Exam Questions C2150-612

IBM Security QRadar SIEM V7.2.6 Associate Analyst

https://www.2passeasy.com/dumps/C2150-612/

NEW QUESTION 1
Which log source and protocol combination delivers events to QRadar in real time?

A. Sophos Enterprise console via JDBC
B. McAfee ePolicy Orchestrator via JDBC
C. McAfee ePolicy Orchestrator via SNMP
D. Solaris Basic Security Mode (BSM) via Log File Protocol

Answer: C

NEW QUESTION 2
What is an effective method to fix an event that is parsed an determined to be unknown or in the wrong QReader category/

A. Create a DSM extension to extract the category from the payload
B. Create a Custom Property to extract the proper Category from the payload
C. Open the event details, select map event, and assign it to the correct category
D. Write a Custom Rule, and use Rule Response to send a new event in the proper category

Answer: B

NEW QUESTION 3
Which type of search uses a structured query language to retrieve specified fields from the events, flows, and simarc tables?

A. Add Filter
B. Asset Search
C. Quick Search
D. Advanced Search

Answer: D

Explanation: References:
http://www.ibm.com/support/knowledgecenter/en/SS42VS_7.2.7/com.ibm.qradar.doc/c_qradar_ug_search_bar.

NEW QUESTION 4
Which device uses signatures for traffic analysis when deployed in a network environment to detect, allow, block, or simulated-block traffic?

A. Proxy
B. QRadar
C. Switch
D. IDS/IPS

Answer: D

NEW QUESTION 5
What are two default Report Groups? (Choose two.)

A. Analyst
B. Executive
C. Administration
D. Log Management
E. Network Management

Answer: AC

NEW QUESTION 6
What is the correct procedure for closing an offense?

A. From the Offenses Ta
B. select the offense(s). click on Actions, select Close
C. From the Dashboard, select the offense(s) in question, right click and select Close
D. From the Offense Summary Page, click Display and select Close and select the reason
E. From the Offenses Ta
F. select the offense(s). right click on selection, select Close

Answer: A

NEW QUESTION 7
Which two high level Event Categories are used by QRadar? (Choose two.)

A. Policy
B. Direction
C. Localization
D. Justification

E. Authentication

Answer: AE

NEW QUESTION 8
What is the difference between TCP and UDP?

A. They use different port number ranges
B. UDP is connectionless, whereas TCP is connection based
C. TCP is connectionless, whereas UDP is connection based
D. TCP runs on the application layer and UDP uses the Transport layer

Answer: B

NEW QUESTION 9
What set of Key fields can trigger coalescing?

A. Source IP address, Source port, Severity, Username, and Event ID
B. Source IP address, Destination IP address, Destination port, Direction, and Event ID
C. Source IP address, Destination IP address, Destination port, Username, and Event ID
D. Destination IP address, Destination port, Relevance, Username, and Low Level Category

Answer: C

Explanation: References:
http://www-01.ibm.com/support/docview.wss?uid=swg21622709

NEW QUESTION 10
Events and Flows both have multiple different timestamps available to them. Which timestamp is available to both events and flows?

A. End Time
B. Storage Time
C. First Activity Time
D. Last Activity Time

Answer: D

NEW QUESTION 10
Which QRadar component is designed to help increase the search speed in a deployment by allowing more data to remain uncompressed?

A. QRadar Data Node
B. QRadar Flow Processor
C. QRadar Event Collector
D. Qradar Event Processor

Answer: A

NEW QUESTION 15
What is the largest differentiator between a flow and event?

A. Events occur at a moment in time while flows have a duration.
B. Events can be forwarded to another destination, but flows cannot.
C. Events allow for the creation of custom properties, but flows cannot.
D. Flows only contribute to local correlated rules, while events are global.

Answer: A

NEW QUESTION 18
Given the following supplied payload of a supported Juniper device:

```
[syslog@juniper.net dayId="20061012" recordId="0" timeRecv="2006/10/12 21:52:21"
timeGen="2006/10/12 21:52:21" devDomVer2="0" device_ip="10.209.83.4" cat="Predefined"
attack="TROJAN:SUBSEVEN:SCAN" srcAddr="192.168.170.20" srcPort="63396"
dstAddr="192.168.170.10" dstPort="27374" protocol="TCP" ruleVer="5" policy="Policy2"
rulebase="IDS" ruleNo="4" action="NONE" severity="LOW" alert="no" varEnum="31" misc="<017>'
interface=eth2"]
```

Which QRadar normalized fields will be populated?

