PCSAE Q&As

Palo Alto Networks Certified Security Automation Engineer

Pass Palo Alto Networks PCSAE Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/pcsae.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

Correct Answer: C

QUESTION 2

Which two features does XSOAR offer to help recover from a server failure? (Choose two.)

A. Live backup (disaster recovery)

B. Distributed database

C. Backup data to XSOAR engines

D. Local backup

Correct Answer: AC

QUESTION 3

What happens when an integration is deprecated?

A. The integration commands in a playbook can no longer be used

B. The integration commands can be used, but it is recommended to update to the latest content pack

C. The configuration settings will be lost and the integration will no longer function

D. The integration commands in a playbook can be used, but it will fail at runtime

Correct Answer: C

QUESTION 4

In which two options can an automation script be executed? (Choose two.)

A. Engine

B. Integration

C. War room

D. Playbook

Correct Answer: CD

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar-admin/playbooks/automations.html

QUESTION 5

What is the most effective way to correlate multiple raw events coming from a SIEM and link them together?

A. Process all alerts by running the respective playbook and link related incidents during post-processing

B. Ingest all raw events, run a custom script to find the relationship between them and proceed to link them together

C. Configure a pre-process rule to link related events as they are ingested

D. Manually go through the incidents created by the raw events and link related incidents

Correct Answer: A

QUESTION 6

An XSOAR Engineer has developed a playbook and would like to contribute it to the XSOAR Marketplace to share with other users.

Which two options are available to the Engineer for contributing to the Marketplace? (Choose two.)

A. Open a ticket with the XSOAR support team

B. Create a pull request directly on Github

C. Contribute through the XSOAR UI

D. Send an email to contributions@xsoar.com

Correct Answer: BC

QUESTION 7

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

Correct Answer: C

QUESTION 8

In which two ways can data be transferred between playbooks and sub-playbooks? (Choose two.)

