ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

Which two advanced attributes can be applied to incident fields when editing? (Choose two.)

A. Set a field trigger script

B. Associate to an incident type

C. Change field type

D. Change field name

Answer: AB

Explanation:

Reference: https://docs.servicenow.com/bundle/quebec-it-service-management/page/product/incident- management/reference/incident-management- properties.html

Question: 2

Given an incident with three files, how could the name of the second file be referenced?

A. ${Files.[2].Name}

B. ${Files.Name.[2]}

C. ${File.[1].Name}

D. ${File.Name.[1]}

Answer: D

Explanation:

Question: 3

Which component can be part of a load balancing group?

A. Distributed database
B. D2 agent
C. Engine
D. Load balancing server

Answer: C

Explanation:
Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/5-5/cortex-xsoar-admin/engines/understand- demisto-engines.html

Question: 4

Which method accesses a field called 'User Mail' in a playbook?

A. ${incident.usermail}
B. ${incident.User Mail}
C. ${incident.UserMail}
D. ${usermail}

Answer: A

Explanation:

Question: 5

A SOC manager built a dashboard and would like to share the dashboard with other team members. How

would the SOC manager create a dashboard that meets this requirement?

A. Manually share the dashboard through user emails
B. Dashboard is shared to all XSOAR users
C. Propagate the dashboard based on SAML authentication
D. Dashboard is shared to all XSOAR users in a selected role

Answer: D

Explanation:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-1/cortex-xsoar-admin/dashboards/share- a-dashboard.html

Question: 6

Which two methods will allow data to be saved in incident fields within a playbook? (Choose two.)

A. setFields
B. Field mapping
C. setIncident
D. Layout inline editing

Answer: BC

Explanation:

Question: 7

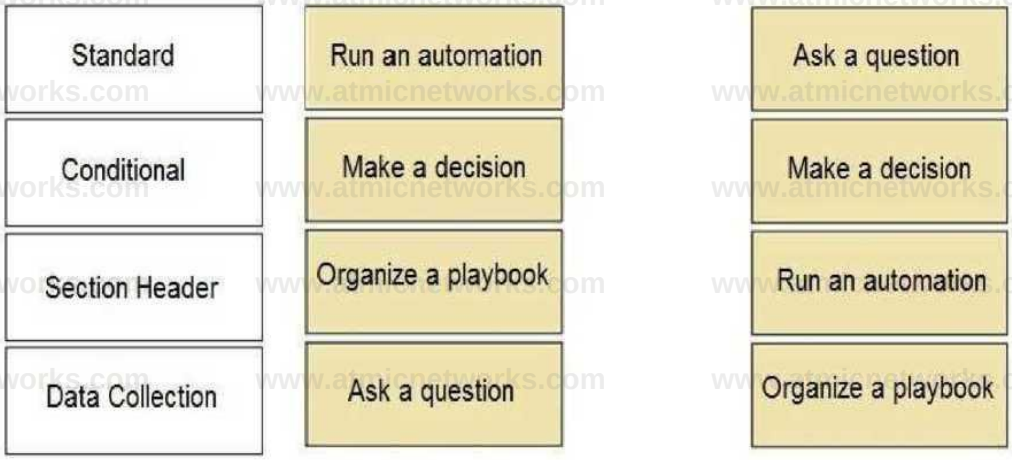
DRAG DROP
Match the action with the most appropriate playbook task type.

Answer Area

Answer:

Explanation:

Answer Area



https://www.jaacostan.com/2021/02/palo-alto-cortex-xsoar-playbook-icons.html

Question: 8

Which built-in automation/command cab be used to change an incident's type?

A. setIncident

B. Set

C. GetFieldsByIncidentType

D. modifyIncidentFields

Answer: A

Explanation:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/5-5/cortex-xsoar-admin/incidents/incidents- management/incident-fields/field-trigger-scripts.html

Question: 9

An engineer notices that playbooks only start once the user clicks the 'investigate' button and he/she would like the playbook to start automatically.

How can this be implemented?

A. Add the playbook to the integration's settings
B. Select 'Run playbook automatically' from the incident type settings
C. Add the !startinvestigation automation to the beginning of the playbook
D. Select 'Run playbook automatically' from the integration settings

Answer: B

Explanation:

Question: 10

Which two causes may be occurring if an integration test is working, but the integration is not fetching incidents? (Choose two.)

A. The 'Fetches Incidents' option may not have been enabled
B. There are no new events from the external service
C. The first fetch should be manually triggered to start the fetching process
D. It can take up to 1-hour before incidents are initially fetched

Answer: AB

Explanation:

Question: 11

Which two capabilities do Automation script settings include? (Choose two.)

A. Define 'parameters'
B. Correlate to incident types
C. Define 'outputs'
D. Set password protection

Answer: CD

Explanation:

Question: 12

DRAG DROP

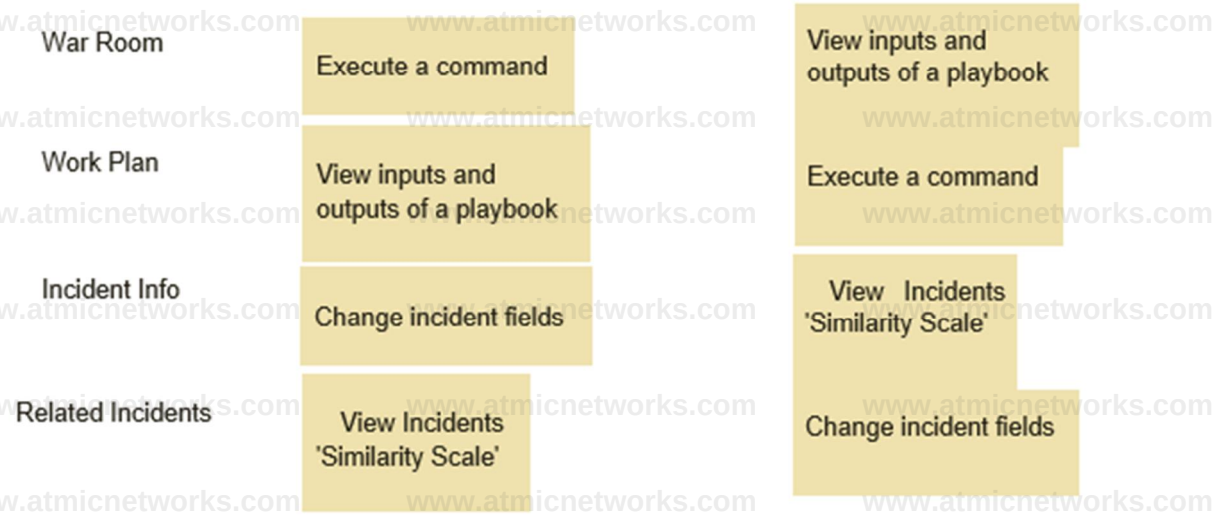
Match the appropriate action to the layout type.

Answer Area

Answer:

Explanation:

Answer Area



Question: 13

What is a primary use case of data collection tasks?