A. Policy, Attack, Source IP, Username
B. Source IP, Destination I
C. Destination Port, Protocol
D. Source Port, Destination Port, Domain, Source Bytes
E. Source IP, Destination IP, Destination Por
F. Destination Bytes

Answer: B

NEW QUESTION 23
What is a primary goal with the use of building blocks?

A. A method to create reusable rule responses
B. A reusable test stack that can be used in other rules
C. A method to generate reference set updates without using a rule
D. A method to create new events back into the pipeline without using a rule

Answer: B

NEW QUESTION 25
What are three examples of a custom Dashboard? (Choose three.)

A. Asset View
B. Top Applications
C. Most Recent Offenses
D. Tabs which are accessible
E. Source and Destination DNS
F. Internet Threat Information Center

Answer: BCE

NEW QUESTION 30
Which QRadar component provides Layer 7 visibility within a physical network infrastructure?

A. QRadar Data Node
B. QRadar Flow Analyzer
C. QRadar Flow Collector
D. QRadar VFlow Collector

Answer: D

NEW QUESTION 32
Which key elements does the Report Wizard use to help create a report?

A. Layout, Container, Content
B. Container, Orientation, Layout
C. Report Classification, Time, Date
D. Pagination Option, Orientation, Date

Answer: A

Explanation: References:
IBM Security QRadar SIEM Users Guide. Page: 201

NEW QUESTION 35
When QRadar processes an event it extracts normalized properties and custom properties. Which list includes only Normalized properties?

A. Start time, Source IP, Username, Unix Filename
B. Start time, Username, Unix Filename, RACF Profile
C. Start time, Low Level Category, Source IP, Username
D. Low Level Category, Source IP, Username, RACF Profile

Answer: C

NEW QUESTION 36
What is the key difference between Rules and Building Blocks in QRadar?

A. Rules have Actions and Responses; Building Blocks do not.
B. The Response Limiter is available on Building Blocks but not on Rules.
C. Building Blocks are built-in to the product; Rules are customized for each deployment.
D. Building Blocks are Rules which are evaluated on both Flows and Events; Rules are evaluated on Offenses of Flows or Events.

Answer: A

NEW QUESTION 37
A Security Analyst was asked to search for an offense on a specific day. The requester was not sore of the time frame, but had Source Host information to use as well as networks involved, Destination IP and username.
Which fitters can the Security Analyst use to search for the information requested?

A. Offense ID, Source IP, Username
B. Magnitude, Source IP, Destination IP

C. Description, Destination I
D. Host Name
E. Specific Interval, Username, Destination IP

Answer: D

NEW QUESTION 40
What is a benefit of using a span port, mirror port, or network tap as flow sources for QRadar?

A. These sources are marked with a current timestamp.
B. These sources show the ASN number of the remote system.
C. These sources show the username that generated the flow.
D. These sources include payload for layer 7 application analysis.

Answer: D

Explanation: References:
https://www.ibm.com/developerworks/community/forums/html/topic?id=dd3861e0-f630-4a53-94c3-b426a47b6

NEW QUESTION 41
What are Mow sources used to monitor?

A. Vulnerability information
B. End point network activity
C. Server performance metrics
D. User account credential usage activity

Answer: C

NEW QUESTION 44
Which information can be found under the Network Activity tab?

A. Flows
B. Events
C. Reports
D. Offenses

Answer: A

NEW QUESTION 45
Which flow fields should be used to determine how long a session has been active on a network?

A. Start time and end time
B. Start time and storage time
C. Start time and last packet time
D. Last packet time and storage time

Answer: C

NEW QUESTION 48
What are the various timestamps related to a flow?

A. First Packet Time, Storage Time, Log Source Time
B. First Packet Time, Storage Time, Last Packet Time
C. First Packet Time, Log Source Time, Last Packet Time
D. First Packet Time, Storage Time, Log Source Time, End Time

Answer: B

Explanation: References:
IBM Security QRadar SIEM Users Guide. Page: 101

NEW QUESTION 53
What is the difference between an offense and a triggered rule?

A. Offenses are created every time a rule's tests are satisfied, but a rule may only trigger if the response limiter allows.
B. The first time a rule triggers, it will create an offense, after that no new offense will be created for the same index type.
C. A rule will always trigger if its tests are satisfied, but an offense may only be created if the event magnitude is greater than 6.
D. An offense may be created or updated by a triggered rule, but a rule will always trigger when the tests are satisfied.

