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.certbus.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 two input requirements are needed to train a machine learning model? (Choose two.)

A. 3000 Incidents

B. Incident Field

C. Verdict Label

D. Incident Type

Correct Answer: BD

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar- admin/machine-learing-models/machine-learning-models-overview.html

QUESTION 2

Which two solutions are available to scale an overloaded XSOAR environment? (Choose two.)

A. Add a distributed database server

B. Add an indexing server

C. Add a live backup server (disaster recovery)

D. Add an engine

Correct Answer: AC

QUESTION 3

Which two methods are used to add new content to the XSOAR Content Repository? (Choose two.)

A. Create content and add it to the standard content by contributing through the Marketplace

B. Use the XSOAR GitHub Contribution Guide to add the contribution to the standard content

C. Create a support ticket with the custom content for review by the support team

D. Any custom content will be automatically uploaded to the content repository

Correct Answer: AD

QUESTION 4

Which three actions can an engineer take on the troubleshooting page? (Choose three.)

A. Download the debug log bundle

B. Put the XSOAR server in maintenance mode

C. View and modify server configuration settings

D. Export and import custom content

E. View a list of server administrators

Correct Answer: ABC

QUESTION 5

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: B

QUESTION 6

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 7

Which development languages are supported when creating XSOAR automation scripts?

A. C++, Python, Powershell

B. Ruby, C++, Python

C. Javascript, Powershell, C++

D. Python, Powershell, Javascript

Correct Answer: D

QUESTION 8

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

QUESTION 9

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: B

QUESTION 10

Which investigation element is best suited for collaboration among users?

A. Work Plan

B. Related Incidents

C. War Room

D. Context Data

Correct Answer: D

Reference: https://blog.paloaltonetworks.com/2020/01/cortex-security-operations/

QUESTION 11

What is used to trigger playbooks automatically based on the classification of an incident?

A. Indicator type

B. Incoming mapper

C. Incident types

D. Integration configuration

Correct Answer: C

QUESTION 12

At what stage during the incident lifecycle is an incident type assigned?

A. Pre-processing

B. Incident creation

C. Classification

D. Playbook execution

Correct Answer: C

QUESTION 13

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

Correct Answer: A

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

Newly created subplaybooks do not have any inputs, or outputs. What is necessary to make them functional? (Choose two.)

A. Define input key in the subplaybook task. Map context values to pull from parent playbook.

B. The output of the previous task automatically becomes the input of the subplaybook.

C. Map inputs and outputs to the parent playbook and the subplaybook will use the same values.

D. Open the subplaybook and add inputs or outputs in the Playbook triggered task.

Correct Answer: AD

[PCSAE VCE Dumps](#)   [PCSAE Study Guide](#)   [PCSAE Braindumps](#)