A. To allow multi-QUESTIO N NO: surveys without authentication restrictions

B. To automate tasks such as parsing a file or enriching indicators

C. To generate new widgets for a dashboard

D. To determine different paths in a playbook

Answer: A

Explanation:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/5-5/cortex-xsoar-admin/playbooks/playbook- tasks/communication-tasks/create-a-data-collection-task.html

Question: 14

In which three locations can an engineer try to find information, when troubleshooting a failed integration instance error produced by the test button? (Choose three.)

A. The audit log

B. The log bundle

C. The source code for an integration

D. The error message returned directly below the button

E. The playground war room

Answer: BCD

Explanation:

Question: 15

Which two statements describe how timers are configured to start and stop automatically in a playbook? (Choose two.)

A. Use a field of Number to count the number of seconds elapsed between two tasks

B. After the playbook has run, calculate the total time taken and set the timer field with this value

C. To begin counting time taken, add a task in the playbook with automation startTimer. To end the counting, add a task with automation stopTimer

D. From the Timers tab of the playbook task, choose the action for the timer and the timer field to perform the action on

Answer: CD

Explanation:

Question: 16

How long is the trial period for paid content packs?

A. 30 days
B. 14 days
C. 7 days
D. 60 days

Answer: A

Explanation:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar- admin/marketplace/ marketplace-subscriptions.html

Question: 17

After enriching a username using Active Directory, an engineer would like to send an email to the user's manager. However, this functionality is not part of the command output. The engineer checks with raw- response=true and notices that the manager's email is returned, but not saved in the context.

How can the engineer save the data so it will be accessible?

A. Mark ignore output = true
B. Use extend-context
C. Use raw-response = save
D. Mark ignore input = true

Answer: B

Explanation:
Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/5-5/cortex-xsoar-admin/playbooks/extend- context/extend-context-using-the-command-line.html

Question: 18

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

Explanation:

Question: 19

An engineer would like to present a trend using widgets to compare to a previous week's dat
a. Which two methods will allow the engineer to meet the requirement? (Choose two.)
A. Create widget of type Line, check 'Display Trend' and define as 7 days ago
B. Create a custom widget using a new incident query
C. Create widget of type Number, check 'Display Trend' and define as 7 days ago
D. Create a custom widget using a script

Answer: AD

Explanation:

Question: 20

What happens when an integration is deprecated?

A. The integration commands in a playbook can no longer be used

B. The integration commands can be used, but it is recommended to update to the latest content pack

C. The configuration settings will be lost and the integration will no longer function

D. The integration commands in a playbook can be used, but it will fail at runtime

Answer: B

Explanation:

Question: 21

Which investigation element is best suited for collaboration among users?

A. Work Plan

B. Related Incidents

C. War Room

D. Context Data

Answer: D

Explanation:

Reference: https://blog.paloaltonetworks.com/2020/01/cortex-security-operations/

Question: 22

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: BCD

Explanation:

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

Question: 23

Which three authentication methods are supported when logging into XSOAR? (Choose three.)

A. OTP token

B. User name and password

C. SAML

D. Active Directory authentication

E. RADIUS

Answer: CDE

Explanation:

Reference: https://www.paloguard.com/GlobalProtect.asp

Question: 24

Which two components have their own context data? (Choose two.)

A. Sub-playbook
B. Task
C. Field
D. Incident

Answer: AD

Explanation:

Question: 25

What are two main uses of context data? (Choose two.)

A. Store incident information in JSON format
B. Store incident information in XML format
C. Pass data between playbook tasks
D. Pass data between to-do tasks

Answer: AC

Explanation:

Reference: https://xsoar.pan.dev/docs/integrations/context-and-outputs#:~:text=The%20main%20use%20of% 20the,the%20Context%20and%20uses%20it.

Question: 26

Multiple company assets were reported by vulnerability scanners as being vulnerable to CVE-2017- 11882. This vulnerability affects applications installed on workstations. The SOC team needs to take action and apply the new vulnerability patch that was just released. The team must first create a cause for each of the identified assets in ServiceNow IT Service Management (ITSM), in order to notify the IT department. Next, the team creates a task in the main playbook, which extracts the list of assets from the scanner report.
After the list of assets are created, what are the two solutions that the SOC team could take so that a case could be created and a patch installed? (Choose two.)

A. Create a sub-playbook with a single input containing the computer names that will loop until the last item from the asset list (Condition: AreValuesEqual – Exit on yes – left:1, right 1) and perform the following tasks:

- Active Directory User Enrichment based on the computerName
- Create the ServiceNow Record by adding the enrichment information
- Mark the ticket severity as Urgent

B. Create a sub-playbook with a single input containing the computer names that will loop 'For Each Input' and perform the following tasks:

- Active Directory User Enrichment based on the computerName
- Create the ServiceNow Record by adding the enrichment information
- Mark the ticket severity as Urgent

C. Set a key for storing the iteration number and create a sub-playbook with a single input containing the computer names that will loop until the last item from the asset list (Exit condition: iterator contains the count of the number of items in the list) and perform the following tasks:

- Active Directory User Enrichment based on the computerName
- Create the ServiceNow Record by adding the enrichment information
- Mark the ticket severity as Urgent

D. Set a key for storing the iteration number and create a sub-playbook with a single input containing the computer names that will loop until the last item from the asset list (Exit condition: iterator equal to count of the number of item in the list) and perform the following tasks:

- Increase the iterator value by one each time

- Active Directory User Enrichment based on the computerName
- Create the ServiceNow Record by adding the enrichment information
- Mark the ticket severity as Urgent

Answer: BD

Explanation:

Question: 27

When creating a new tab in the layout, which section cannot be added?
A. Retrieve widget chart based on script
B. Related incidents
C. War room entries picked by entry query
D. Incident team members

Answer: B

Explanation:

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

Question: 28

In which two ways can data be transferred between playbooks and sub-playbooks? (Choose two.)
A. Inputs and outputs
B. Through integration context
C. Automatically extracted by sub-playbooks
D. From context data, if context is shared globally

Answer: AD

Explanation:

Question: 29

By default, which components does an XSOAR implementation include?

A. XSOAR server, XSOAR engine
B. Application server, distributed DB server
C. Application server, distributed DB server, Backup server
D. All in one server

Answer: B

Explanation:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar-admin/installation/install- demisto-on-a-physical-or-virtual-server.html

Question: 30

DRAG DROP

Match the operations with the appropriate context.

