Practice Exam Questions

paloalto
NETWORKS

PCSAE

Palo Alto Networks Certified Security Automation Engineer

EXAMKILLER

Help Pass Your Exam At First Try

Paloalto Networks

Exam PCSAE

Palo Alto Networks Certified Security Automation Engineer

Version: 4.0

[Total Questions: 156]

Question No : 1

Reliability scores in XSOAR range from A through F. What do A and F stand for?

A. F - Reliability cannot be judged, A - Completely Reliable
B. F - Not reliable, A - Usually Reliable
C. F - Not usually reliable, A - Fairly Reliable
D. F - Unreliable, A - Completely Reliable

Answer: D

Question No : 2

Which two incident search queries are valid? (Choose two.)

A. created:>=”7 days”
B. owner===admin
C. role is Analyst
D. status:closed –category:job

Answer: A,D

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/5-5/cortex-xsoar-admin/cortex-xsoar- overview/how-to-search-in-cortex-xsoar.html

Question No : 3

Where can engineers add the post-processing scripts to incidents?

A. The post-processing tag must be added to the automation
B. Post-processing scripts must be added at the end of playbooks
C. Post-processing scripts must be added from the Incident Type editor
D. Post-processing scripts must be added from the Post-Process Rules editor

Answer: C

Question No : 4

How would context data be filtered to receive only malicious indicator values with DBotScore?

A. Get DBotScore.value where DBotScore.Score (Larger or equals) 4
B. Get DBotScore.value where DBotScore.Score (equals (int)) 3
C. Get DBotScore where DBotScore.Score (Larger than) 1
D. Get DBotScore where DBotScore.Score (Larger or equals) 2

Answer: B
Reference:
https://github.com/demisto/content/blob/master//Packs/DeprecatedContent/Integrations/PaloAlto_MineMeld/README.md

Question No : 5

How is data transferred between playbook tasks?

A. Read/Write from context data
B. Over war room results
C. Input from the indicator page
D. Directly from a previous task

Answer: A

Question No : 6

What are inputs and outputs in reference to a Playbook Development Lifecycle? (Choose three.)

A. Inputs are data pieces that are present in the playbook
B. Inputs are data pieces that are present in the task
C. Outputs are used as incident trigger for playbook
D. Outputs can be derived from the result of a task or command
E. Inputs are the data fields parsed by the Classifier

Answer: A,D,E

Question No : 7

Which two statements accurately describe layouts? (Choose two.)

A. Layouts override classification and mapping
B. New tabs can be added to the incident layout
C. Layouts can display incident information and custom fields
D. Layouts add or remove custom fields from an incident type

Answer: B,C

Question No : 8

Which configuration is a valid distributed database (DB) implementation?

A. 2 main DBs, 1 application server, 2 node servers
B. 1 main DB, 1 application server, 3 node servers
C. 2 application servers, 1 main DB, 1 node server
D. 1 application server, 2 main DBs, 1 node server

Answer: B

Question No : 9

Threat Intel search queries can be shared with which of the following? (Select 1)

A. Users defined in the platform (email or username)
B. Other organizations via the Marketplace
C. Users outside XSOAR via email invite
D. Roles defined in the platform

Answer: B

Question No : 10

Which of these would be the most operationally efficient repository for moving XSOAR custom content from a development server to a production environment?

A. A content repository specified in the Marketplace
B. Remote git repository specified in the dev-prod configuration parameters
C. The development server's default repository
D. Cortex XSOAR public content repository

Answer: B

Question No : 11

Whar are possible war room result (entry) types?

A. Context, file, error, image
B. Note, indicator, error, image
C. Video, file, error, image
D. Note, file, error, image

Answer: B

Question No : 12

An engineer asked for a specific command in an integration but the capability does not exist. The engineer decided to edit the existing integration by copying the integration and adding the needed commands.

What is the main concern when adding these commands?

A. The commands must return a proper result to the war room for the analysts to understand
B. The code may not be written to XSOAR standards
C. The integrations are locked and cannot be edited with additional commands
D. The custom integration will not be maintained and updated by XSOAR content team

Answer: D

Question No : 13

You need to retrieve a list of all malicious hashes over the last 30 days. What is the correct query to use?

A. type:File reputation:Malicious sourcetimestamp:"30 days ago"
B. type:File verdict:Malicious sourcetimestamp:<="30 days ago"
C. type:File reputation:Malicious sourcetimestamp:="30 days ago"
D. type:File verdict:Malicious sourcetimestamp:>="30 days ago"

Answer: A

Question No : 14

When creating an automation in XSOAR, what is the best way to create a log message?

A. Using a debug statement
B. Using the demisto.debug() function
C. Using a print statement
D. Using the demisto.results() function

Answer: B

Question No : 15

The XSOAR administrator is writing an automation and would like to return an error entry back into XSOAR if a particular command errors out. How can this be achieved?

