

KTest

更に上のクオリティ 更に上のサービス



問題集

<http://www.ktest.jp>

1年で無料進級することに提供する

Exam : **PCSAE**

Title : Palo Alto Networks Certified
Security Automation
Engineer

Version : DEMO

1. Reliability scores in XSOAR range from A through F.

What do A and F stand for?

- A. F - Reliability cannot be judged, A - Completely Reliable
- B. F - Not reliable, A - Usually Reliable
- C. F - Not usually reliable, A - Fairly Reliable
- D. F - Unreliable, A - Completely Reliable

Answer: A

2. 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: A,D

Explanation:

Reference: <https://docs.paloaltonetworks.com/cortex/cortex-xsoar/5-5/cortex-xsoar-admin/cortex-xsoar-overview/how-to-search-in-cortex-xsoar.html>

3. Where can engineers add the post-processing scripts to incidents?

- A. The post-processing tag must be added to the automation
- B. Post-processing scripts must be added at the end of playbooks
- C. Post-processing scripts must be added from the Incident Type editor
- D. Post-processing scripts must be added from the Post-Process Rules editor

Answer: C

4. 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:

Reference:

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

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