Answer Area

Run a Set command manually from the CLI to save data	Drag answer here	Global Context
Save information from third party systems during fetch incidents	Drag answer here	Private Context
Run a command multiple times and save the output to a different key each time	Drag answer here	Extended Context
Run the Generic Polling playbook for checking the status of a detonation orocess	Drag answer here	Integration Context

Answer:

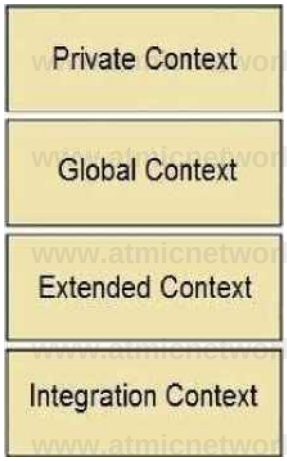
Explanation:

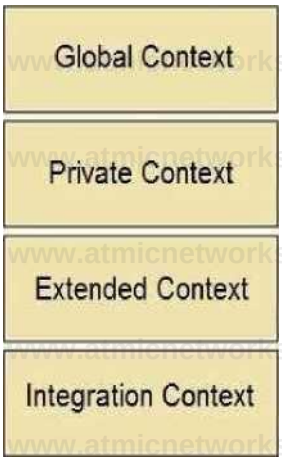
Answer Area

Run a Set command manually from the CLI to save data

Save information from third party systems during fetch incidents

Run a command multiple times and save the output to a different key each time ___ _____ Run the Generic Polling playbook for checking the status of a detonation process





Question: 31

Which three statements are true about the Marketplace? (Choose three.)

A. Allows reverting back to a previous version of a content pack
B. Enables users to participate in the community by sharing content
C. Publishes content without additional review from the Cortex XSOAR team
D. Allows uploading of content in additional languages
E. Offers granularity in installation through content packs

Answer: ABE

Explanation:

Question: 32

What can be added to ofload integration instance processing from the main server?

A. Database node

B. Application server

C. Engine

D. Development server

Answer: A

Explanation:

Question: 33

Which XSOAR architecture would be recommended for Managed Security Service Providers (MSSP)?

A. Multi-region

B. Dev-Prod

C. Multi-tenant

D. Distributed database

Answer: C

Explanation:
Reference: https://www.ncsi.com/wp-content/uploads/2020/11/cortex-xsoar.pdf

Question: 34

An incident field is created having the display name as Source_IP. How can the field be accessed?

A. ${incident.sourceip}

B. ${incident.Source_IP}

C. ${incident.srcip}

D. ${incident.Source IP}

Answer: C

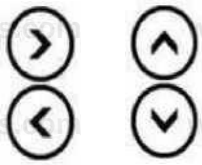
Explanation:

Question: 35

DRAG DROP

Arrange these steps in the order that they occur during an incident fetch.

Unordered Options	Ordered Options
An incident is created	
Mapping is applied to populate the incident fields	
Classification is applied to determine the incident type	
An integration performs the fetch-incidents command to check for new events/incidents	



Answer:

Explanation:

Integration performs

Classification is applied

Mapping is applied

Incident is created (before incident creation it should be also pre-process rule step)

Question: 36

An engineer deployed two different instances of Active Directory for each organization site. As part of account enrichment use case, the engineer would like to delete a user from one specific site.

Which command will accomplish this?

A. run 'ad-delete-user' command with 'user-dn' arg and using-brand="Active Directory Query v2"

B. run 'ad-delete-user' command with 'user-dn' arg and raw-response=true

C. run 'ad-delete-user' command with 'user-dn' arg and ignore-outputs=true

D. run 'ad-delete-user' command with 'user-dn' arg and using="Active Directory Query v2_instance_1"

Answer: D

Explanation:

Question: 37

An engineer is developing a playbook that will be run multiple times for testing purposes. What is the recommended first task to be used in the playbook?

A. DeleteContext

B. GenerateTest

C. PrintContext

D. SetContext

Answer: A

Explanation:

Reference: https://xsoar.pan.dev/docs/integrations/test-playbooks

Question: 38

What is the most effective way to correlate multiple raw events coming from a SIEM and link them together?

A. Process all alerts by running the respective playbook and link related incidents during postprocessing

B. Ingest all raw events, run a custom script to find the relationship between them and proceed to link them together

C. Configure a pre-process rule to link related events as they are ingested

D. Manually go through the incidents created by the raw events and link related incidents

Answer: C

Explanation:

Question: 39

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:

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

Question: 40

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

Explanation:

Question: 41

What 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: B

Explanation:

Question: 42

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

Explanation:

Question: 43

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

Explanation:

Question: 44

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
Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar-admin/disaster-recovery- and-live-backup/disaster-recovery-and-backup-overview.html

Question: 45

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

Explanation:

Question: 46

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

Explanation:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar-threat-intel-management- guide/manage-indicators/understand-indicators/indicator-types/indicator-type- profile

Question: 47

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: AB

Explanation:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar- admin/manage-data/

migrate-data-to-another-server-for-multi-tenant.html

Question: 48

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:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-1/cortex-xsoar-admin/incidents/customize- incident-view-layouts/customize-incident-layouts.html

Question: 49

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

Explanation:

Question: 50

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: AC

Explanation:

Question: 51

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

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

Answer: AB

Explanation:

Question: 52

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

Explanation:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-

admin/monitoring/cortex- xdr-dashboard/manage-dashboards.html

Question: 53

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

Question: 54

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

Explanation:

Question: 55

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:

Reference: https://xsoar.pan.dev/docs/integrations/fetching-incidents

Question: 56

DRAG DROP

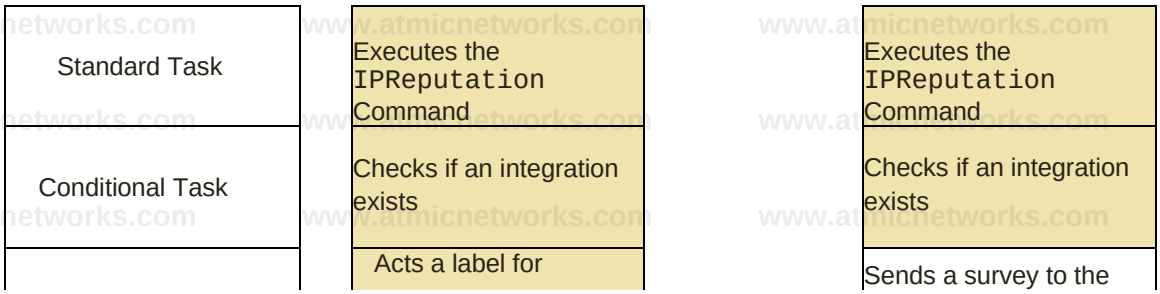
Match the corresponding action with the appropriate playbook tasks.

Answer Area

Answer:

Explanation:

Answer Area



Reference:

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

Question: 57

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:

Reference: 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: 58

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

Question: 59

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

Explanation:

Reference: https://xsoar.pan.dev/docs/incidents/incident-classification-mapping

Question: 60

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

Explanation:

Question: 61

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: AB

Explanation:

Question: 62

Which three scripting languages can an engineer use to write XSOAR automations? (Choose three.)

A. Python

B. Perl

C. Go

D. JavaScript

E. Powershell

Answer: ADE

Explanation:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar- admin/playbooks/

automations.html

Question: 63

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

Explanation:

Question: 64

An engineer would like to change an incident's SLA according to the severity field changes. How can the engineer achieve this task?