Answer: B

NEW QUESTION 56

Which approach allows a rule to test for Active Directory (AD) group membership?

A. Import the AD membership information into the Asset Database using AXIS and use an asset rule test
B. Use the built-in LDAP integration to execute a search for each event as it is received by the EventProcessor to test for group membership
C. Maintain reference data for the AD group(s) of interest containing lists of usernames and then add rule tests to see if the normalized username is in the reference data
D. Export the AD group membership information to a CSV file and place it inthe /store/AD_mapping.csv file on the console, then use the "is a member of AD group' test in the rule

Answer: B

NEW QUESTION 58
How is an event magnitude calculated?

A. As the sum of the three properties Severity, Credibility and Relevance of the Event
B. As the sum of the three properties Severity, Credibility and Importance of the Event
C. As a weighted mean of the three properties Severity, Credibility and Relevance of the Event
D. As a weighted mean of the three properties Severity, Credibility and Importance of the Event

Answer: C

NEW QUESTION 62
What is the purpose of coalescing?

A. To reduce the number of events which count against EPS licenses
B. To reduce the amount of data received by QRadar event collectors
C. To reduce the amount of data going through the pipeline and stored onto disk
D. To reduce the number of offenses generated by QRadar as part of the tun.ng process

Answer: A

NEW QUESTION 64
What is an example of the use of a flow data that provides more information than an event data?

A. Represents a single event on the network
B. Automatically identifies and better classifies new assets found on a network
C. Performs near real-time comparisons of application data with logs sent from security devices
D. Represents network activity by normalizing IP addresses ports, byte and packet counts, as well as other details

Answer: D

Explanation: References:
http://www-01.ibm.com/support/docview.wss?uid=swg21682445

NEW QUESTION 65
What is the default view when a user first logs in to QRadar?

A. Report Tab
B. Offense Tab
C. Dashboard tab
D. Messages menu

Answer: C

Explanation: References:
http://www.ibm.com/support/knowledgecenter/SSKMKU/com.ibm.qradar.doc/c_qradar_dash_tab.html

NEW QUESTION 69
What are two common uses for a SI EM? (Choose two.)

A. Managing and normalizing log source data
B. Identifying viruses based on payload MD5s
C. Blocking network traffic based on rules matched
D. Enforcing governmental compliance auditing and remediation
E. Performing near real-time analysis and observation of a network and its devices

Answer: AC

NEW QUESTION 70
What is the maximum number of supported dashboards for a single user?

A. 10
B. 25
C. 255

D. 1023

Answer: C

Explanation: References:
http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/c_qradar_custom_dboard.ht

NEW QUESTION 75
Which type of rule requires a saved search that must be grouped around a common parameter

A. Flow Rule
B. Event Rule
C. Common Rule
D. Anomaly Rule

Answer: B

NEW QUESTION 80
An event is happening regularly and frequently; each event indicates the same target username. There is a rule configured to test for this event which has a rule action to create an offense indexed on the username.
What will QRadar do with the triggered rule assuming no offenses exist for the username and no offenses are closed during this time?

A. Each matching event will be tagged with the Rule name, but only one Offense will be created.
B. Each matching event will cause a new Offense to be created and will be tagged with the Rule name.
C. Events will be tagged with the rule name as long as the Rule Response limiter is satisfie
D. Only one offense will be created.
E. Each matching event will be tagged with the Rule name, and an Offense will be created if the event magnitude is greater than 6.

Answer: C

NEW QUESTION 83
Where can event data be exported from for external analysis?

A. From the Offenses Ta
B. select the offense and right click, select export event data
C. From the list of events page, select actions and click export to XML or export to CSV
D. From the offense summary page, select actions and click on export to XML or export to CSV
E. From the Offenses Ta
F. select the offense, click on actions, select export to XML or export to CSV

Answer: C

NEW QUESTION 85
What are the steps to get this window within an offense?
Given the following window:

A. Right click on the IP > Information > DNS Lookup
B. Right click on the IP > Information > Reverse DNS
C. Right click on the IP > Information > WHOIS Lookup
D. Right click on the IP > Information > Asset Profile

Answer: A

NEW QUESTION 90
Which advantage of a report helps distinguish it from a search?

A. Scheduling is available.
B. It can be added as a dashboard item.
C. It can be labeled for later use.
D. A report can be assigned to specific users.