A. Using the demisto_error() function
B. Using a print statement
C. Using the demisto.debug() function
D. Using the return_error() function

Answer: C

Question No : 16

Which two functions in XSOAR are incident types used for? (Choose two.)

A. To run dedicated playbooks for different event types
B. To classify events ingested from various sources into the relevant types
C. To classify indicators extracted in XSOAR incidents to their respective types
D. To facilitate role based access to XSOAR incidents

Answer: B,C

Question No : 17

Which of the following is a prerequisite to editing out-of-the-box (OOTB) content?

A. Download the content from the Marketplace.
B. Go to Settings > About >Troubleshooting and set a flag to allow custom content.
C. Register a user account with support.paloaltonetworks.com .
D. Detach the content item you want to edit from the Marketplace.

Answer: B

Question No : 18

Which field type provides an interactive and editable display of table-based data?

A. HTML
B. Grid (table)
C. Markdown
D. Multi Select

Answer: B

Question No : 19

An incident field is created having the display name as Source_IP. How can the field be accessed?

A. ${incident.sourceip}
B. ${incident.Source_IP}
C. ${incident.srcip}
D. ${incident.Source IP}

Answer: C

Question No : 20

Which three options can be defined in the layout settings? (Choose three.)

A. Set of fields to present
B. Permission to view the tab based on ‘Users’
C. Permission to view the tab based on ‘Roles’
D. Delete built-in tabs including the war room
E. Dynamic sections

Answer: A,C,E
Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-1/cortex-xsoar-admin/incidents/customize- incident-view-layouts/customize-incident-layouts.html

Question No : 21

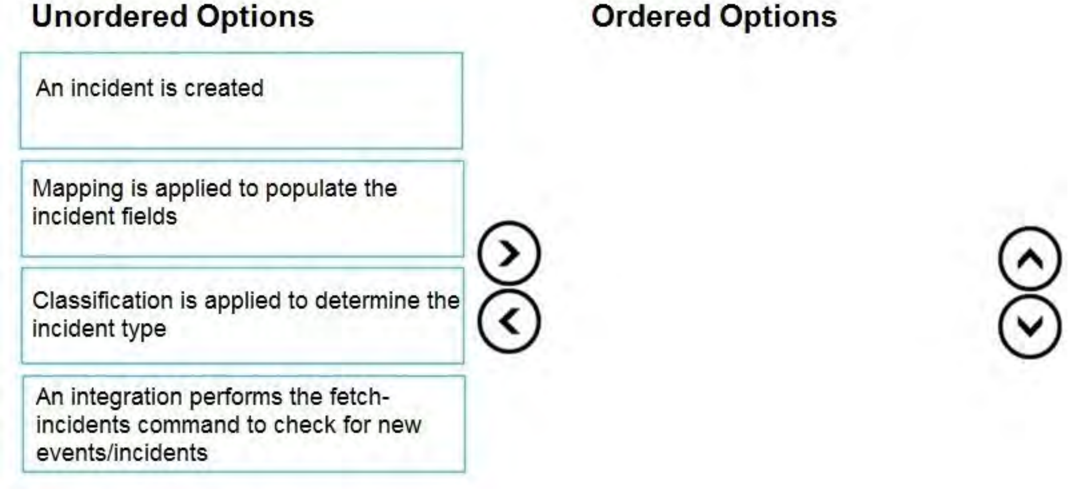
Can an automation script execute an integration command and an integration command execute an automation script?

A. An automation script cannot execute an integration command and an integration command cannot execute an automation script
B. An automation script can execute an integration command and an integration command cannot execute an automation script
C. An automation script cannot execute an integration command and an integration command can execute an automation script
D. An automation script can execute an integration command and an integration command can execute an automation script

Answer: B

Question No : 22 DRAG DROP

Arrange these steps in the order that they occur during an incident fetch.



