Number: PCSAE
Passing Score: 800
Time Limit: 120
File Version: 5.0

Exam Code: PCSAE
Exam Name: Palo Alto Networks Certified Security Automation Engineer

Exam A

QUESTION 1
What is the default configuration for indicator auto-extraction when incidents are created?

A. Inline
B. Inband
C. None
D. Out of band

Correct Answer: A
Section:

QUESTION 2
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

Correct Answer: C
Section:

QUESTION 3
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

Correct Answer: D
Section:

QUESTION 4
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

Correct Answer: B
Section:

QUESTION 5
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

Correct Answer: A
Section:

QUESTION 6
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

Correct Answer: D
Section:

QUESTION 7
What assigns newly ingested event attributes to incident fields?

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

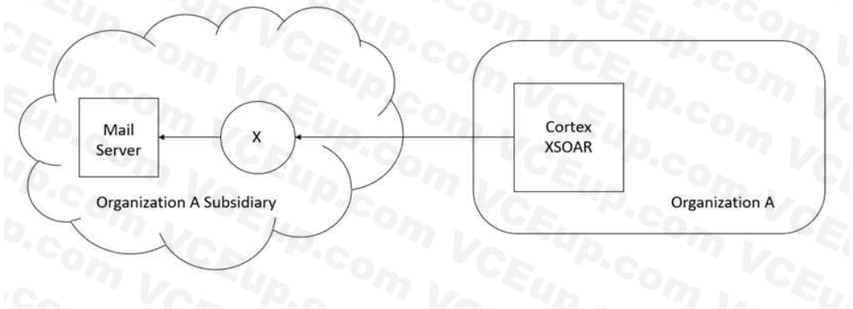
Correct Answer: C
Section:

QUESTION 8
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

Correct Answer: C
Section:

QUESTION 9
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.

Correct Answer: D
Section:

QUESTION 10
Which component can be part of a load balancing group?

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

Correct Answer: C
Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/5-5/cortex-xsoaradmin/engines/understand- demisto-engines.html

QUESTION 11
Which method accesses a field called 'User Mail' in a playbook?

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

Correct Answer: A
Section:

QUESTION 12
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

Correct Answer: D
Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-1/cortex-xsoaradmin/dashboards/share- a-dashboard.html

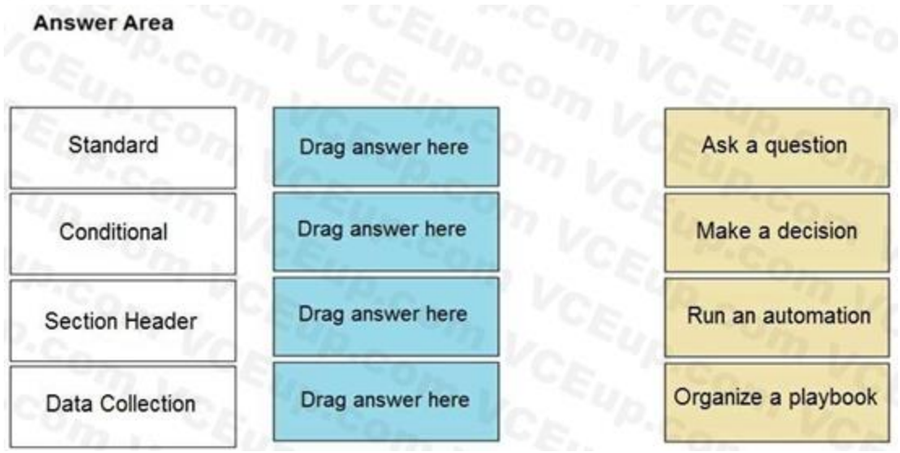
QUESTION 13
Which two methods will allow data to be saved in incident fields within a playbook? (Choose two.)

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

Correct Answer: B, C
Section:

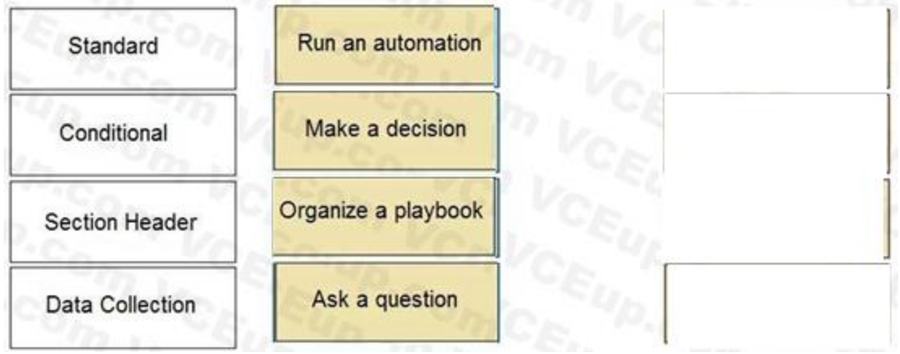
QUESTION 14
DRAG DROP
Match the action with the most appropriate playbook task type.