A. Use a field trigger script
B. Use a field display script
C. Create a job that queries for incident severity changes

D. Change the SLA manually every time the severity changes

Answer: A

Explanation:

Reference: https://xsoar.pan.dev/docs/incidents/incident-fields

Question: 65

What are three different loop types in a playbook? (Choose three.)

A. Automation
B. Built-in
C. Data collection
D. Conditional
E. For-each

Answer: CDE

Explanation:

Question: 66

What are two common use cases for conditional tasks? (Choose two.)

A. They are used for branching paths in a playbook

B. They are used to interact with users through survey functionality

C. They are used to determine which incident will be executed

D. They are used for sending a specific QUESTIO N NO: to a person or team

Answer: AD

Explanation:

Reference: https://docs-new.paloaltonetworks.com/cortex/cortex-xsoar/5-5/cortex-xsoar- admin/cortex-xsoar- overview/use-cases.html#id7b31e50b-5aca-4d65-bdb5-ba61b4eac0b4

Question: 67

An engineer wants to customize the regex for the default IP indicator type. How can this change be implemented?

A. Create a new indicator type and disable the built-in IP indicator

B. Edit the regex of the default IP Indicator

C. Add a new server configuration key that will overwrite the default regex of the IP indicator

D. Delete the default IP indicator

Answer: A

Explanation:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar-admin/manage-indicators/ understand-indicators/indicator-types/indicator-type-profile.html

Question: 68

In which two scenarios would it be appropriate to implement a loop for a sub-playbook? (Choose two.)

A. In repetitive process flows to iterate for each playbook input
B. When continuously ingesting incidents from third-party systems
C. In repetitive process flows with no more than 10 loops
D. In repetitive processes that requires sub-playbook re-execution

Answer: AB

Explanation:

Question: 69

Which configuration is a valid distributed database (DB) implementation?

A. 2 main DBs, 1 application server, 2 node servers
B. 1 main DB, 1 application server, 3 node servers
C. 2 application servers, 1 main DB, 1 node server
D. 1 application server, 2 main DBs, 1 node server

Answer: B

Explanation:

Question: 70

An engineer would like to add a custom field to the New Job form for a job triggered from a threat intel feed. How would the engineer implement this?

A. The new job form changes based on the threat intel feed integration configuration
B. The new job form can be edited from the Indicator Feed incident type editor
C. The new job form for a threat intel feed job cannot be edited
D. The new job form can be edited from the threat intel feeds integration settings

Answer: B

Explanation:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar-threat-intel-management- guide/manage-indicators/understand-indicators/create-a-feed-based-job.html

Question: 71

An automation returned an output called: csvReport.
What filter would be used to check if the automation returned results?

A. Contains/Includes
B. Equals/Matches
C. In/In list
D. Is defined/Exist

Answer: D

Explanation:

This filter will be used to check if the automation returned results, as it checks to see if the output variable called csvReport is defined and exists. If it is, then the automation returned results.

Question: 72

What is the difference between labels and fields?

A. Fields can be used in playbooks and labels cannot
B. Fields are indexed in the database and labels are not
C. Labels can be used in queries and fields cannot
D. Labels are indexed in the database and fields are not

Answer: C

Explanation:

Question: 73

What is the default task type when creating an empty task?

A. Standard (Manual)
B. Conditional
C. Section header
D. Standard (Automated)

Answer: B

Explanation:
Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/5-5/cortex-xsoar-admin/playbooks/playbook- tasks/playbook-task-fields.html

Question: 74

Which two methods are used to add new content to the XSOAR Content Repository? (Choose two.)
A. Create content and add it to the standard content by contributing through the Marketplace
B. Use the XSOAR GitHub Contribution Guide to add the contribution to the standard content
C. Create a support ticket with the custom content for review by the support team
D. Any custom content will be automatically uploaded to the content repository

Answer: AD

Explanation:

Question: 75

In which two options can an automation script be executed? (Choose two.)
A. Engine
B. Integration
C. War room
D. Playbook

Answer: CD

Explanation:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar- admin/playbooks/automations.html

Question: 76

By default, automation written in which language will be executed in a Docker container?

A. Python

B. Go

C. JavaScript

D. Perl

Answer: B

Explanation:

Question: 77

What is the correct definition regarding integration parameters and command arguments?

A. Parameters are global variables which means that every command can use these configurable options in order to run. Arguments are shared with other commands and must be present for each command.

B. Parameters are local variables which means that every command can use these configurable options in order to run. Arguments are shared with other commands and must be present for each command.

C. Parameters are local variables which means that every command can use these configurable options in order to run. Arguments are specific to only one command.

D. Parameters are global variables which means that every command can use these configurable options in order to run. Arguments are specific to only one command.

Answer: D

Explanation:

Question: 78

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

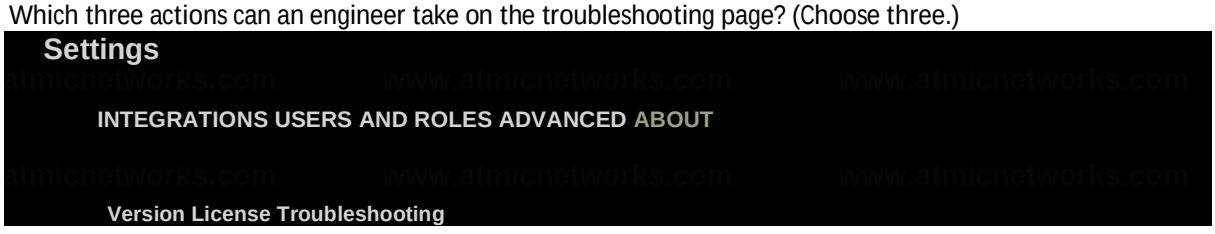
Answer: BD

Explanation:

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

Question: 79

Which three actions can an engineer take on the troubleshooting page? (Choose three.)



A. Download the debug log bundle
B. Put the XSOAR server in maintenance mode
C. View and modify server configuration settings

D. Export and import custom content

E. View a list of server administrators

Answer: ABC

Explanation:

Question: 80

An XSOAR Engineer has developed a playbook and would like to contribute it to the XSOAR Marketplace to share with other users.

Which two options are available to the Engineer for contributing to the Marketplace? (Choose two.)

A. Open a ticket with the XSOAR support team

B. Create a pull request directly on Github

C. Contribute through the XSOAR UI

D. Send an email to contributions@xsoar.com

Answer: BC

Explanation:

Question: 81

Which two input requirements are needed to train a machine learning model? (Choose two.)

A. 3000 Incidents

B. Incident Field

C. Verdict Label

D. Incident Type

Answer: BD

Explanation:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar-admin/machine-learing- models/machine-learning-models-overview.html

Question: 82

Which two solutions are available to scale an overloaded XSOAR environment? (Choose two.)