Unordered Options

An incident is created

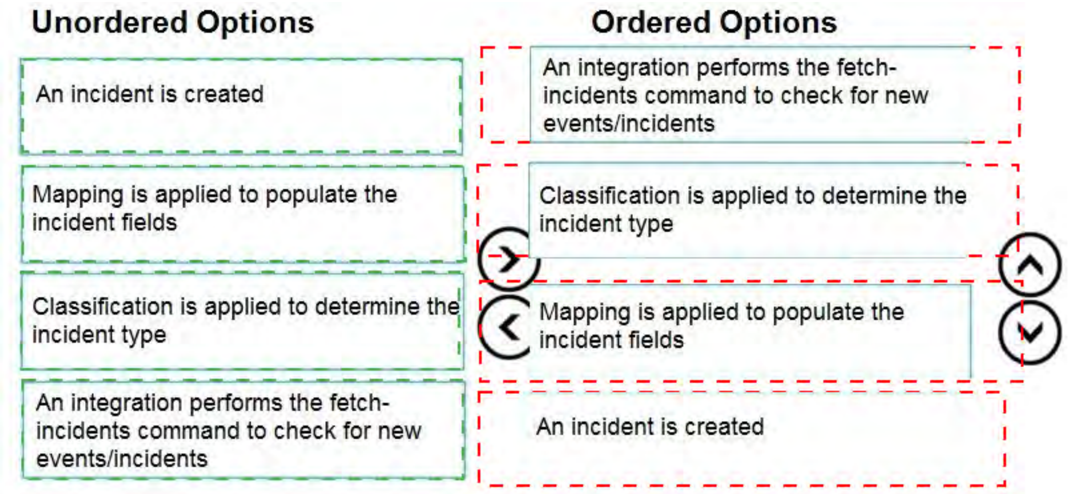
Mapping is applied to populate the incident fields

Classification is applied to determine the incident type

An integration performs the fetch-incidents command to check for new events/incidents

Ordered Options

Answer:



Unordered Options

An incident is created

Mapping is applied to populate the incident fields

Classification is applied to determine the incident type

An integration performs the fetch-incidents command to check for new events/incidents

Ordered Options

An integration performs the fetch-incidents command to check for new events/incidents

Classification is applied to determine the incident type

Mapping is applied to populate the incident fields

An incident is created

Explanation:

Integration performs

Classification is applied

Mapping is applied

Incident is created (before incident creation it should be also pre-process rule step)

Question No : 23

What are two common use cases for conditional tasks? (Choose two.)

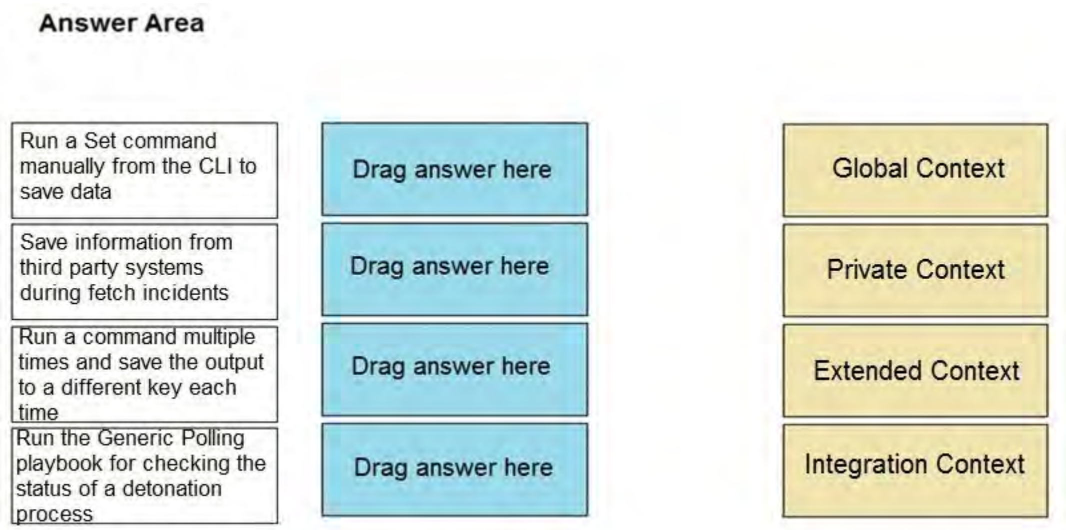
A. They are used for branching paths in a playbook
B. They are used to interact with users through survey functionality
C. They are used to determine which incident will be executed
D. They are used for sending a specific QUESTION NO: to a person or team

Answer: A,D

Reference: https://docs-new.paloaltonetworks.com/cortex/cortex-xsoar/5-5/cortex-xsoar-admin/cortex-xsoar- overview/use-cases.html#id7b31e50b-5aca-4d65-bdb5-ba61b4eac0b4