Select and Place:



Correct Answer:

Answer Area



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

QUESTION 15
Which built-in automation/command cab be used to change an incident's type?

A. setIncident
B. Set
C. GetFieldsByIncidentType
D. modifyIncidentFields

Correct Answer: A
Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/5-5/cortex-xsoaradmin/incidents/incidents- management/incident-fields/field-trigger-scripts.html

QUESTION 16
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

Correct Answer: B
Section:

QUESTION 17
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

Correct Answer: A, B
Section:

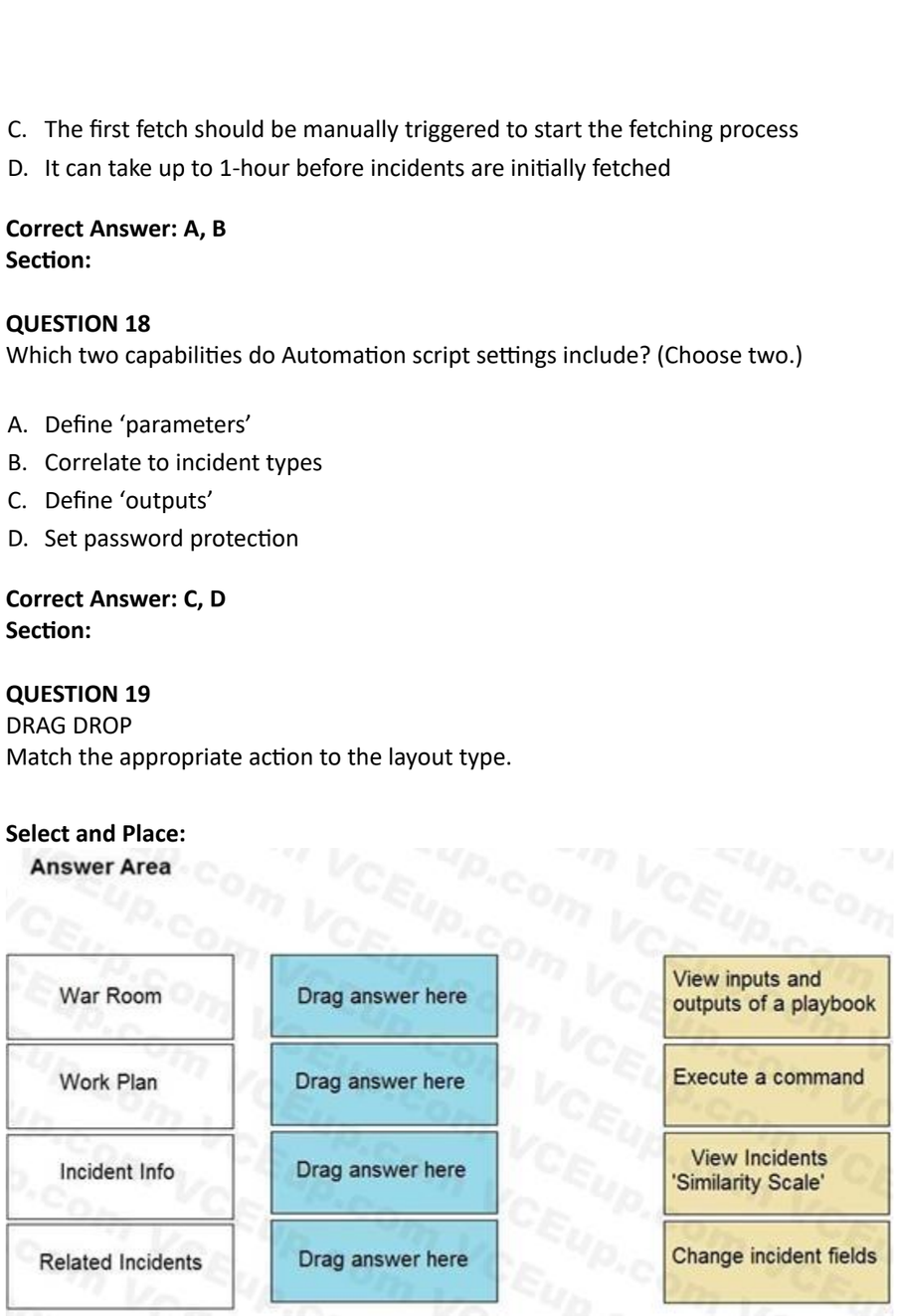
QUESTION 18
Which two capabilities do Automation script settings include? (Choose two.)

