QUESTIONS & ANSWERS

Kill your exam at first Attempt

KILL EXAMS

IBM

C2150-614

IBM Security QRadar SIEM V7.2.7 Deployment

References:
http://www.ibm.com/support/knowledgecenter/SSKMKU/com.ibm.qradar.doc/c_qradar_adm_tenant_mg mt_overview.htmI

QUESTION: 53
A client has configured a log source to fonzvard events to IBM Security QRadar SIEM V7.2.7. It is recommended that the log source level be configured at the notice level by the DSM Guide, but the client has a policy to log all events at a debug level.
The Deployment Professional notices that the configured DSM is parsing most events, but some are being labeled as stored. The client is very interested in correlating some of the events that are being stored.
What should be created to meet this cIient's goal?

A. Custom flow property
B. Custom event property
C. Custom DSM for parsing overrule
D. Custom DSM for parsing enhancement

Answer: D

Explanation:
Parsing Enhancement- When the DSM is unable to parse correctly and the event is categorized as stored, the selected log source extension extends the failing parsing by creating a new event as if the new event came from the DSM.

References: I
BM Security QRadar SIEM Version 7.1.0 MRI, Log Sources User Guide, page 6

QUESTION: 54
You are tasked with configuring IBM Security QRadar SIEM V7.2.7 to pull a log file that generated daily at midnight from a custom application on a Microsoft© Windows Server. Which log source protocol should be used to accomplish this task?

A. WinCollect MSRPC
B. WinCollect Agent
C. WinCollect Log File
D. WinCollect File Forvvarder

Answer: B

Explanation:
A managed WinCoIIect deployment has a QRadar appliance that shares information with the WinCoIIect agent installed on the Windows hosts that you want to monitor. The Windows host can either gather information from itself, the local host, and, or remote Windows hosts.
Note: The WinCollect application is a Syslog event fon/varder that administrators can use for Windows event collection with QRadar. The WinCoIIect application can collect events from systems with WinCoIIect software installed (local systems), or remotely poll other Windows systems for events.

References:
http://www.ibm.com/support/knowledgecenter/SSKIVIKU/com.ibm.wincoIIect.doc/c_winco|Iect_overview_ new.htmI

QUESTION: 55
A Deployment Professional has a reference list of usernames that is used in rules. The Deployment Professional needs to be able to remove a username from the reference list when an offense is detected from a log event.
How can a Deployment Professional accomplish this goal?

A. As a rule response, select update Reference Set option
B. As a rule response, select remove from Reference Set option
C. As a rule response, select execute custom action in order to call REST-API: UPDATE:/reference_data/sets/{name}
D. As a rule response, select execute custom action in order to call REST-API: RENIOVE:/reference_data/sets/{name}/{value}

Answer: B

Explanation:
On the Rule Responses page of the customer rule, configure the responses that you want this rule to generate.
The rule response parameters include Remove from Reference Set, which is used to remove data from a reference set.
A reference set is a set of elements, such as a list of IP addresses or user names, that are derived from events and flows occurring on your network.

References:
http://www.ibm.com/support/knowledgecenter/SSKIVIKU/com.ibm.qradar.doc/t_qradar_create_cust_ruI.ht ml

QUESTION: 56
A Deployment Professional has created a new Building Block (BB), and it's not returning any expected events. The Deployment Professional has checked to ensure the BB is enabled and active. No errors are returned. What should be done to correct this BB problem?

A. Add your new custom BB to the "System: Load Building B|ocks" rule
B. Ensure that the BB has been set to "use" and a Deploy Full Configuration was done
C. Make sure that you use "GIobaI System" so that all of the QRadar deployment uses it
D. Manually enter in all QID's of the events it till monitor so it will automatically be used

Answer: A

Explanation:
Note: Question Will a building block of type: Common work when added to 'System: Load Building Blocks'? Answer The rule, System: Load Building Blocks is an Event only rule. If a building block is created from Type: Common, which includes both Events and Flows, and is then added to the System: Load Building Blocks rule, it will load, but will only refilect Event offenses and not Flow offenses. Flow offenses can be triggered when using Flow rules, which are then bound to the building block used in a Flow rule.

References:
http://wvwv-01 .ibm.com/support/docview.wss?uid=swg21963724

QUESTION: 57
A Deployment Professional has come on-site to upgrade a IBM Security QRadar SIEM V7.2.7 deployment to a new fix level. Before running the upgrade, the software and fix versions must be verified. What must the Deployment Professional verify?

A. Appliances in a deployment must be same version and same fix level.
B. Appliances in a deployment could be different version and different fix level.
C. Appliances in a deployment must be same version but fix level could be different.
D. Appliances in a deployment could be different version but fix level must be the same.

Answer: A

Explanation:
Software versions for all IBM Security QRadar appliances in a deployment must be

same version and fix level. Deployments that use different QRadar versions of software are not supported.

References:
IBM Security Qradar Version 7.2.7 Upgrade Guide, page 1
http://publIc.dhe.ibm.com/software/security/products/qradar/documents/7.2.7/en/b_qradar_upgrade.pdf

QUESTION: 58
A Deployment Professional has been asked to create a new dashboard which consists of utilizing a saved search. Which box should be checked when creating this search?

A. Add to my Dashboard
B. Include in my Dashboard
C. Add to my Dashboard items
D. Include in my Quick Searches

Answer: B

Explanation:
When you create a Search there is a parameter Include in my Dashboard, which must be selected to include the data from your saved search on the Dashboard tab.

References:
http://www-01 .ibm.com/support/docview.wss?uid=swg21679314#create

QUESTION: 59
A Deployment Professional is alerted that flows between two assets within a local network are communicating at a higher rate than normal between midnight and 2 a.m. The Deployment Professional is asked to determine why this is occurring and decides to create an alert that will send a notification when the communication happens again. Which action could be used?

A. Run an AQL query
B. Perform Quick search
C. Perform Custom search
D. Create rule to test for events/flows

Answer: D

Explanation:
IBM Security QRadar includes rules that detect a wide range of activities, including excessive firewall denies, multiple failed login attempts, and potential botnet activity. You can also create your own rules to detect unusual activity.

QUESTION: 60
A custom with IBM Security QRadar SIEIVI V7.2.7 is using Active Directory to authenticate users. After a crash, the authentication sewers are down and some users tried to log in before the authentication servers came back up. What will happen to these users?

A. Local users are able to log in with their local password.
B. Active Directory users are able to log in with their password.
C. Administrative and non-administrative users are unable to log in with their password until authentication sewers come back online.
D. Logging on is restricted to administrative users and non-administrative will needed to wait until the authentication sewer comes back online.

Answer: D

Explanation:
QRadar provides authentication options for both local and external authentication methods, such as Active Directory or LDAP.
The QRadar Administrative roles have both the external and local authentication methods available in case the external authentication method fails. If the remote authentication fails, the Administrative users can login using the local password.

References:
http://www-01 .ibm.com/support/docview.wss?uid=swg21959344