Vendor: Palo Alto Networks

Exam Code: PCSAE

Exam Name: Palo Alto Networks Certified Security Automation Engineer

Version: DEMO

QUESTION 1
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: AD
Explanation:
https://docs.paloaltonetworks.com/cortex/cortex-xsoar/5-5/cortex-xsoar-admin/cortex-xsoar-overview/how-to-search-in-cortex-xsoar.html

QUESTION 2
What is the correct expression to use when filtering only PDF files?

A. Use File.Extension that does not equal (string comparison) PDF
B. Use File.Name contains PDF
C. Use File.Extension contains (general) PDF
D. Use File.Extension equals (string comparison) PDF

Answer: D

QUESTION 3
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: D

QUESTION 4
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 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 6
A large number of incidents were deleted by mistake.

Which two architecture components can be used to recover the lost data? (Choose two.)

A. Live backup
B. Engine
C. Distributed database
D. Local backup

Answer: AD
Explanation:
https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-6/cortex-xsoar-admin/disaster-recovery-and-live-backup/backup-the-database.html

QUESTION 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: BC

QUESTION 8
An engineer's organization system is registered in the following manner:

<SiteName-SystemID-Username>. 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

Answer: C

QUESTION 9
Which two options are the most effective for moving content between two environments? (Choose two.)

A. Remote repository based content sharing
B. UI based content import/export button
C. Copy the content backup from one environment file system (/var/lib/demisto/backup/content-backup-*) and move it to the other environment
D. Download the content items separately and upload them to the other environment

Answer: AC
Explanation:
https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar-admin/manage-data/migrate-data-to-another-server-for-multi-tenant.html

QUESTION 10
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: ACE
Explanation:
https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-1/cortex-xsoar-admin/incidents/customize-incident-view-layouts/customize-incident-layouts.html

QUESTION 11
What can be used as integration parameters?

A. URL, API key, port
B. URL, certificate, image
C. Token, query, playbook
D. User-password, csv file, query

Answer: A

QUESTION 12
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

Answer: AD

QUESTION 13
When uploading content, which two options could the upload include? (Choose two.)

A. Indicators
B. Incidents
C. Reports
D. Fields

Answer: AC

QUESTION 14
An engineer defined a dashboard which allows important metrics to be displayed. The engineer would like to make this dashboard the default dashboard.

How can it be accomplished?

A. Default Dashboard can be defined by `Role'
B. Use the server configuration key: default.dashboards
C. Save the dashboard as a widget and apply it to all users
D. Right click on the dashboard tab and `Set as Default'

Answer: A

QUESTION 15
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
Explanation:
https://github.com/demisto/content/blob/master//Packs/DeprecatedContent/Integrations/PaloAlto_MineMeld/README.md

QUESTION 16
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 17
Which two options will troubleshoot an integration's fetch incidents command? (Choose two.)

A. In the instance settings, enable the fetch incidents parameter and wait for one minute
B. Create a one task playbook with a fetch-incident command
C. execute !<integration_instance_name>-fetch
D. execute !<integration_name>-fetch

Answer: AC
Explanation:
https://xsoar.pan.dev/docs/integrations/fetching-incidents

QUESTION 18
Incidents need to be filtered by all of the following criteria:

1. Status - Pending
2. Exclude Category - Job
3. Severity - High
4. Owner - None (No owner assigned)
5. Type - Phishing
6. Email Subject - "You have won a million dollars"

What is the correct query syntax for the above incident search filter?

A. status=="Pending" && category!="job" && severity=="High" && owner=="None" && type=="Phishing" && emailsubject=="You have won a million dollars"
B. Status:Pending and -category:job and Severity:High and Owner:"" and Type:Phishing and Email Subject:You have won a million dollars
C. status:Pending and -category:job and severity:High and owner:"" and type:Phishing and emailsubject:"You have won a million dollars"
D. status:Pending or -category:job or severity:High or owner:"" or type:Phishing or emailsubject:"You have won a million dollars"

Answer: C
Explanation:
https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-1/cortex-xsoar-admin/cortex-xsoar-overview/how-to-search-in-cortex-xsoar.html#idcd7fe505-c1c1-42f5-a698-08b5710196d3

QUESTION 19
What does Script helper contain?

A. Available commands
B. Permission settings
C. Automation version history
D. Automation timeout configuration

Answer: A
Explanation:

https://xsoar.pan.dev/docs/concepts/xsoar-ide

QUESTION 20
When mapping incoming data to incident fields, which statement is correct?

A. Data that is not mapped is placed under labels
B. Only text fields are classified
C. Classification cannot be used if mapping is enabled
D. Every incoming field must be mapped

Answer: A

QUESTION 21
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

Answer: AB

QUESTION 22
Which two options may be added when a content pack is being installed? (Choose two.)

A. Lists
B. Roles
C. Other content packs
D. Indicator layouts

Answer: CD

QUESTION 23
What are two primary uses of standard tasks? (Choose two.)

A. To highlight different paths in a playbook
B. To generate new widgets for a dashboard
C. To create an incident or escalate an existing incident
D. To automate tasks such as parsing a file or enriching indicators

Answer: CD

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**