

DUMPS ARENA

Palo Alto Networks Certified Security Automation Engineer

Palo Alto Networks PCSAE

Version Demo

Total Demo Questions: 10

Total Premium Questions: 165

Buy Premium PDF

<https://dumpsarena.co>

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1 - (DRAG DROP)

DRAG DROP

Match the corresponding action with the appropriate playbook tasks.

Select and Place:

Answer Area

Standard Task	Drag answer here	Executes the IPReputation Command
Conditional Task	Drag answer here	Checks if an integration exists
Section Header Task	Drag answer here	Sends a survey to the access team for reviewing a specific user
Data Collection Task	Drag answer here	Acts as a label for organizing playbook structure

ANSWER:

Answer Area

Standard Task	Executes the IPReputation Command	Executes the IPReputation Command
Conditional Task	Checks if an integration exists	Checks if an integration exists
Section Header Task	Acts as a label for organizing playbook structure	Sends a survey to the access team for reviewing a specific user
Data Collection Task	Sends a survey to the access team for reviewing a specific user	Acts as a label for organizing playbook structure

Explanation:

Reference:

<https://docs.paloaltonetworks.com/cortex/cortex-xsoar/5-5/cortex-xsoar-admin/playbooks/playbooks-overview.html>

QUESTION NO: 2

In which two locations can filters and transformers be used in XSOAR? (Choose two.)

- A. Classification and Mapping
- B. Playbook Tasks
- C. Evidence Fields
- D. Incident Fields

ANSWER: B D

Explanation:

Reference: <https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar-admin/playbooks/filters-and-transformers.html>

QUESTION NO: 3

Where would you look to find a personalized view of your own incidents and tasks?

- A. Incident Summary View
- B. My Incidents
- C. My Threat Landscape
- D. My Dashboard

ANSWER: D

QUESTION NO: 4

What will happen if a playbook debugger is left running for more than 24 hours?

- A. By default, every 24 hours, the system closes any debugger sessions that have been open for more than 180 minutes.
- B. The session must be stopped during 180 minutes manually by administrator, user will receive notification automatically.
- C. The session will be running till stopped manually by administrator.
- D. By default, the system closes automatically any debugger session that have been open 180 minutes.

ANSWER: D

QUESTION NO: 5

Where are incident layouts customized?

- A. Settings > Object Setup > Incidents > Layouts
- B. Settings > Integrations > Instance configuration
- C. Settings > Object Setup > Indicators > Layouts
- D. Settings > Advanced > Incident Layouts

ANSWER: A

Explanation:

Reference: <https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.6/Cortex-XSOAR-Administrator-Guide/Customize-Incident-Layouts>

QUESTION NO: 6

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

ANSWER: B C D

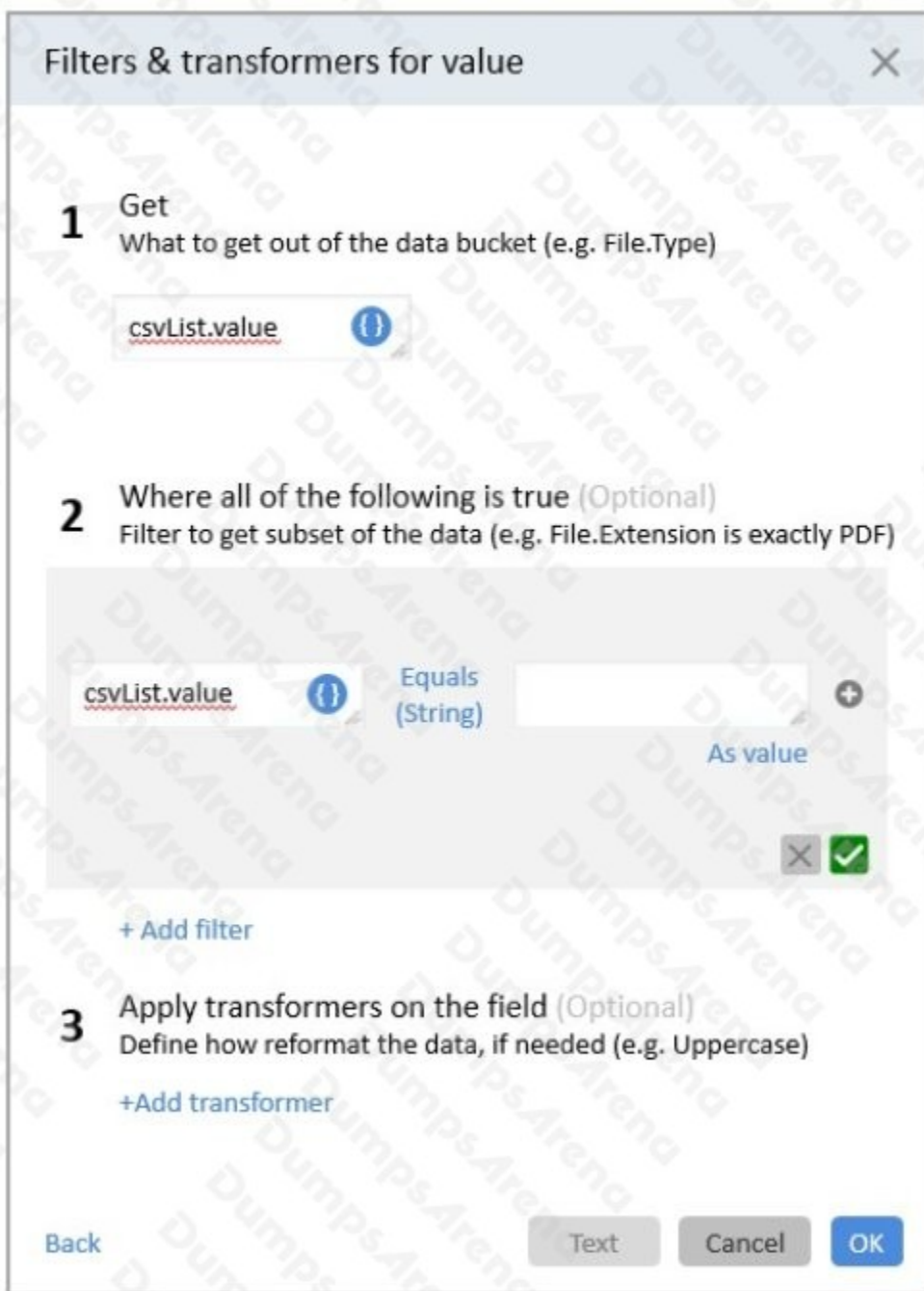
Explanation:

