IBM

Exam Questions C2150-612

IBM Security QRadar SIEM V7.2.6 Associate Analyst

NEW QUESTION 1
Which feature of a Next Generation Firewall is not available on previous firewalls?

A. VPN Support
B. Layer 3 based firewall rules
C. Integrated signature based IPS engine
D. Network and Port-Address Translation (NAT)

Answer: D

NEW QUESTION 2
What is a main function of a Cisco Adaptive Security Appliance (ASA)?

A. A Proxy
B. A Switch
C. A Firewall
D. An Authentication device

Answer: C

NEW QUESTION 3
What can be considered a log source type?

A. ICMP
B. SNMP
C. Juniper IOP
D. Microsoft SMBtail

Answer: C

NEW QUESTION 4
What is a primary benefit of building blocks?

A. They can notify users of strange behavior.
B. They allow the execution of its test within all rules.
C. They generate new events into the pipeline before rules fire.
D. They allow for report results to be used in custom rules tests.

Answer: B

NEW QUESTION 5
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 6
Which three data sources contribute to the creation an updates of assets? (Choose three.)

A. Log sources
B. Flow sources
C. Reference set imports
D. Vulnerability scanners
E. QRadar log source auto-updates
F. X-Force reference list integration

Answer: BEF

NEW QUESTION 7
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 8
Which QRadar component stores and forwards events from local and remote log sources?

A. QRadar Data Node
B. QRadar Event Collector
C. QRadar Event Processor
D. QRadar Distributed Console

Answer: B

NEW QUESTION 9
What are two default Report Groups? (Choose two.)

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

Answer: AC

NEW QUESTION 10
Which saved searches can be included on the Dashboard?

A. Event and Flow saved searches
B. Asset and Network saved searches
C. User and Vulnerability saved searches
D. Network Activity and Risk saved searches

Answer: A

NEW QUESTION 10
A Security Analyst has noticed that an offense has been marked inactive.
How long had the offense been open since it had last been updated with new events or flows?

A. 1 day + 30 minutes
B. 5 days + 30 minutes
C. 10 days + 30 minutes
D. 30 days + 30 minutes

Answer: B

NEW QUESTION 15
While on the Offense Summary page, a specific Category of Events associated with the Offense can be investigated.
Where should a Security Analyst click to view them?

A. Click on Events, then filter on Flows
B. Highlight the Category and click the Events icon
C. Scroll down to Categories and view Top 10 Source IPs
D. Right Click on Categories and choose Filter on Network Activity

Answer: B

Explanation: References:
IBM Security QRadar SIEM Users Guide. Page: 42

NEW QUESTION 17
Which kind of information do log sources provide?

A. User login actions
B. Operating system updates
C. Flows generated by users
D. Router configuration exports.

Answer: A

NEW QUESTION 19
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 22
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 24
What is the correct procedure to both assign and add a note to an offense from the Graphical User Interface (GUI)?

A. Both tasks must be done independently and can only be done on the Offenses Tab
B. With the new release of 7.2.6 this can now be done in one step from the Offenses Tab only.
C. Both tasks must be done independently but can be completed from both the Offenses Tab and the Offense Summary Page.
D. With the new release of 7.2.6 this can now be done in one step, both from the Offenses Tab and the Offense Summary Page.

Answer: D

NEW QUESTION 29
A Security Analyst, looking at a Log Activity search result, wants to limit the results to one Log Source. Which right-click method would be the fastest way for the Security Analyst to ensure this?

A. Right click on a Log Source name, then select Filter on Log Source is <log source>
B. Right click on a Source IP Address, then select Filter on Log Source is <log source>
C. Right click on the Log Source Type name, then select Filter on Log Source Group is <log source group>
D. Right click on the Log Source Group name, then select Filter on Log Source Group is <log source group>

Answer: A

NEW QUESTION 32
Which three optional items can be added to the Default and Custom Dashboards without requiring additional licensing? (Choose three.)

A. Offenses
B. Log Activity
C. Risk Change
D. Flow Search
E. Risk Monitoring
F. Asset Management

Answer: ACE

NEW QUESTION 33
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 38
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 39
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 40
Which set of information is provided on the asset profile page on the assets tab in addition to ID?

A. Asset Name, MAC Address, Magnitude, Last user
B. IP Address, Asset Name, Vulnerabilities, Services
C. IP Address, Operating System, MAC Address, Services
D. Vulnerabilities, Operative System, Asset Name, Magnitude

Answer: C

Explanation: References:
https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.1/com.ibm.qradar.doc_7.2.1/c_qradar_ug_asset_su

NEW QUESTION 45
What is a key difference between the magnitude of an event and the magnitude of an offense?

A. The magnitude of an event is derived when the event is received and does not vary, the magnitude of an offense can only increase.
B. The magnitude of an event is derived when the event is received and does not vary, the magnitude of an offense can increase or decrease over time.
C. The magnitude of an event is derived from the current magnitude of the offense it creates, the magnitude of an offense can increase or decrease overtime.
D. The magnitude of an event is derived when the event is received and does not vary, the magnitude of an offense is derived when the offense is created and does not vary.

Answer: B

NEW QUESTION 47
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 50
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 52
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 55
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 59
When using the right click event filtering functionality on a Source IP, one can filter by “Source IP is not [*]”. Which two other filters can be shown using the right click event filtering functionality? (Choose two.)

