data sources send updates to the Asset profiler? (Choose two.)

A. Source IP
B. Source Port
C. Scan Result
D. Destination IP
E. Identity Events

Answer: A,B

Question No : 15

What does My Offenses display?

A. Offenses closed by the user
B. Offenses assigned to the user
C. Offenses protected by the user
D. Offenses triggered by rules created by the user

Answer: B

Explanation:

References:

Question No : 16

There are unknown log records from unsupported security device events in the Log activity tab. You are planning to write an LSX for an unsupported security device type based on UDSM.

What is the file format for exporting the unknown log records?

A. CSV
B. PDF
C. XLS
D. Text

Answer: D

Explanation:

References:

Question No : 17

What are the two support formats for exporting an Assets list from QRadar console? (Choose two.)

A. XML
B. RTF
C. PDF
D. CSV
E. HTML

Answer: A,E

Question No : 18

There are unknown log records from unsupported security device events in the Log activity tab. You are planning to write an LSX for an unsupported security device type based on UDSM. What is the file format and payload option for exporting the unknown log records?

A. XLS and full export
B. CSV and full export
C. XML and visible column
D. PDF and visible column

Answer: C

Question No : 19

Which function allows a custom event property to be removed from a selected event?

A. Anomaly
B. Map Event
C. False Positive
D. Extract Property

Answer: D

Question No : 20

In which three ways can you create Log Sources? (Choose three.)

A. Bulkload

B. Manually
C. Automatically
D. Scripting
E. Autoupdate
F. QRadar Enterprise template

Answer: B,D,E

Question No : 21

Which appliance is used to collect, store, and process event and flow data in case of hardware and network failure?

A. Replicated appliance
B. Secondary appliance
C. High availability appliance
D. High accessibility appliance

Answer: B

Question No : 22

A QRadar administrator is sizing a distributed deployment. The deployment has approximately 2 million flows per minute (FPM) and needs at least 7 terabytes of storage.

Which architecture is correct?

A. One 1724 flow processor
B. One 1705 flow processor
C. Two 1724 flow processors
D. Two 1705 flow processors

Answer: C

Question No : 23

What is the result when adding host definition building blocks to QRadar?

A. Creates Offenses
B. Reduces false positives

C. Makes searches run faster
D. Authorizes QRadar Services

Answer: B

Question No : 24

Which feature of QRadar is used for correlation purposes to help reduce false positives?

A. Flow information
B. Events information
C. Asset port information
D. Asset profile information

Answer: D

Explanation:

References:

Question No : 25

Which tab in the QRadar web console allows flows to be monitored and investigated?

A. Admin
B. Assets
C. Offenses
D. Network Activity

Answer: C

Explanation:

References:

Question No : 26