Question No : 24 DRAG DROP

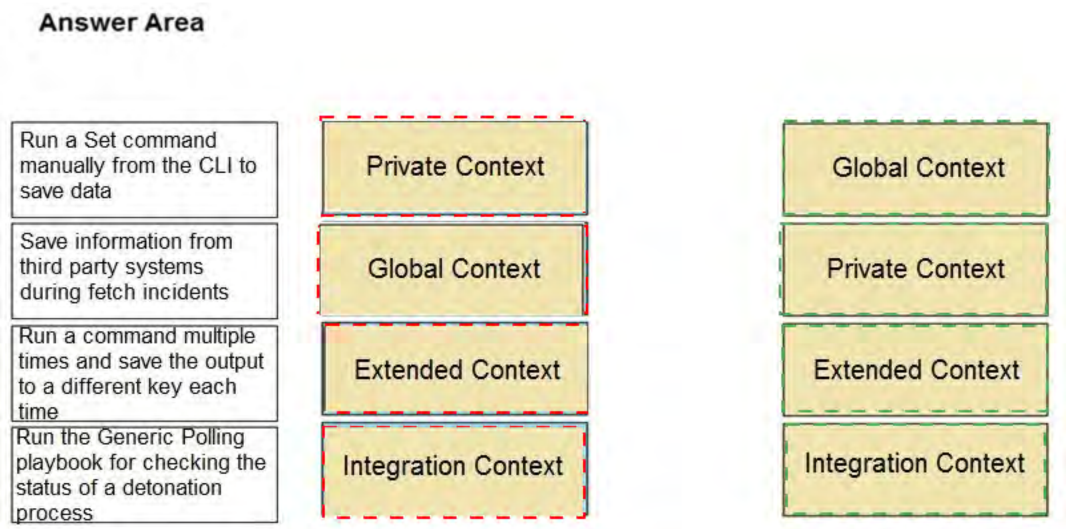
Match the operations with the appropriate context.



Answer Area

Run a Set command manually from the CLI to save data	Drag answer here	Global Context
Save information from third party systems during fetch incidents	Drag answer here	Private Context
Run a command multiple times and save the output to a different key each time	Drag answer here	Extended Context
Run the Generic Polling playbook for checking the status of a detonation process	Drag answer here	Integration Context

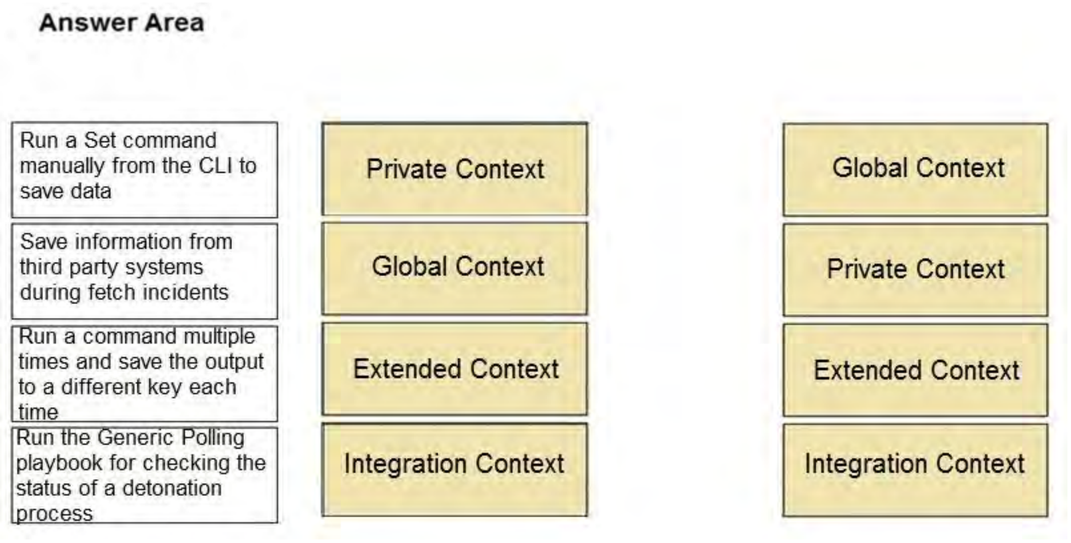
Answer:



Answer Area

Run a Set command manually from the CLI to save data	Private Context	Global Context
Save information from third party systems during fetch incidents	Global Context	Private Context
Run a command multiple times and save the output to a different key each time	Extended Context	Extended Context
Run the Generic Polling playbook for checking the status of a detonation process	Integration Context	Integration Context

Explanation:



Answer Area

Run a Set command manually from the CLI to save data	Private Context	Global Context
Save information from third party systems during fetch incidents	Global Context	Private Context
Run a command multiple times and save the output to a different key each time	Extended Context	Extended Context
Run the Generic Polling playbook for checking the status of a detonation process	Integration Context	Integration Context

Question No : 25

A playbook task generates a report as HTML in the context data.

An engineer creates a custom indicator field of type "HTML" and adds the field to a section in a custom indicator layout. How can the engineer populate the HTML field in the indicator layout?

A. Populate the custom indicator field with the built-in !SetIndicator command.
B. Add HTML to a list using !setList and use it as an HTML template to populate the custom indicator field.
C. Create a custom Indicator Mapper and populate the custom indicator field.
D. Use the Mapping option in the playbook task that generates the HTML report to populate the custom indicator field.

Answer: D
Reference: https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.6/Cortex-XSOAR-Administrator-Guide/Configure-the-HTML-Field

Question No : 26