A. Add a distributed database server

B. Add an indexing server

C. Add a live backup server (disaster recovery)

D. Add an engine

Answer: AC

Explanation:

Question: 83

Management would like to get an incident report automatically following an incident's closure. How would this be accomplished?

A. Define a task in a playbook to generate an incident report before the closure occurs

B. Manually create an 'Incident Report'

C. Configure post-processing using a script

D. Create an 'Incident Report' from the Reports page

Answer: C

Explanation:

Question: 84

Which two reasons would lead an engineer to create a custom widget? (Choose two.)

A. To visualize server configuration keys
B. To visualize XSOAR list data
C. To visualize complex incident data calculations
D. To visualize context data
E. To visualize a custom query

Answer: DE

Explanation:

Reference: https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/cortex/cortex-xsoar/6-0/ cortex-xsoar-admin/cortex-xsoar-admin.pdf/cortex-xsoar-admin.pdf

Question: 85

While testing a custom integration, an XSOAR engineer noticed that the incident fetch interval is missing. How can this be fixed?

A. Define the Incident Fetch Interval when running the integration's commands.

B. Duplicate the integration. Edit the resulting copy and add incidentFetchInterval as a parameter. Save the integration. Configure the new integration instance with the interval required.

C. Configure the application to send incidents on the required interval.

D. Duplicate the integration. Add the interval in the code. Save the integration and Configure the new integration instance with the interval required.

Answer: A

Explanation:

Question: 86

What is the default landing page for a new user in XSOAR?

A. Dashboards
B. Threat Intel
C. Settings
D. Marketplace

Answer: A

Explanation:

Question: 87

On the System Diagnostics page, what is the default minimum size for a Work Plan to be considered big?

A. 2MB
B. 3MB
C. 1MB
D. 5MB

Answer: C

Explanation:

Question: 88

Which development languages are supported when creating XSOAR automation scripts?

A. C++, Python, Powershell
B. Ruby, C++, Python
C. Javascript, Powershell, C++
D. Python, Powershell, Javascript

Answer: D

Explanation:

Question: 89

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

Explanation:

Question: 90

You need to retrieve a list of all malicious hashes over the last 30 days. What is the correct query to use?

A. type:File reputation:Malicious sourcetimestamp:"30 days ago"

B. type:File verdict:Malicious sourcetimestamp:<="30 days ago"

C. type:File reputation:Malicious sourcetimestamp:="30 days ago"

D. type:File verdict:Malicious sourcetimestamp:>="30 days ago"

Answer: A

Explanation:

Question: 91

What is the default configuration for indicator auto-extraction when incidents are created?

A. Inline

B. Inband

C. None

D. Out of band

Answer: A

Explanation:

Question: 92

What are the out-of-the-box aggregate values that can be applied on widgets data?

A. Min, Max, Count, Average, Custom Transformers
B. Min, Max, Count, Average, Custom Group By
C. Count, Average, Sum, Min, Max
D. Count, Sum, Min, Max, Transformers

Answer: C

Explanation:

Question: 93

What assigns newly ingested event attributes to incident fields?

A. Playbooks
B. Classification
C. Mapping
D. Layouts

Answer: C

Explanation:

Question: 94

The XSOAR administrator is writing an automation and would like to return an error entry back into XSOAR if

a particular command errors out. How can this be achieved?

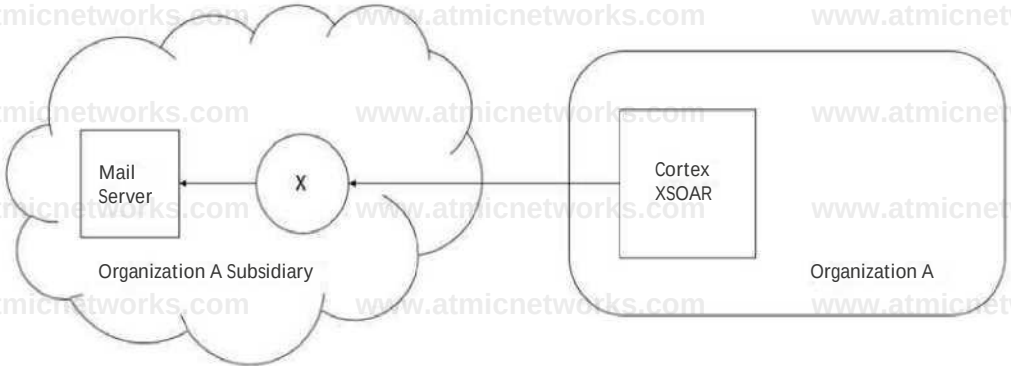
A. Using the demisto_error() function
B. Using a print statement
C. Using the demisto.debug() function
D. Using the return_error() function

Answer: C

Explanation:

Question: 95

An organization has recently acquired another company as its subsidiary. The subsidiary has its infrastructure on AWS cloud as illustrated in the image below:



The organization wants to use the mail server location on the subsidiary's cloud to send emails. Without acquiring additional licenses, which XSOAR component can fulfill the requirement?

A. XSOAR D2 Agents, to send the required emails.

B. An XSOAR engine that is downloaded from the XSOAR server and installed within the subsidiary.

C. Another XSOAR server that uses the same license as their primary XSOAR server.

D. A Linux server connected with an XSOAR server using SSH integration. Commands can be run remotely to access the mail server.

Answer: D

Explanation:

Question: 96

A playbook task generates a report as HTML in the context data.
An engineer creates a custom indicator field of type "HTML" and adds the field to a section in a custom indicator layout. How can the engineer populate the HTML field in the indicator layout?

A. Populate the custom indicator field with the built-in !SetIndicator command.

B. Add HTML to a list using !setList and use it as an HTML template to populate the custom indicator field.

C. Create a custom Indicator Mapper and populate the custom indicator field.

D. Use the Mapping option in the playbook task that generates the HTML report to populate the custom indicator field.

Answer: D

Explanation:

Reference: https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.6/Cortex-XSOAR-Administrator-Guide/Configure-the-HTML-Field

Question: 97

What are the three ways to add/mark entries as evidence inside the Evidence Board? (Choose three.)

A. Manually directly from the War Room with the Actions drop-down

B. From the Notes section (mark as entry icon)

C. Manually from the playbook task (mark as entry icon)

D. Automatically from playbook tasks when the option is selected on the Advanced tab

E. By running the command !MarkAsEvidence

Answer: A, B, D

Explanation:

Question: 98

Which tag must be applied to an Automation Script in order for it to be available when configuring an Indicator Type?

A. reputation-script

B. enrich

C. reputationScript

D. reputation

Answer: C

Explanation:

Question: 99

Which playbook will a job run by default?

A. The playbook assigned to the incident type

B. The playbook assigned to the indicator type

C. The playbook assigned during pre-processing

D. The playbook assigned by the integration

Answer: A

Explanation:

Question: 100

Which of the following is a feature of XSOAR automations?