Answer: A

NEW QUESTION 92
Which two pieces of information can be found under the Log Activity tab? (Choose two)

A. Offenses
B. Vulnerabilities
C. Firewall events

D. Destination Bytes
E. Internal QRadar messages

Answer: CD

NEW QUESTION 95
What is a difference between Rule Actions and Rule Responses?

A. Rule Actions are executed when the Rule is Disabled; Rule Responses require the Rule to be Enabled.
B. Rule Actions are only available for Event and Flow Rules; Rule Responses are available for all Rules.
C. Rule Actions only directly affect the SIEM internal
D. Rule Responses may send information to external systems.
E. Rule Responses are always processed; Rule Actions may be throttled to ensure they are not executed too frequently.

Answer: C

NEW QUESTION 97
What is the effect of toggling the Global/Local option to Global in a Custom Rule?

A. It allows a rule to compare events & flows in real time.
B. It allows a rule to analyze the geographic location of the event source.
C. It allows rules to be tracked by the central processor for detection by any Event Processor.
D. It allows a rule to inject new events back into the pipeline to affect and update other incoming events.

Answer: D

NEW QUESTION 101
A Security Analyst found multiple connection attempts from suspicious remote IP addresses to a local host on the DMZ over port 80. After checking related events no successful exploits were detected.
Upon checking international documentation, this activity was part of an expected penetration test which requires no immediate investigation.
How can the Security Analyst ensure results of the penetration test are retained?

A. Hide the offense and add a note with a reference to the penetration test findings
B. Protect the offense to not allow it to delete automatically after the offense retention period has elapsed
C. Close the offense and mark the source IP for Follow-Up to check if there are future events from the host
D. Email the Offense Summary to the penetration team so they have the offense id, add a note, and close the Offense

Answer: B

Explanation: References:
http://www.ibm.com/support/knowledgecenter/SSKMKU/com.ibm.qradar.doc/c_qradar_Off_Retention.html

NEW QUESTION 102
What is the primary goal of data categorization and normalization in QRadar?

A. It allows data from different kinds of devices to be compared.
B. It preserves original data allowing for forensic investigations.
C. It allows for users to export data and import it into other system.
D. It allows for full-text indexing of data to improve search performance.

Answer: A

NEW QUESTION 104
What is a Device Support Module (DSM) function within QRadar?

A. Unites data received from logs
B. Provides Vendor specific configuration information
C. Scans log information based on a set of rules to output offenses
D. Parses event information for SIEM products received from external sources

Answer: D

NEW QUESTION 106
Which pair of options are available in the left column on the Reports Tab?

A. Reports and Owner
B. Reports and Branding
C. Reports and Report Grouping
D. Reports and Scheduled Reports

Answer: B

NEW QUESTION 108
Which two actions can be performed on the Offense tab? (Choose two.)

A. Adding notes
B. Deleting notes
C. Hiding offenses
D. Deleting offenses
E. Creating offenses

Answer: AC

NEW QUESTION 113
Which three log sources are supported by QRadar? (Choose three.)

A. Log files via SFTP
B. Barracuda Web Filter
C. TLS multiline Filter
D. Oracle Database Listener
E. Sourcefire Defense Center
F. Java Database Connectivity (JDBC)

Answer: DEF

NEW QUESTION 115
What does the Network Hierachy provide relating to the "whole picture" that is helpful durin an investigation?

A. It allows hosts that are marked to be known to have vulnerabilities to be seen quickly.
B. It allows for the isolation of traffic between the hosts in question for more in depth analysis.
C. It allows for the removal of infected hosts from the network before being added back into the network.
D. It allows for the identification of known hosts on the network versus those that aren't members of the network.

Answer: D

NEW QUESTION 120
Which filter in the Log & Network Activity tabs is supported by both flows and events?

A. Source Payload Contains is [Pattern]
B. Application [Indexed] matches [Application]
C. Source IP [Indexed] equals any off [IP Address]
D. Username [Indexed] equals any of [Username]

Answer: C

NEW QUESTION 121
What are two benefits of using a netflow flow source? (Choose two)

A. They can include data payload
B. They can include router interface information.
C. They can include usernames involved in the flow.
D. They can include ASN numbers of remote addresses.
E. They can include authentication methods used to access the network.

Answer: BD

NEW QUESTION 124
Where are events related to a specific offense found?

