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.passapply.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

QUESTION 1

An engineer would like to change an incident\\'s SLA according to the severity field changes. How can the engineer achieve this task?

A. Use a field trigger script

B. Use a field display script

C. Create a job that queries for incident severity changes

D. Change the SLA manually every time the severity changes

Correct Answer: B

Reference: https://xsoar.pan.dev/docs/incidents/incident-fields

QUESTION 2

Multiple company assets were reported by vulnerability scanners as being vulnerable to CVE-2017-11882. This vulnerability affects applications installed on workstations. The SOC team needs to take action and apply the new vulnerability patch that was just released. The team must first create a cause for each of the identified assets in ServiceNow IT Service Management (ITSM), in order to notify the IT department. Next, the team creates a task in the main playbook, which extracts the list of assets from the scanner report.

After the list of assets are created, what are the two solutions that the SOC team could take so that a case could be created and a patch installed? (Choose two.)

A. Create a sub-playbook with a single input containing the computer names that will loop until the last item from the asset list (Condition: AreValuesEqual – Exit on yes – left:1, right 1) and perform the following tasks:

-Active Directory User Enrichment based on the computerName

-Create the ServiceNow Record by adding the enrichment information

-Mark the ticket severity as Urgent

B. Create a sub-playbook with a single input containing the computer names that will loop `For Each Input\\' and perform the following tasks:

-Active Directory User Enrichment based on the computerName

-Create the ServiceNow Record by adding the enrichment information

-Mark the ticket severity as Urgent

C. Set a key for storing the iteration number and create a sub-playbook with a single input containing the computer names that will loop until the last item from the asset list (Exit condition: iterator contains the count of the number of items in the list) and perform the following tasks:

-Active Directory User Enrichment based on the computerName

-Create the ServiceNow Record by adding the enrichment information

-Mark the ticket severity as Urgent

D. Set a key for storing the iteration number and create a sub-playbook with a single input containing the computer names that will loop until the last item from the asset list (Exit condition: iterator equal to count of the number of item in the list) and perform the following tasks:

-Increase the iterator value by one each time

-Active Directory User Enrichment based on the computerName

-Create the ServiceNow Record by adding the enrichment information

-Mark the ticket severity as Urgent

Correct Answer: BD

QUESTION 3

An engineer notices that playbooks only start once the user clicks the `investigate\\' button and he/she would like the playbook to start automatically. How can this be implemented?

A. Add the playbook to the integration\\'s settings

B. Select `Run playbook automatically\\' from the incident type settings

C. Add the !startinvestigation automation to the beginning of the playbook

D. Select `Run playbook automatically\\' from the integration settings

Correct Answer: A

QUESTION 4

By default, which components does an XSOAR implementation include?

A. XSOAR server, XSOAR engine

B. Application server, distributed DB server

C. Application server, distributed DB server, Backup server

D. All in one server

Correct Answer: B

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar-admin/installation/install-demisto-on-a-physical-or-virtual-server.html

QUESTION 5

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

Correct Answer: B

QUESTION 6

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 7

Which two methods will allow data to be saved in incident fields within a playbook? (Choose two.)

A. setFields

B. Field mapping

C. setIncident

D. Layout inline editing

Correct Answer: BC

QUESTION 8

Which three statements are true about the Marketplace? (Choose three.)

A. Allows reverting back to a previous version of a content pack

B. Enables users to participate in the community by sharing content

C. Publishes content without additional review from the Cortex XSOAR team

D. Allows uploading of content in additional languages

E. Offers granularity in installation through content packs

Correct Answer: BCD

QUESTION 9

In which three locations can an engineer try to find information, when troubleshooting a failed integration instance error produced by the test button? (Choose three.)

A. The audit log

B. The log bundle

C. The source code for an integration

D. The error message returned directly below the button

E. The playground war room

Correct Answer: BCD

QUESTION 10

By default, automation written in which language will be executed in a Docker container?

A. Python

B. Go

C. JavaScript

D. Perl

Correct Answer: B

QUESTION 11

Which three support types are included in the Marketplace Content Packs? (Choose three.)

A. Customer supported

B. Contex XSOAR supported

C. Community supported

D. Partner supported

E. Prisma Cloud supported

Correct Answer: BCD

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar-admin/marketplace/marketplace-overview/content-packs-support-types.html

QUESTION 12

Which two causes may be occurring if an integration test is working, but the integration is not fetching incidents? (Choose two.)

A. The \\'Fetches Incidents\\' option may not have been enabled

B. There are no new events from the external service

C. The first fetch should be manually triggered to start the fetching process

D. It can take up to 1-hour before incidents are initially fetched

Correct Answer: AC

QUESTION 13

Which three authentication methods are supported when logging into XSOAR? (Choose three.)

A. OTP token

B. User name and password

C. SAML

D. Active Directory authentication

E. RADIUS

Correct Answer: CDE

Reference: https://www.paloguard.com/GlobalProtect.asp

QUESTION 14

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 15

In which two scenarios would it be appropriate to implement a loop for a sub-playbook? (Choose two.)

A. In repetitive process flows to iterate for each playbook input

B. When continuously ingesting incidents from third-party systems

C. In repetitive process flows with no more than 10 loops

D. In repetitive processes that requires sub-playbook re-execution

Correct Answer: AB