Question 1

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

Options:

A- Pre-processing

B- Incident creation

C- Classification

D- Playbook execution

Answer:

C

Question 2

Which of the following is a prerequisite to editing out-of-the-box (OOTB) content?

A- Download the content from the Marketplace.

B- Go to Settings > About >Troubleshooting and set a flag to allow custom content.

C- Register a user account with support.paloaltonetworks.com .

D- Detach the content item you want to edit from the Marketplace.

Answer:

B

Question 3

Question Type: **MultipleChoice**

Which of the following does a XSOAR Admin need to create an integration with a third party cloud application?

Options:

A- Marketplace access

B- Application with API

C- Private key/Public key integration

D- Multitenant deployment

Answer:

B

Question 4

Question Type: MultipleChoice

Select the correct incident life cycle on XSOAR.

Options:

A- Planning > Incident Ingestion > Incident Creation > Mapping and Classification > Pre-processing > Playbook runs > Post-processing

B- Planning > Incident Ingestion > Pre-processing > Incident Creation > Mapping and Classification > Playbook runs > Post-processing

C- Planning > Incident Ingestion > Pre-processing > Mapping and Classification > Incident Creation > Playbook runs > Post-processing

D- Planning > Incident Ingestion > Mapping and Classification > Pre-processing > Incident Creation > Playbook runs > Post-processing

Answer:

D

Question 5

Question Type: MultipleChoice

An administrator wants to run an automation in the War Room to set the incident field "Description" to "Confirmed Phishing". Which command should they enter in the War Room CLI?

Options:

A- !incidentSet description='Confirmed Phishing'

B- /incidentSet description=Confirmed Phishing

C- !setIncident description='Confirmed Phishing'

D- /setIncident description=Confirmed Phishing

Answer:

A

Question 6

Threat Intel search queries can be shared with which of the following? (Select 1)

Options:

A- Users defined in the platform (email or username)

B- Other organizations via the Marketplace

C- Users outside XSOAR via email invite

D- Roles defined in the platform

Answer:

B

Question 7

An analyst runs the following command in a playbook task:

!ip ip=1.1.1.1

Which extraction mode needs to be enabled on the Advanced tab of the playbook task to synchronously extract indicators from the results of this command?

Options:

A- Synchronous

B- Extract

C- Out of band

D- Inline

Answer:

D

Question 8

An administrator has noticed that an incident fetch has failed, causing several internal workflows to be backed up. The administrator would like to receive notifications the next time the incident fetch fails.

How can they achieve this?

Options:

A- Create a custom playbook that sends an email each time the fetch fails.

B- Create a new integration that monitors the incident fetch and sends an email if the fetch fails.

C- Schedule a job that runs and monitors incidents in XSOAR that will send an email if there are no new incidents.

D- Add a server config to notify when incident fetch fails.

Answer:

B

Question 9

An XSOAR engineer has been tasked with exporting all indicators from the production environment in the last 90 days. The final report needs to be in CSV format containing all indicator fields. How can this task be achieved?

Options:

A- Run the command !GetIndicatorsByQuery in CLI with its default arguments and export all indicators in the last 90 days.

B- SSH into the server and copy the indicator's database.

C- In the Threat Intel page, add query firstSeen:>='90 days ago', select All columns in Table View, and click Export to export as a CSV.

D- Run the command !findIndicators in CLI with the query firstSeen:>='90 days ago' and export to CSV.

Answer:

C