A. Offenses Tab and Event List window
B. Dashboard and List of Events window
C. Offense Summary Page and List of Events window
D. Under Log Activity, search for Events associated with an Offense

Answer: A

NEW QUESTION 129
What is one of the major differences between event and network data (flow)?

A. Flows can replay a whole packet by packet sessions, while events are just a snapshot.
B. A flow can have a life span that can last seconds, minutes, hours or days, while events ate only a snapshot,
C. An event can have a life span that can last seconds, minutes, hours or days, while flows can only span 1 minute.
D. Events represent network activity by normalizing IP addresses, ports, byte and pucket count
E. while flows do not.

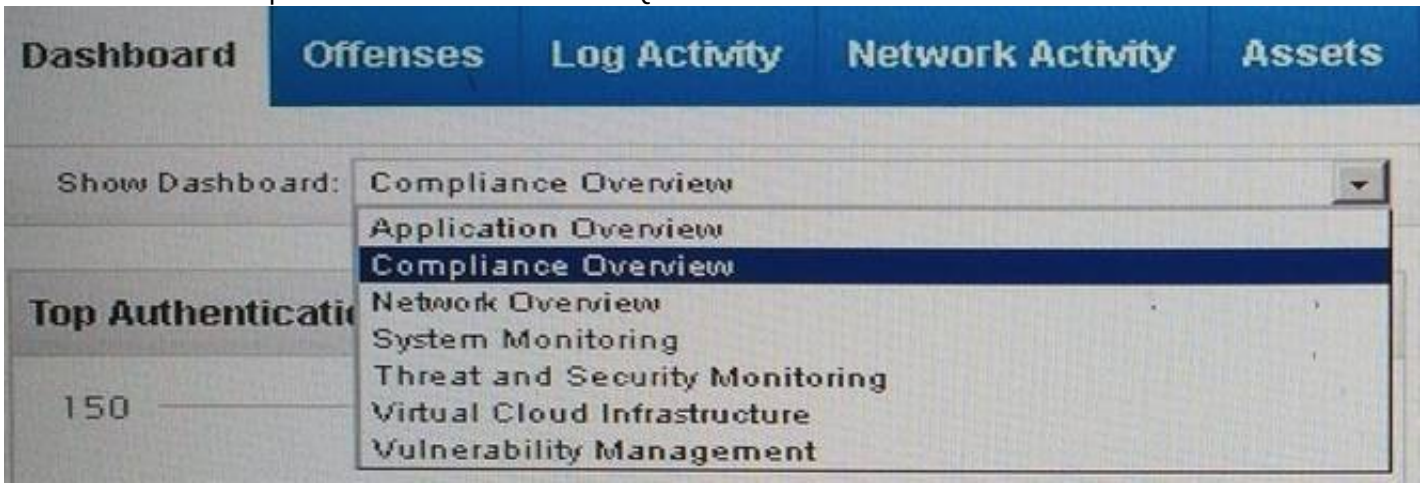
Answer: B

NEW QUESTION 133
Which column shows information as icons on the Reports tab?

A. Owner
B. Formats
C. Schedule
D. Report Name

Answer: B

NEW QUESTION 135
Given these default options for dashboards on the QRadar Dashboard Tab:



Which will display a list of offenses?

A. Network Overview
B. System Monitoring
C. Vulnerability Management
D. Threat and Security Monitoring

Answer: D

NEW QUESTION 138
Which file type is available for a report format?

A. TXT
B. DOC
C. PDF
D. PowerPoint

Answer: C

NEW QUESTION 142
Where can a user add a note to an offense in the user interface?

A. Dashboard and Offenses Tab
B. Offenses Tab and Offense Detail Window
C. Offenses Detail Window, Dashboard, and Admin Tab
D. Dashboard, Offenses Tab, and Offense Detail Window

Answer: B

Explanation: References:
IBM Security QRadar SIEM Users Guide. Page: 34

NEW QUESTION 146
Which QRadar add-on component can generate a list of the unencrypted protocols that can communicate from a DMZ to an internal network?

A. QRadar Risk Manager
B. QRadar Flow Collector
C. QRadar Incident Forensics
D. QRadar Vulnerability Manager

Answer: A

NEW QUESTION 149
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual C2150-612 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the C2150-612 Product From:

https://www.2passeasy.com/dumps/C2150-612/

Money Back Guarantee

C2150-612 Practice Exam Features:

* C2150-612 Questions and Answers Updated Frequently

* C2150-612 Practice Questions Verified by Expert Senior Certified Staff

* C2150-612 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* C2150-612 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year