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

QUESTION NO: 7

An Engineer wants to filter a csvList value according to a dynamic value saved under the test context key.

Which three values would save the test context key? (Choose three.)



- A. Get csvList.value where csvList.value equals test [from previous tasks]
- B. Get csvList.value where csvList.value equals \${test} [from previous tasks]
- C. Get csvList.value where csvList.value equals test {}[from previous tasks]
- D. Get csvList.value where csvList.value equals test [as value]
- E. Get csvList.value where csvList.value equals \${test} [as value]

ANSWER: A B E

QUESTION NO: 8

Context

Context Data [X]

Search in JSON context data...

Collapse Expand

- File: [] 3 items
 - 0: [] 10 items
 - Size: 88226
 - SHA1: e6ef5142e2553c1e442a0ffac07636eac61e6edd
 - SHA256: cd6e64faec38579a9a96f0fb83327fbffec57b229446f111341d5397e5ffcbd3
 - SHA512: 733c94f19bfb5abdfc64cc11af6bec2cd563bad0af8627e7173fa2f55d2d575...
 - Name: weeklyOpenIncidents
 - SSDeep: 768:90pS0Hquln5T7Qo3QoipsHSOQ04080cTA0w0k7b7G0p0fhBHScd0S8...
 - EntryID: 169@14ce72de-6a01-4e32-8111-888ec3f5e778
 - Info: text/html
 - Type: HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF lin...
 - MD5: f5204d5822fca78cd5ab596826ce261f
 - 1: [] 10 items
 - Size: 5453
 - SHA1: 8d193fa162a305e4859ba8c48f5121f7265e3abb
 - SHA256: 2492ae51567eca2cb1b5132ccb535bff2b23cbfb54ff282906e1328c3da2a166
 - SHA512: ee346e6fc207c21bc880d247ea4655e68b43e575f1cd2087b49a4039fcf59d...
 - Name: weeklyOpenIncidents
 - SSDeep: 96:ZkFfw76dEzP7T1GdEMbnEYoUd+NKhAetVFWPRBNT5qitJ:WfVVKzT12...
 - EntryID: 170@14ce72de-6a01-4e32-8111-888ec3f5e778
 - Info: text/plain
 - Type: ASCII text, with very long lines, with CRLF line terminators
 - MD5: 120f4720d777abd54987bb44a5ff33e0
 - 2: [] 11 items
 - Size: 22640
 - SHA1: 1e56733826e5035233a097fcea2046af96ec616c
 - SHA256: 40a95bba020da46cd38e8f163062eb5d0bd57b3535c4ea2d143cf55e5fea2...
 - SHA512: 3f10428e47dfe79f8705d5a513c98c602d9e7c5fc70b022ab5dae33ffdda8c...
 - Name: incident by type..JPG
 - SSDeep: 192:VkrRkxO6vwrR4Q0eHELpb24tcwdj3DcaQ5Yt9gJA+uw84DtALp3LjfyIQW...
 - EntryID: 236@14ce72de-6a01-4e32-8111-888ec3f5e778
 - Info: image/jpeg
 - Type: JPEG image data, JFIF standard 1.01
 - MD5: 8b8150c3c2948d97532b20b2e8b0137a
 - Extension: JPG

Input

contextKey

contextKey	
Get	File.SHA1
Where	File.Size Greater than 6000
	File.Info Equals text/html
Transformers	To upper case

Given the following context data, what would be the expected output of the expression?

- A. 1E56733826E5035233A097FCEA2046AF96EC616C
- B. E6EF5142E2553C1E442A0FFAC07636EAC61E6EDD
- C. 8D193FA162A305E4859BA8C45F5121F7265E3ABB
- D. e6ef5142e2553c1e442a0ffac07636eac61e6edd

ANSWER: D

QUESTION NO: 9

Inside the Incidents table view, which actions can be performed on the selected incidents? (Choose two.)

- A. Run Command, Export, and Close and Delete for all selected incidents regardless of their status
- B. Assign, Edit, and Mark as Duplicate for all selected incidents regardless of their status
- C. Run Command for all selected incidents having Active status
- D. Export incidents as JSON and change incident status

ANSWER: A B

QUESTION NO: 10

What does Script helper contain?

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

ANSWER: A

Explanation:

Reference: <https://xsoar.pan.dev/docs/concepts/xsoar-ide>