A. can run on multiple docker containers

B. can be set to run on a scheduled basis in the automation settings

C. can be password protected

D. can be written in C++

Answer: B

Explanation:

Reference: https://www.paloaltonetworks.com/resources/datasheets/cortex-xsoar-overview

Question: 101

An administrator wants to send an email via the Mail Sender integration. Which of the following out of the box methods would be used for that?

A. XSOAR D2 agent

B. external integration command

C. XSOAR shared agent

D. common automation script

Answer: B

Explanation:

Question: 102

When is the post-processing script executed in XSOAR?

A. Just after the incident is created

B. Just after the pre-processing is executed

C. Just after the playbook is executed

D. Just after the Close Incident button is clicked

Answer: C

Explanation:

Question: 103

Which option is available in XSOAR to create the body of a Threat Intel Report?

A. Markdown

B. Grid Fields

C. DOC format

D. Javascript

Answer: A

Explanation:

Reference: https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.9/Cortex-XSOAR-Threat-Intel-Management-Guide/Create-a-Threat-Intel-Report

Question: 104

Context

File: |Tllnu
' 0: 010 item-
She 88226
SHA1: e€efS142e2553cle442a0ffa<07636eacGIe«edd
SHA2S6: cd6e64taec3«S79a9a9«Ofb83327fbffec5Zb229446! 111341d5397e5fkbd3
SHAS 12: 733c94f 19bfbSabdkMcc 11aftbec2cdS63bad0af862Ze7173fa2fS5d2dS7S...
Name: weektyOpenIncidents
SSDeep: 7G8.-9OpSOHquln5T7Qa3QoipsH5OQO4O8OcTAOwOk7b7GOpOfh0HScdOS8.„
EntrylO: 169^14ce72de 6a01 4e32 8111 8Mec3fSe778
Info: text/html
Type; HTML document, UTE 8 Unicode text, with wry long lines, with CRLF, IF Un...
MDS: tS204d5822fca78cdSabS96S2Ca2«If
' J; .- rr>-
Size: 5453
SHA1: 8dl93blWaJ05e4859ba8<48f5121f7265e3abb
SHA256: 2492aeSlS67eca2cblbS132ccbS3Sbff2b23cbn>S4ff2829O6el328<3da2al66
SHAS12: ee344e6k207c21bc880d247ea465Se68b43e575fkd2087b49a4039kf59d...
Name: weektyOpenIncidents
SSDeep: %^ZkFfw76dEtP7TlGd£MBnEYoUd*NKhAEtVFWPRBNl5qitJ;WFfVK2T12...
EntryID: 17 0@14ce7 2de-6a01-4e32-8111-888ec3f5e7 7 8
info: text/pbin
type: ASCI text, with very long Unes, with CRtF Une terminators
MDS: l20f4720d777abdM987bb44a5ff33e0
' 2: 11 Item
Stic 22640
SHA1: le56733826e503S233a097fcea2046af96ec616c
SHA256: 4Oa9Sbba020da46cd38e8fl63062eb5d0bdS7b3S35c4ea2dl43cfS5eSfea2.„
SHA512: 3fl0428e47dfe79f870SdSa513<98c602d9e7cSk70b022abSdae33ffdda8c...
Name: incident by type JPG
SSDeep: 192:VkRkx06vwR4yoeHlLpb24tcwdj30caQSYt9gjA*uw»4DtAl.p3lify<QW...
EntrylO: 2 36<214ce7 2deGaOl 4e3 2 8111 8«8ec3f5e?78
info: Image/jpeg
Type: JPEG image data. JFIF standard 1.01
MOS: 8b81SOc3c2948d97532b20b2e8bO137a
Extension: JPG

Input

con tod Key

FfeSHAI

FilcSiM Greater than 6000 FUe.Info Equals text/html

Get

To upper case

Where

Transformer

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

A. 1E56733826E5035233A097FCEA2046AF96EC616C

B. E6EF5142E2553C1E442A0FFAC07636EAC61E6EDD

C. 8D193FA162A305E4859BA8C45F5121F7265E3ABB

D. e6ef5142e2553c1e442a0ffac07636eac61e6edd

Answer: D

Explanation:

Question: 105

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: 106

How can Cortex XSOAR administrators prevent junior analysts from viewing a senior analyst dashboard?

A. Share the dashboard in Read and Edit mode for senior analysts.

B. Share the dashboard in Read & Edit mode for senior analysts and Read Only for juniors analysts.

C. Share the dashboard in Read and Write mode for senior analysts.

D. Share the dashboard in Read Only mode for junior analysts and senior analysts.

Answer: B

Explanation:

Reference: https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.5/Cortex-XSOAR-Administrator-Guide/Create-the-Read-Only-Dashboard

Question: 107

Which content type cannot be managed using remote repositories?

A. Lists

B. Jobs

C. Pre-processing rules

D. Exclusion List

Answer: A

Explanation:

Question: 108

An analyst wants to run a script to remove usernames from an incident before the incident becomes active in XSOAR. How can this be achieved?

A. Run an automation script in the Playground to remove usernames from the incident.

B. Create a pre-processing rule that runs an automation script to remove usernames from the incident as it comes into XSOAR.

C. Run an automation script on the XSOAR server to remove usernames from the incident.

D. Create a playbook task to remove the usernames from the incident.

Answer: B

Explanation:

Reference: https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.6/Cortex-XSOAR-Administrator-Guide/Incident-Management

Question: 109

Which task type would be used to verify/check that an integration was enabled?

A. Standard task
B. Conditional task

C. Section Header task

D. Data Collection task

Answer: D

Explanation:

Question: 110

What is used to trigger playbooks automatically based on the classification of an incident?

A. Indicator type

B. Incoming mapper

C. Incident types

D. Integration configuration

Answer: C

Explanation:

Question: 111

After executing the DeleteContext automation with all=yes argument, how would the context data of an incident present?

A. All the data, including the incident key will be deleted, and the context data will be completely empty.

B. No difference, the automation cannot be executed manually.

C. All context data, including custom incident fields will be deleted, system incident fields will remain.

D. All context data, except the incident key will be deleted.

Answer: D

Explanation:

Question: 112

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?

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

Explanation:

Question: 113

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?

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

Explanation:

Question: 114

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?

A. Synchronous

B. Extract

C. Out of band

D. Inline

Answer: D

Explanation:

Question: 115

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

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

Explanation:

Question: 116

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?

A. !incidentSet description="Confirmed Phishing"

B. /incidentSet description=Confirmed Phishing

C. !setIncident description="Confirmed Phishing"

D. /setIncident description=Confirmed Phishing

Answer: A

Explanation:

Question: 117

Select the correct incident life cycle on XSOAR.

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

Explanation:

Question: 118

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

A. Marketplace access

B. Application with API

C. Private key/Public key integration

D. Multitenant deployment

Answer: B

Explanation:

Question: 119

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

Explanation:

Question: 120

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

A. Pre-processing

B. Incident creation

C. Classification

D. Playbook execution

Answer: C

Explanation:

Question: 121

What can you use to assign a layout, field, and playbook to an incoming incident?