A. Inputs and outputs

B. Through integration context

C. Automatically extracted by sub-playbooks

D. From context data, if context is shared globally

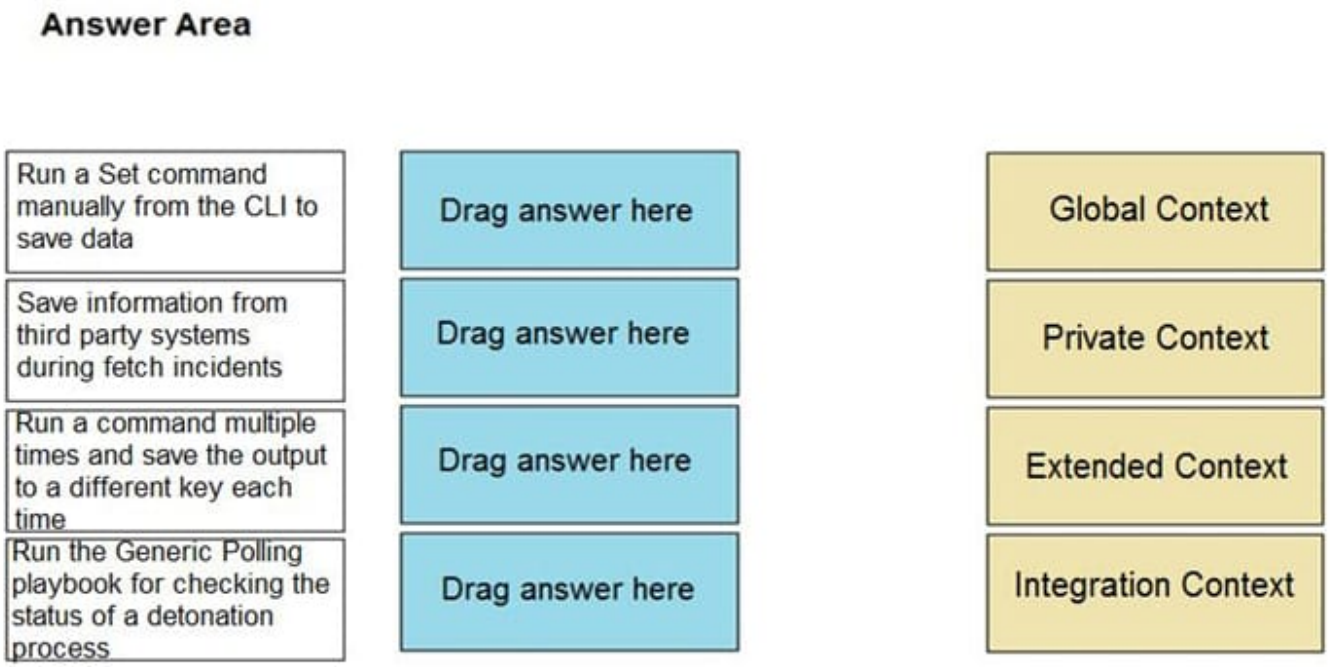
Correct Answer: AD

QUESTION 9

DRAG DROP

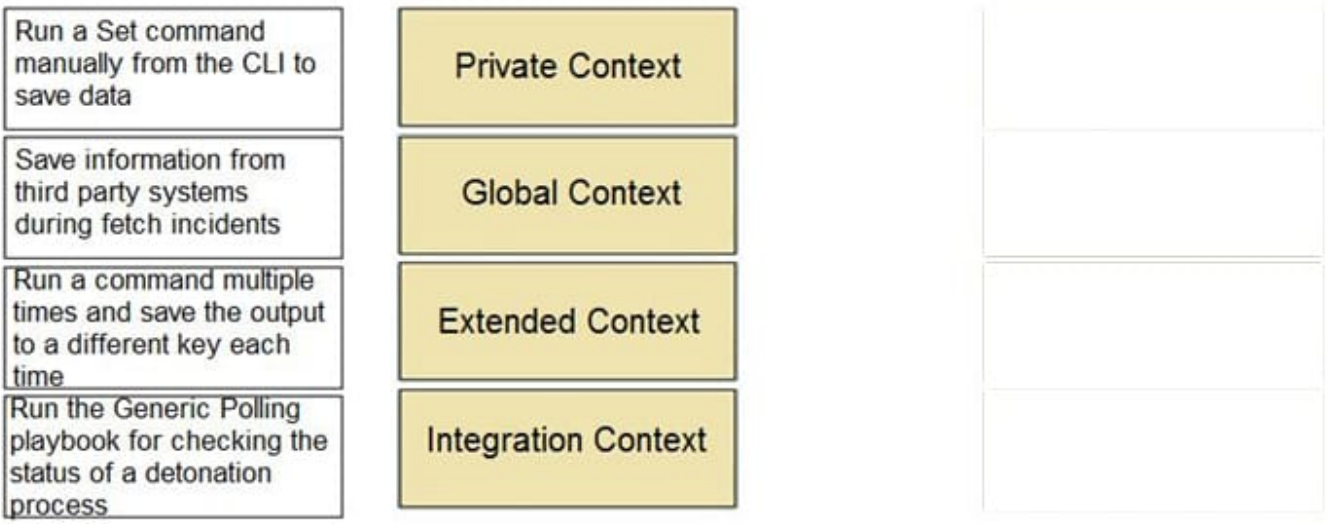
Match the operations with the appropriate context.

Select and Place:



Correct Answer:

Answer Area



QUESTION 10

An engineer\\'s organization system is registered in the following manner: . The engineer created a new indicator type for detecting systems using regex. The engineer would now like the username to be created as a separate `User\\' indicator automatically once a system is found.

What is the most efficient way for the engineer to achieve this?

A. Create a custom indicator field named `username\\' and link it to the internal system indicator

B. Change the reputation command for the internal system indicator type

C. Create a new indicator type of the internal username and set a formatting script to extract only the username

D. Create a new indicator type of the internal username and have the regex included on any string that has dash at the beginning

Correct Answer: B

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar-threat-intel-management-guide/manage-indicators/understand-indicators/indicator-types/indicator-type-profile

QUESTION 11

What are three different loop types in a playbook? (Choose three.)

A. Automation

B. Built-in

C. Data collection

D. Conditional

E. For-each

Correct Answer: CDE

QUESTION 12

Which method accesses a field called `User Mail\\' in a playbook?

A. ${incident.usermail}

B. ${incident.User Mail}

C. ${incident.UserMail}

D. ${usermail}

Correct Answer: A

QUESTION 13

A SOC manager built a dashboard and would like to share the dashboard with other team members. How would the SOC manager create a dashboard that meets this requirement?

A. Manually share the dashboard through user emails

B. Dashboard is shared to all XSOAR users

C. Propagate the dashboard based on SAML authentication

D. Dashboard is shared to all XSOAR users in a selected role

Correct Answer: D

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-1/cortex-xsoar-admin/dashboards/share-a-dashboard.html

QUESTION 14

Which built-in automation/command cab be used to change an incident\\'s type?

A. setIncident

B. Set

C. GetFieldsByIncidentType

D. modifyIncidentFields

Correct Answer: A

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/5-5/cortex-xsoar-admin/incidents/incidents-management/incident-fields/field-trigger-scripts.html

QUESTION 15

Which two situations would an engineer consider when configuring classification and mapping for an incident type? (Choose two.)

A. When creating incidents from the XSOAR REST API

B. When manually creating an incident from the UI

C. When adding a new analyst account to XSOAR

D. When fetching many different incident types from a single mailbox

Correct Answer: AB