DUMPSQUEEN

Palo Alto Networks System Engineer - Cortex Professional

Palo Alto Networks PSE-Cortex

Version Demo

Total Demo Questions: 10

Total Premium Questions: 60

Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

QUESTION NO: 1

The prospect is deciding whether to go with a phishing or a ServiceNow use case as part of their POC We have integrations for both but a playbook for phishing only Which use case should be used for the POC?

A. phishing

B. either

C. ServiceNow

D. neither

ANSWER: A

QUESTION NO: 2

Cortex XDR can schedule recurring scans of endpoints for malware. Identify two methods for initiating an on-demand malware scan (Choose two)

A. Response > Action Center

B. the local console

C. Telnet

D. Endpoint > Endpoint Management

ANSWER: A D

QUESTION NO: 3

In Cortex XDR Prevent, which three matching criteria can be used to dynamically group endpoints? (Choose three)

A. alert root cause

B. hostname

C. domain/workgroup membership

D. OS

E. presence of Flash executable

ANSWER: B C D

QUESTION NO: 4

Which option describes a Load-Balancing Engine Group?

A. A group of engines that use an algorithm to efficiently share the workload for integrations

B. A group of engines that ensure High Availability of Demisto backend databases.

C. A group of engines that use an algorithm to efficiently share the workload for automation scripts

D. A group of D2 agents that share processing power across multiple endpoints

ANSWER: C

QUESTION NO: 5

Which two filter operators are available in Cortex XDR? (Choose two.)

A. not Contains

B. !*

C. =>

D. < >

ANSWER: A B

Explanation:

: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-proadmin/get-started-with-cortex-xdr-pro/use-cortex-xdr/manage-tables.html

QUESTION NO: 6

Which CLI query would bring back Notable Events from Splunk?

A)

```
!splunk-search query="`notable` | head 3"
```

B)

```
!splunk-search query="'notable' | head 3"
```

C)

```
!splunk-search query="*"
```

D)

```
!splunk-search query="* | head 3"
```

A. Option A

B. Option B

C. Option C

D. Option D

ANSWER: D

QUESTION NO: 7

When analyzing logs for indicators, which are used for only BIOC identification'?

A. observed activity

B. artifacts

C. techniques

D. error messages

ANSWER: C

QUESTION NO: 8

Which two types of IOCs are available for creation in Cortex XDR? (Choose two.)

A. IP

B. endpoint hostname

C. domain

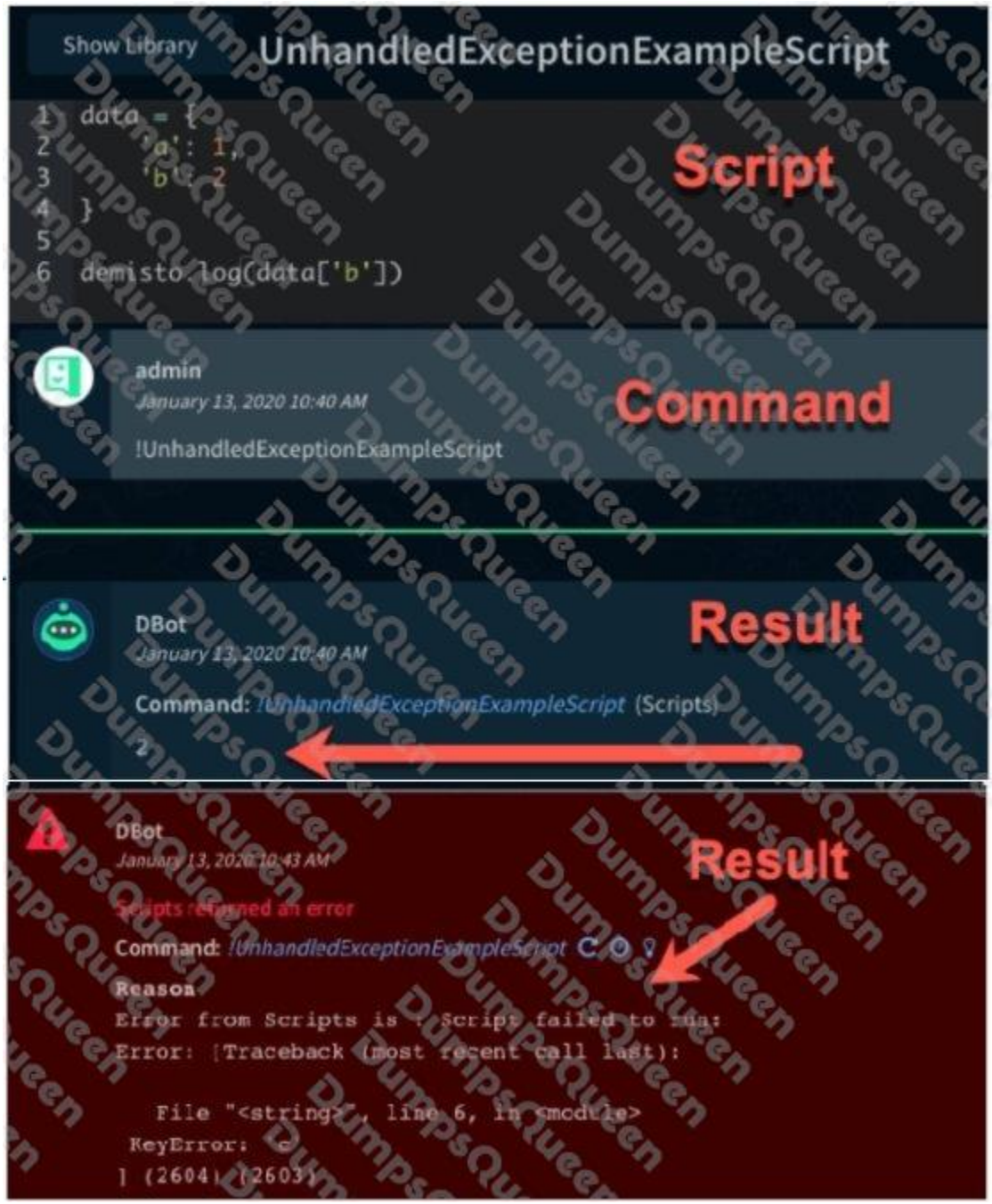
D. registry entry

ANSWER: A C

QUESTION NO: 9

The images show two versions of the same automation script and the results they produce when executed in Demisto. What are two possible causes of the exception thrown in the second Image? (Choose two.)

SUCCESS



A. The modified scnpt was run in the wrong Docker image

B. The modified script required a different parameter to run successfully.

C. The dictionary was defined incorrectly in the second script.

D. The modified script attempted to access a dictionary key that did not exist in the dictionary named "data"

ANSWER: A

QUESTION NO: 10

Which two items are stitched to the Cortex XDR causality chain" (Choose two)

A. firewall alert

B. SIEM alert

C. full URL

D. registry set value

ANSWER: A C