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

Correct Answer: C, D
Section:

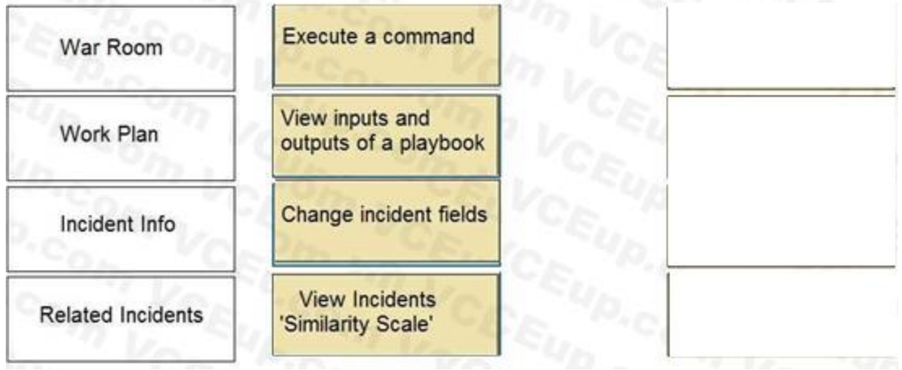
QUESTION 19
DRAG DROP
Match the appropriate action to the layout type.

Select and Place:



Correct Answer:

Answer Area



Section:
Explanation:

QUESTION 20
What is a primary use case of data collection tasks?

A. To allow multi-

Correct Answer: A
Section:

QUESTION 21

A. To automate tasks such as parsing a file or enriching indicators
B. To generate new widgets for a dashboard
C. To determine different paths in a playbook

Correct Answer: A
Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/5-5/cortex-xsoaradmin/playbooks/playbook- tasks/communication-tasks/create-a-data-collection-task.html

QUESTION 22
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

Correct Answer: B, C, D
Section:

QUESTION 23
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

Correct Answer: C, D
Section:

QUESTION 24
How long is the trial period for paid content packs?

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

Correct Answer: A
Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoaradmin/marketplace/ marketplace-subscriptions.html

QUESTION 25
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

Correct Answer: B
Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/5-5/cortex-xsoaradmin/playbooks/extend- context/extend-context-using-the-command-line.html

QUESTION 26
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

Correct Answer: C
Section:

QUESTION 27
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

Correct Answer: A, D
Section:

QUESTION 28
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

Correct Answer: B
Section:

QUESTION 29
Which investigation element is best suited for collaboration among users?

A. Work Plan
B. Related Incidents
C. War Room
D. Context Data

Correct Answer: D
Section:
Explanation:
Reference: https://blog.paloaltonetworks.com/2020/01/cortex-security-operations/

QUESTION 30
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

Correct Answer: B, C, D
Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoaradmin/marketplace/ marketplace-overview/content-packs-support-types.html

QUESTION 31
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

Correct Answer: C, D, E
Section:
Explanation:
Reference: https://www.paloguard.com/GlobalProtect.asp

QUESTION 32
Which two components have their own context data? (Choose two.)

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

Correct Answer: A, D
Section:

QUESTION 33
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

Correct Answer: A, C
Section:
Explanation:
Reference: https://xsoar.pan.dev/docs/integrations/context-andoutputs#:~:text=The%20main%20use%20of% 20the,the%20Context%20and%20uses%20it.

QUESTION 34
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

Correct Answer: B, D
Section:

QUESTION 35
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

Correct Answer: B
Section:
Explanation:
https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.6/Cortex-XSOAR-Administrator-Guide/Customize-Incident-Layouts

QUESTION 36
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

Correct Answer: A, D
Section:

QUESTION 37
By default, which components does an XSOAR implementation include?