A. Playbook

B. Classification and mapping

C. Incident type

D. Pre-processing

Answer: B

Explanation:

Question: 122

For troubleshooting, after a log bundle is created, where do the logs appear on the XCSOAR server?

A. /var/lib/demisto

B. /tmp/log/demisto

C. /usr/local/demisto

D. /var/log/demisto

Answer: D

Explanation:

Question: 123

Which three types of information are displayed on the incident Quick View? (Choose three.)

A. Indicators and relationships

B. Timeline information

C. Evidence Board

D. Context data

E. Incident severity

Answer: A, B, C

Explanation:

Question: 124

Where do you navigate to monitor and improve the system performance and resilience for hosts in a multitenant environment?

A. Settings > About > Troubleshooting, in the main host account. Each host has a System Diagnostics page.

B. Settings > Advanced > System Diagnostics, in the main host account. Each host has a System Diagnostics page.

C. Settings > Account Management > Hosts, in the main host account. Each host has a System Diagnostics page.

D. Settings > About > System Diagnostics, in the main host account. Each host has a System Diagnostics page.

Answer: D

Explanation:

Question: 125

When creating an automation in XSOAR, what is the best way to create a log message?

A. Using a debug statement
B. Using the demisto.debug() function
C. Using a print statement
D. Using the demisto.results() function

Answer: B

Explanation:

Question: 126

What is an example of a generic reputation command?

A. !ip
B. !getReputation

C. !reputation

D. !enrichIndicator

Answer: C

Explanation:

Question: 127

During the regular maintenance of XSOAR a customer noticed that there was an update available for the Active Directory content pack (current version 1.4.6) and updated the content pack to the latest version (version 1.4.11). However, after the update the customer noticed that the Active Directory Query integration is not working properly and asked you to resolve the issue.

Which of the following set of steps can help to resolve the issue?

A. Navigate to Settings

View the configured integrations and select Active Directory Authentication

Delete all integration instances and add all integration instances again

B. Navigate to Marketplace

View the installed content pack and select Active Directory content pack

Select version 1.4.6 and click on "Revert to this version"

C. Navigate to Settings

View the configured integrations and select Active Directory Query

Delete all integration instances and add all integration instances again

D. Navigate to Marketplace

View the installed content pack and select Active Directory content pack

Click on uninstall content pack

Navigate to Marketplace browser and reinstall the Active Directory content pack

Answer: C

Explanation:

Reference: https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.8/Cortex-XSOAR-Administrator-Guide/Content-Pack-Update-Notifications

Question: 128

When developing the playbook, which of the following can be used by a XSOAR Administrator?

A. The Debugger panel to test data with one of last five incidents. This will affect the incident's original incident data.

B. Context data from existing incidents by exporting the YAML data from incidents and importing it to playbook editor.

C. Debugger panel and XML data from a similar incident with New Mock Incident. This will not affect the incidents original incident data.

D. The Debugger panel to test data with one of last fifty incidents. This will not affect the incident's original incident data.

Answer: C

Explanation:

Question: 129

Which field type provides an interactive and editable display of table-based data?

A. HTML

B. Grid (table)

C. Markdown

D. Multi Select

Answer: B

Explanation:

Question: 130

What is the function of timer SLA fields in Cortex XSOAR?

A. To track SLA breaches per playbook

B. To run a script that executes on SLA assignment

C. To automatically alert the analyst on SLA breach

D. To count the time between one or more tasks

Answer: C

Explanation:

Reference: https://docs-cortex.paloaltonetworks.com/cortex/cortex-xsoar//6-2/cortex-xsoar-admin/work-with-slas/create-an-sla-field

Question: 131

What are inputs and outputs in reference to a Playbook Development Lifecycle? (Choose three.)

A. Inputs are data pieces that are present in the playbook

B. Inputs are data pieces that are present in the task

C. Outputs are used as incident trigger for playbook

D. Outputs can be derived from the result of a task or command

E. Inputs are the data fields parsed by the Classifier

Answer: A, D, E

Explanation:

Question: 132

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

Explanation:

Question: 133

An administrator has noticed that an integration has failed to fetch incidents. Where would they go to download logs to troubleshoot the error?

A. Go to the Marketplace > Download the Fix my XSOAR playbook pack > Run the playbook > Download logs from War Room

B. Settings > About > Troubleshooting > Set Log Level to Debug > Download Logs
C. Dashboards & Reports > System Health
D. Settings > About > System Diagnostics

Answer: B

Explanation:

Question: 134

In Cortex XSOAR multi tenant setup, when content from a development server is pushed to the remote repository, where in the production server can the updates be found?

A. Main Account
B. Tenants
C. Agent tools
D. Marketplace

Answer: B

Explanation:

Reference: https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.6/Cortex-XSOAR-Multi-Tenant-Guide/Configure-a-Remote-Repository-on-the-Main-Account

Question: 135

To avoid exceeding API quotas for third-party services, indicators are only updated after the indicator cache expiration period. What is the default cache expiration period for indicators in XSOAR (minutes/days)?

A. 10,080 minutes (7 days)
B. 20,160 minutes (14 days)
C. 21,600 minutes (15 days)
D. 4,320 minutes (3 days)

Answer: D

Explanation:

Reference: https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.6/Cortex-XSOAR-Administrator-Guide/Indicator-Type-Profile

Question: 136

When browsing the Marketplace for new content packs, which details about each pack are you able to view?

A. The integration's source code

B. A summary of each version history

C. A test instance for the content pack

D. The source code of each playbook

Answer: B

Explanation:

Question: 137

A SOC analyst needs to retrieve the list of all open phishing incidents in the last 30 days. What is the correct query to use?

A. -status:closed -category:job type:Phishing created:>="30 days ago"
B. status:closed -category:job & type:Phishing created:>="30 days ago"

C. -status:closed -category:job & type:Phishing created:<="30 days ago"

D. -status:closed -category:job type:Phishing created:="30 days ago"

Answer: C

Explanation:

Question: 138

During configuration of the inputs of a sub-playbook in the main playbook, there is an option under the Loop tab called "For Each Input". What is this option used to?

A. To loop the sub-playbook over all context values present in the investigation

B. To loop the sub-playbook over all incident fields for the given incident

C. To loop the sub-playbook over all the fields marked as important

D. To loop the sub-playbook over all defined sub-playbook inputs

Answer: D

Explanation:

Question: 139

What are two of the actions available on the Version History tab of a content pack in the marketplace? (Choose two.)

A. Download content for ofline installation

B. Uninstall content pack

C. Update to x version

D. Revert to x version

Answer: C, D

Explanation:

Question: 140

Which of these would be the most operationally efficient repository for moving XSOAR custom content from a development server to a production environment?

A. A content repository specified in the Marketplace

B. Remote git repository specified in the dev-prod configuration parameters

C. The development server's default repository

D. Cortex XSOAR public content repository

Answer: B

Explanation:

Question: 141

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

Explanation:

Question: 142

Which of the following is a basic setting that can be configured in an automation?

