Vendor: IBM

Exam Code: C1000-163

Exam Name: IBM Security QRadar SIEM V7.5 Deployment

Version: DEMO

QUESTION 1
What are unknown events?

A. Both of the above
B. The event cannot be understood or parsed by Qradar
C. The event is collected and parsed, but cannot be mapped or categorized to a specific log source.
D. None of the above

Answer: C

QUESTION 2
What does it mean when a custom rule is partially matched in QRadar?

A. The rule is not fully enabled.
B. The AND NOT operator is set incorrectly in the first test.
C. All the tests in the rule were fully matched.
D. Not all the the tests in the rule were fully matched.

Answer: D

QUESTION 3
Which QRadar log file contains information about the rates of EPS?

A. /var/log/qradar.old
B. /var/qradar.log
C. /var/log/qradar.log
D. /var/log/eps.log

Answer: C

QUESTION 4
For a Source IP based offense, which field helps determine relative importance of the targets to the business?

A. Relative importance of Destination IP(s)
B. Duration of the offense
C. Total number of Events
D. Last Event/Flow

Answer: A

QUESTION 5
Which of the following is used to process flows in Qradar?

A. Event Collector
B. Flow Processor
C. Event Processor
D. Flow Collector

Answer: B

QUESTION 6
A deployment professional needs to migrate test rules developed in a test QRadar deployment to a production QRadar deployment.
Which approach can be used to migrate the rules?

A. Use the Use Case Manager to sync rules between the two deployments.
B. Use the Content Management Tool (CMT) to migrate the specific rules.
C. Use rsync to copy the /store/postgres/ directory that contains configurations.
D. Create a configuration backup, copy it to the production system, and import/restore the backup configuration.

Answer: B

QUESTION 7
An analyst reviewed an active offense that was many attackers, generating many events in the same category, targeting many systems. Upon further analysis, the analyst determined that the traffic from the attackers is legitimate and should not contribute to the offenses. Which tuning methodology guideline can the analyst use to tune out this traffic?

A. Edit the building blocks by using the Custom Rules Editor to tune the specific event.
B. Use the Log Source Management app to tune the category.
C. Edit building blocks by using the Custom Rules Editor to tune the category.
D. Use the False Positive Wizard to tune the specific event.

Answer: C

QUESTION 8
Where can a deployment professional find updates to DSMs?

A. The QRadar Admin console
B. Fix Central
C. The Log Source Management app
D. QRadar on Cloud website

Answer: D

QUESTION 9
What must a deployment professional select when defining a new flow source?

A. The destination port
B. The source IP address
C. The flow source type
D. The router brand

Answer: C

QUESTION 10
Several counts of the system notification message 38750088 - Performance degradation that were detected in the Event pipeline showed in a report.
In this case, what does the Event collection system do?

A. Bypasses EPS Licensing
B. Drops events from the pipeline
C. Routes data to storage
D. Queues events in RAM

Answer: C

QUESTION 11
What is correct order to stop Qradar Services?

A. hostcontext>tomcat>hostservice
B. hostcontext>hostservice>tomcat
C. tomcat>hostservice>hostcontext
D. The order doesn't matter

Answer: A

QUESTION 12
On a QRadar appliance, you might see a warning that you cannot connect to port 32006. Which command you will use for determining port information?

A. netstat
B. nc
C. nmap
D. psexec

Answer: A

QUESTION 13
Which regex statement extracts the DNS host from the cs-host value from the payload?

A. cs-host=www.?([^\|]*)\
B. cs-host=.?www.(.*.?)
C. cs-host=(?:www\.)?([^\|]*)\|(?:add|get|query|delete)\s+(?:www\.)?([^\s]+)
D. cs-host=(?:www\.)?([^\|]*)\|(?:http|ftp|tcp|https)\s+(?:www\.)?([^\s]+)

Answer: D

QUESTION 14
This partial Network diagram was provided to a QRadar deployment professional who is trying to determine if the deployment requires the definition of multiple domains.
How many domains are required, and why?

A. Three domains are required, one for each network: HR-A, HR-B, and FIN.

B. At least two domains are required to handle overlapping address spaces for the HR-B and FIN networks.
C. Three domains are required: one for each of the event processors, plus the default domain for the console.
D. No domains are required, but they might be useful to separate stored events and flows between the HR and Finance teams.

Answer: B

QUESTION 15
Which two options does a QRadar analyst need to configure in the False Positive window of the QRadar Console to mark an event or flow as False Positive?

A. Event or flow property and username
B. Asset and traffic direction
C. Event or flow property and traffic direction
D. Event or flow property and port number

Answer: C

QUESTION 16
A QRadar deployment professional is asked to migrate the configuration of a system from Log Manager to QRadar SIEM.
How should the custom rules, saved searches, and reports be migrated?

A. Use the QRadar config backup and restore process to transfer all configurations.
B. Use the content management tool (CMT) to transfer the security configuration.
C. The only option is to use the GUI to manually recreate any required content.
D. Use rsync to transfer the contents of the /store partition to the new system.

Answer: D

QUESTION 17
Which two statements are prerequisites for an to upgrade of QRadar? (Choose two.)

A. Verify that scan runs and reports are complete.
B. Verify that all changes are deployed on the appliances.
C. Ensure an admin account is logged on the UI.
D. Clean up all the Offenses before any version upgrade.
E. Ensure that the ISO file is copied to all the appliances.

Answer: AC

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**