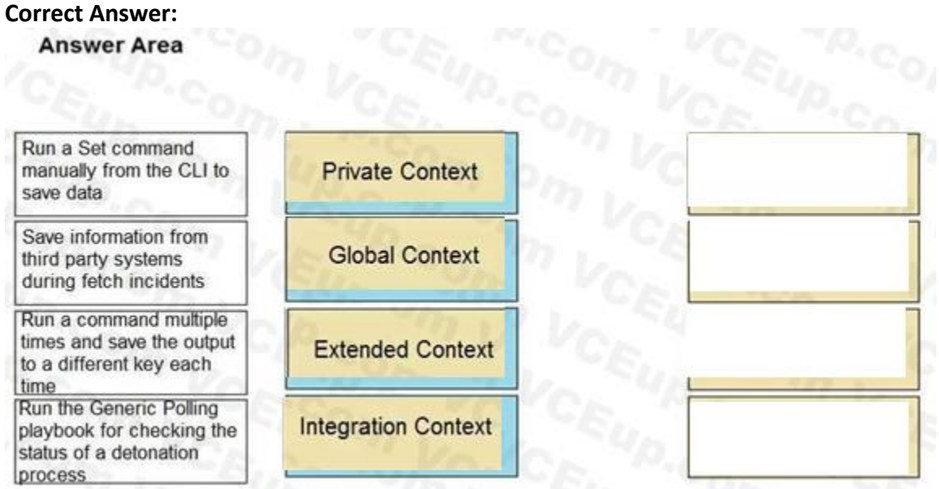
A. XSOAR server, XSOAR engine
B. Application server, distributed DB server
C. Application server, distributed DB server, Backup server
D. All in one server

Correct Answer: B
Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoaradmin/installation/install- demisto-on-a-physical-or-virtual-server.html

QUESTION 38
DRAG DROP
Match the operations with the appropriate context.

Select and Place:

Correct Answer:



Section:
Explanation:

QUESTION 39
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

Correct Answer: A, B, E
Section:

QUESTION 40
What can be added to offload integration instance processing from the main server?

A. Database node
B. Application server
C. Engine
D. Development server

Correct Answer: A
Section:

QUESTION 41
Which XSOAR architecture would be recommended for Managed Security Service Providers (MSSP)?

A. Multi-region
B. Dev-Prod
C. Multi-tenant
D. Distributed database

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

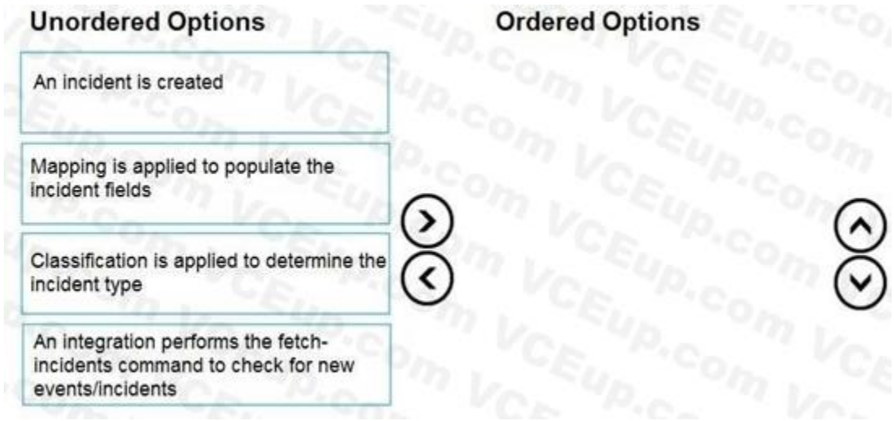
QUESTION 42
An incident field is created having the display name as Source_IP. How can the field be accessed?

A. ${incident.sourceip}
B. ${incident.Source_IP}
C. ${incident.srcip}
D. ${incident.Source IP}

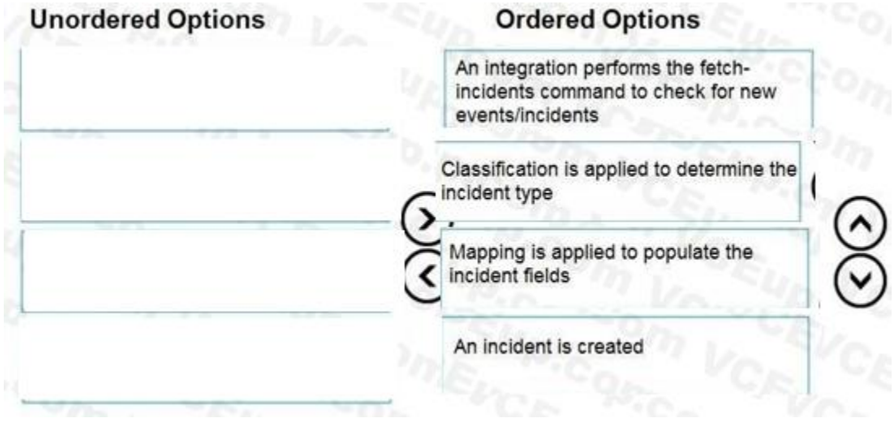
Correct Answer: C
Section:

QUESTION 43
DRAG DROP
Arrange these steps in the order that they occur during an incident fetch.