A. Summary
B. Compiler
C. Schedule
D. Run On

Answer: C

Explanation:

Question: 143

Which of the following are valid methods to contribute custom content? (Choose three.)

A. Submit content directly through feature requests
B. Private GitHub repository submission for premium content
C. A Github pull request on the public XSOAR Content Repository
D. Using the marketplace interface to upload the content
E. Using the content submission tool on live.paloaltonetworks.com

Answer: C, D, E

Explanation:

Question: 144

What does the outgoing mapper support?

A. Mirroring
B. Classification
C. Dynamic fields

D. Pre-processing

Answer: D

Explanation:
Reference: https://xsoar.pan.dev/docs/incidents/incident-classification-mapping

Question: 145

What happens if both a Classifier and Incident Type are configured in an integration instance's settings?

A. The administrator will receive a notification that there is both a Classifier and Incident Type set for that integration instance.

B. The Incident Type will be ignored, and incoming incidents will be classified according to the Classifier.

C. The Classifier will be ignored, and incoming incidents will be classified according to the Incident Type.

D. Both the Classifier and Incident Type will classify incoming incidents.

Answer: D

Explanation:

Question: 146

You can customize most aspects of the incident layout, including which three of the following? (Choose three.)

A. Which users have permissions to view the tabs

B. Which roles have permissions to view the tabs

C. Which dashboard settings are applied

D. The information and how is it displayed

E. Which tabs appear and in which order

Answer: C, D, E

Question: 147

Who is permitted to create and submit content to the Marketplace?

A. Only users with a valid Github account

B. Any user who has signed up through the dev portal

C. Any user who has a live.paloaltonetworks.com account

D. All users with the correct XSOAR Role and Permissions

Answer: D

Explanation:

Question: 148

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: D

Explanation:

Question: 149

Newly created subplaybooks do not have any inputs, or outputs. What is necessary to make them functional? (Choose two.)

A. Define input key in the subplaybook task. Map context values to pull from parent playbook.

B. The output of the previous task automatically becomes the input of the subplaybook.

C. Map inputs and outputs to the parent playbook and the subplaybook will use the same values.

D. Open the subplaybook and add inputs or outputs in the Playbook triggered task.

Answer: A, D

Explanation:

Question: 150

A Cortex XSOAR Administrator is tasked with building a button for an analyst in order for the analyst to be assigned to the incident as an owner. What is the process?

A. Edit the incident layout to add a new button that calls the AssignAnalystToIncident automation with no argument

B. Edit the incident layout to add a new button that calls the AssignToMeButton automation with argument assignBy={me}

C. Edit the incident layout to add a new button that calls the AssignAnalystToIncident automation with argument owner={me}

D. Edit the incident layout to add a new button that calls the AssignAnalystToIncident automation with argument assignBy=current

Answer: C

Explanation:

Question: 151

Which field type should be used to hold more than 60,000 characters of unformatted text?

A. Short Text

B. HTML

C. Long Text

D. Markdown

Answer: C

Explanation:

Question: 152

In order to automatically run a playbook on the indicators fetched by an integration, what would an XSOAR Administrator setup?

A. Cron job

B. Time triggered job

C. Feed triggered job

D. REST API job

Answer: C

Explanation:

Reference: https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.5/Cortex-XSOAR-Administrator-Guide/Create-Indicator-Extract-Rules-for-a-Playbook-Task

Question: 153

Which two functions in XSOAR are incident types used for? (Choose two.)

A. To run dedicated playbooks for different event types

B. To classify events ingested from various sources into the relevant types

C. To classify indicators extracted in XSOAR incidents to their respective types

D. To facilitate role based access to XSOAR incidents

Answer: B, C

Explanation:

Question: 154

When creating an incident layout section, it is best to place long field values within which of the following?

A. Section headers

B. Rows

C. Canvas

D. Cards

Answer: B

Explanation:

Question: 155

The default expiration method for non-feed indicators is either to never expire or to expire after a specific period of time. How frequently does XSOAR check tor newly expired indicators?

A. Every 24 hours
B. Every 5 minutes
C. Every 8 hours
D. Every 1 hour

Answer: D

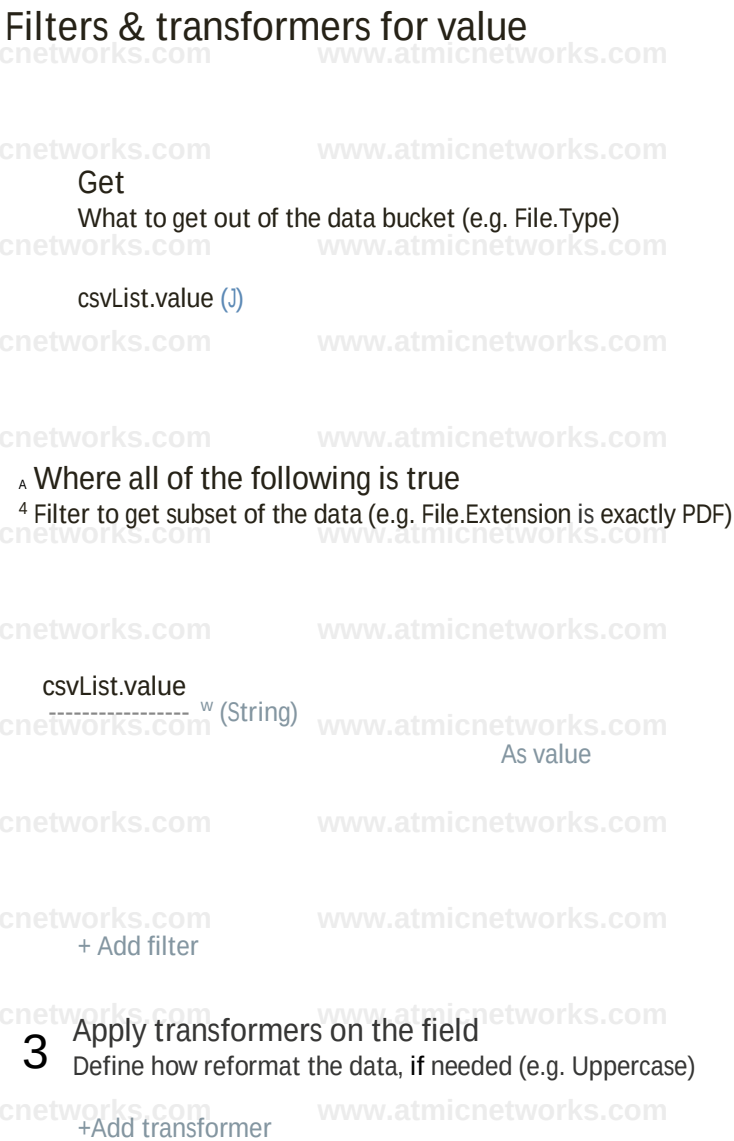
Explanation:

Reference: https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.5/Cortex-XSOAR-Threat-Intel-Management-Guide/Indicator-Expiration

Question: 156

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