A. Filter on DNS entry [*]
B. Filter on Source IP is [*]
C. Filter on Time and Date is [*]
D. Filter on Source or Destination IP is [*]
E. Filter on Source or Destination IP is not [*]

Answer: BD

NEW QUESTION 63
Which information can be found under the Network Activity tab?

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

Answer: A

NEW QUESTION 66
Which Anomaly Detection Rule type is designed to test event and flow traffic for changes in short term events when compared against a longer time frame?

A. Outlier Rule
B. Anomaly Rule
C. Threshold Rule
D. Behavioral Rule

Answer: B

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

NEW QUESTION 71
Which QRadar rule could detect a possible potential data loss?

A. Apply “Potential data loss” on event of flows which are detected by the local system and when any IP is part of any of the following XForce premium Premium_Malware
B. Apply “Potential data loss” on flows which are detected by the local system and when at least 1000 flows are seen with the same Destination IP and different source in 2 minutes
C. Apply “Potential data loss” on events which are detected by the local system and when the event category for the event is one of the following Authentication and when any of Username are contained in any of Terminated_User
D. Apply “Potential data loss” on flows which are detected by the local system and when the source bytes is greater than 200000 and when at least 5 flows are seen with the same Source IP, Destination PortDestination IP in 12 minutes

Answer: D

NEW QUESTION 73
Where could you get additional details on why the offense was triggered when Summary page?

A. Display > Notes
B. Display > Rules
C. Display > Flows
D. Display > Events

Answer: B

NEW QUESTION 76
Which capability is common to both Rules and Building Blocks?

A. Rules and Building Blocks both set the Magnitude of an Event.
B. Rules and Building blocks both have the same selection of tests.
C. Rules and Building Blocks can both be Enabled/Disabled through the GUI.
D. Rules and Building Blocks both have Actions; Building Blocks do not have Responses.

Answer: D

NEW QUESTION 81
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 82
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 85
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 87
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 90
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 92
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 97
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 101
When might a Security Analyst want to review the payload of an event?

A. When immediately after login, the dashboard notifies the analyst of payloads that must be investigated
B. When “Review payload” is added to the offense description automatically by the “System: Notification” rule
C. When the event is associated with an active offense, the payload may contain information that is not normalized or extracted fields
D. When the event is associated with an active offense with a magnitude greater than 5, the payload should be reviewed, otherwise it is not necessary

Answer: C

NEW QUESTION 104
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 109
A Security Analyst is looking on the Assets Tab at an asset with offenses associated to it.
With a "Right Click" on the IP address, where could the Security Analyst go to obtain all offenses associated with it?

A. Information > Asset Profile
B. Navigate > View by Network
C. Run Vulnerability Scan > Source offenses
D. Navigate > View Source Summary or Destination Summary

Answer: C

NEW QUESTION 110
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 112
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 113
Which port does HTTP traffic commonly use?

A. Port 22
B. Port 53
C. Port 80
D. Port 443

Answer: C

NEW QUESTION 115

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 119
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 123
What is indicated by an event on an existing log in QRadar that has a Low Level Category of “Unknown”?

A. That event could not be parsed
B. That event arrived out of order from the original device
C. That event was from a device that is not supported by QRadar
D. That the event was parsed, but not mapped to an existing QRadar category

Answer: D

Explanation: References:
https://www.ibm.com/support/knowledgecenter/SSKMKU/com.ibm.dsm.doc/c_DSM_guide_UniversalLEEF_e

NEW QUESTION 126
When reviewing Network Activity, a flow shows a communication between a local server on port 443, and a random, remote port. The bytes from the local destination host are 2 GB, and the bytes from the remote, source host address are 40KB.
What is the flow bias of this session?

A. Other
B. Mostly in
C. Near-same
D. Mostly out

Answer: D

NEW QUESTION 127
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 132
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 135
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 136
Which three options are available on the New Search on the My Offenses and All Offenses pages (Choose three.)

A. Notes
B. Source IP
C. Magnitude
D. Attack Name
E. Malware Name
F. Specific Interval

Answer: BDF

NEW QUESTION 141
Which Anomaly Detection Rule type can test events or flows for volume changes that occur in regular patterns to detect outliers?

A. Outlier Rule
B. Anomaly Rule
C. Threshold Rule
D. Behavioral Rule

Answer: D

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

NEW QUESTION 144
What is a capability of the Network Hierarchy in QRadar?

A. Determining and identifying local and remote hosts
B. Capability to move hosts from local to remote network segments
C. Viewing real-time PCAP traffic between host groups to isolate malware
D. Controlling DHCP pools for segments groups (i.
E. marketing, DMZ, VoIP)

Answer: A

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

NEW QUESTION 147
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 150
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 154
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 159
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 161
Which list is only Rule Actions?

A. Modify Credibility; Send SNMP trap; Drop the Detected Event; Dispatch New Event.
B. Modify Credibility; Annotate Event; Send to Forwarding Destinations; Dispatch New Event.
C. Modify Severity; Annotate Event; Drop the Detected Event; Ensure the detected event is part of an offense.
D. Modify Severity; Send to Forwarding Destinations; Drop the Detected Event; Ensure the detected event is part of an offense.

Answer: A

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

NEW QUESTION 162
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 167
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 168
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 171
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 173
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 178
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 181
Which file type is available for a report format?

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

Answer: C

NEW QUESTION 182
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 183
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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