Select and Place:



Correct Answer:



Section:
Explanation:
Integration performs
Classification is applied
Mapping is applied
Incident is created (before incident creation it should be also pre-process rule step)

QUESTION 44
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”

Correct Answer: D
Section:

QUESTION 45
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

Correct Answer: A
Section:
Explanation:
Reference: https://xsoar.pan.dev/docs/integrations/test-playbooks

QUESTION 46
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

Correct Answer: C
Section:

QUESTION 47
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

Correct Answer: A, D
Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/5-5/cortex-xsoar-admin/cortexxsoar-overview/how-to-search-in-cortex-xsoar.html

QUESTION 48
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

Correct Answer: C
Section:

QUESTION 49
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

Correct Answer: D, E
Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/cortex/cortexxsoar/6-0/ cortex-xsoar-admin/cortex-xsoar-admin.pdf/cortex-xsoar-admin.pdf

QUESTION 50
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.

Correct Answer: A
Section:

QUESTION 51
What is the default landing page for a new user in XSOAR?

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

Correct Answer: A
Section:

QUESTION 52
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

Correct Answer: C
Section:

QUESTION 53
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

Correct Answer: D
Section:

QUESTION 54
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.

Correct Answer: D
Section:

QUESTION 55
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"

Correct Answer: A
Section:

QUESTION 56
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.

Correct Answer: D
Section:
Explanation:
Reference: https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.6/Cortex-XSOARAdministrator-Guide/Configure-the-HTML-Field

QUESTION 57
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

Correct Answer: A, B, D
Section:

QUESTION 58
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

Correct Answer: C
Section:

QUESTION 59
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

Correct Answer: A
Section:

QUESTION 60
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++

Correct Answer: B
Section:
Explanation:
Reference: https://www.paloaltonetworks.com/resources/datasheets/cortex-xsoar-overview

QUESTION 61
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

Correct Answer: B
Section:

QUESTION 62
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

Correct Answer: C
Section:

QUESTION 63
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

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

QUESTION 64

Context

Input

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

A. 1E56733826E5035233A097FCEA2046AF96EC616C
B. E6EF5142E2553C1E442A0FFAC07636EAC61E6EDD

C. 8D193FA162A305E4859BA8C45F5121F7265E3ABB
D. e6ef5142e2553c1e442a0ffac07636eac61e6edd

Correct Answer: D
Section:

QUESTION 65
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

Correct Answer: A
Section:
Explanation:
Reference: https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.6/Cortex-XSOARAdministrator-Guide/Customize-Incident-Layouts

QUESTION 66
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.

Correct Answer: B
Section:
Explanation:
Reference: https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.5/Cortex-XSOARAdministrator-Guide/Create-the-Read-Only-Dashboard

QUESTION 67
Which content type cannot be managed using remote repositories?

A. Lists
B. Jobs
C. Pre-processing rules
D. Exclusion List

Correct Answer: A
Section:

QUESTION 68
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.

Correct Answer: B
Section:
Explanation:
Reference: https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.6/Cortex-XSOARAdministrator-Guide/Incident-Management

QUESTION 69
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

Correct Answer: D
Section:

QUESTION 70
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

Correct Answer: C
Section:

QUESTION 71
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.

Correct Answer: D
Section:

QUESTION 72
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.

Correct Answer: C
Section:

QUESTION 73
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.

Correct Answer: B
Section:

QUESTION 74
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

Correct Answer: B
Section:

QUESTION 75
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.

Correct Answer: B
Section:

QUESTION 76
At what stage during the incident lifecycle is an incident type assigned?

A. Pre-processing
B. Incident creation
C. Classification
D. Playbook execution

Correct Answer: C
Section:

QUESTION 77
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

Correct Answer: B
Section:

QUESTION 78
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

Correct Answer: D
Section:

QUESTION 79
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

Correct Answer: A, B, C
Section:

QUESTION 80
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.

Correct Answer: D
Section:

QUESTION 81
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

Correct Answer: B
Section:

QUESTION 82
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

Correct Answer: D
Section:

QUESTION 83
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.

Correct Answer: A, D
Section:

QUESTION 84
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

Correct Answer: C
Section: