
**Vendor:**IBM

**Exam Code:**C2150-400

**Exam Name:**IBM Security Qradar SIEM Implementation v 7.2.1

**Version:**Demo

**QUESTION 1**

Which action prevents an offense from being removed from the database?

A. Hide

B. Show

C. Export

D. Protect

Correct Answer: D

---

**QUESTION 2**

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

Correct Answer: AB

---

**QUESTION 3**

What is the benefits of enabling indexes on event properties?

A. Decreased disk usage

B. Improved report accuracy

C. Improved search performance

D. Improved performance for regular expression patterns

Correct Answer: C

---

**QUESTION 4**

You notice the following message in the System Notification Widget on the Dashboard:

"Unable to automatically detect the associated log source for IP address."

When you hover over the message, you see this pop-up message:

Payload: Apr 11 01:00:01 127.0.0.1 [[type=com.eventgnosis.system.ThreadedEventProcessor] [parent=red6.color.inc:ecs0/EC/TrafficAnalysis1/TrafficAnalysis]] com.q1labs.semsources.filters.trafficanalysis.TrafficAnalysisFilter: [WARN] [NOT:0070014101] [172.16.77.25/- -] [-/- -]Unable to determine associated log source for IP address <192.168.2.90>. Unable to automatically detect the associated log source for IP address.

What is the issue?

A. There are events coming from IP 127.0.0.1 that cannot be autodiscovered and a Log Source Created

B. There are events coming from IP 192.168.2.90 that cannot be autodiscovered and a Log Source Created

C. There are events coming from IP 172.16.77.25 that cannot be autodiscovered and a Log Source Created

D. There are events coming from hostname red6.color.com that cannot be autodiscovered and a Log Source Created

Correct Answer: C

---

**QUESTION 5**

A customer is observing the Asset tab on the QRadar console and is getting duplicate assets in the console.

What is the reason for this asset duplication?

A. There are multiple heterogeneous assets present in environment.

B. There are multiple assets having same configuration details present in environment.

C. QRadar creates duplicate assets after a specific periodic interval without considering asset activity or inactivity.

D. Asset doesn\\'t appear in network for specific time period; when it came back QRadar detects it and

created a new asset for the same.

Correct Answer: C

---

**QUESTION 6**

From the given event payload format:

<13>Feb 03 08:07:06 10.201.71.249 03Feb2014 08:07:06 ctl 172.16.77.66 product: ; src: ; s_port: ; dst: ; service: ; proto: ; rule: ; orig: 172.16.77.100; has_accounting: 0;i/f_dir: inbound;i/f_name: daemon;sys_msgs: The eth5 interface is not protected by the anti-spoofing feature. Your network may be at risk;.

You are tasked with creating a Reference Set of the second IPs in the payload.

What needs to be done to complete this task?

A. Create a Custom Event Property to parse the second IP in the payload. From the Log Source config for the above event, choose "add to reference set" and select your reference set.

B. From the Reference Set Management screen, select "create reference set from Log Source Event". Pick the Log Source from the drop down. Pick the Event Name from the drop down.

C. From the Reference Set Management screen, select "create reference set from Log Source Event". Pick the Log Source from the drop down. Pick the Custom Event Property from the drop down.

D. Create a Custom Event Property to parse the second IP in the payload. Create a rule that tests for events from the Log Source that is collecting the above event, and for Rule Response add the Custom

Event Property to the Reference Set.

Correct Answer: A

---

**QUESTION 7**

What does the message in the System Notification Widget on the Dashboard "Disk Sentry: Disk Usage exceeded max threshold" tell you?

A. One of your Files Systems has exceeded 92%.

B. One of your Files Systems has exceeded 95%.

C. One of your Files Systems has exceeded 98%

D. One of your Files Systems has exceeded 90%.

Correct Answer: B

---

**QUESTION 8**

Which two options are available for Override parameter when an administrator views the Asset Profile Summary page? (Choose two.)

A. Forever

B. Until Next Scan

C. After Next Scan

D. Before Next Scan

E. After Specified Time

Correct Answer: AB

---

**QUESTION 9**

Which two file systems does QRadar support for offboard storage partitions? (Choose two.)

A. XFS

B. Btrfs

C. F2FS

D. EXT4

E. NTFS

Correct Answer: AD

---

**QUESTION 10**

A QRadar administrator needs to tune the system by enabling or disabling the appropriate rules in order to ensure that the QRadar console generates meaningful offenses for the environment. Which role permission is required for enabling and disabling the rule?

A. Offenses > Maintain CRE Rules

B. Offenses > Toggle Custom Rules

C. Offenses > Manage Custom Rules

D. Offenses > Maintain Custom Rules

Correct Answer: C

---

**QUESTION 11**

How is a full Event Data Restore on a 1605 appliance performed?

A. Selecting Full Recovery from the Backup/Restore screen in the Qradar UI

B. Selecting Full Data Recovery from the Backup/restore screen in the Qradar UI

C. From the CLI on the 1605 run the command \\'tar-zcvf /store/backup/backup.full.tgz /store/ariel\\'

D. From the CLI on the 1605 run the command \\'tar-zxvf /store/backup/backup.full.tgz /store/ariel\\'

Correct Answer: D

---

**QUESTION 12**

What does the message in the System Notification Widget in the Dashboard "Disk Sentry: Disk usage exceeded WARNING threshold" tell you?

A. One of your File Systems has exceeded 92%.

B. One of your File Systems has exceeded 95%.

C. One of your File Systems has exceeded 98%.

D. One of your File Systems has exceeded 90%.

Correct Answer: D