PCSAE.VCEplus.premium.exam.84q

Number: PCSAE
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

PCSAE

Palo Alto Networks Certified Security Automation Engineer

Version 1.0

Exam A

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
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]}`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3

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: (none)
Explanation

Explanation/Reference:
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}`

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
DRAG DROP

Match the action with the most appropriate playbook task type.

Select and Place:

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:
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`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
DRAG DROP

Match the appropriate action to the layout type.

Select and Place:

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13 What is a primary use case of data collection tasks?

A. To allow multi-question 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

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 stopTimerD. 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: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16 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: (none)
Explanation

Explanation/Reference:
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`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19 An engineer would like to present a trend using widgets to compare to a previous week's data.

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: AD
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21 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: (none)
Explanation

Explanation/Reference:
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

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: CDE
Section: (none)

Explanation
Explanation/Reference:
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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: BD

Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

Select and Place:
Correct Answer:

Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32 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: (none)
Explanation

Explanation/Reference:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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}`

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
DRAG DROP

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

Select and Place:

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:

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"`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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 post-processing
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: A
Section: (none)
Explanation

Explanation/Reference:

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`

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
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`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41 Whar 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
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
Correct Answer: BC

Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51 When uploading content, which two options could the upload include? (Choose two.)

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

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'

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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`

Correct Answer: AC
Section: (none)
Explanation

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

QUESTION 56
DRAG DROP

Match the corresponding action with the appropriate playbook tasks.

Select and Place:

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:
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”`

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: BD
Section: (none)
Explanation

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:

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 question to a person or team

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:
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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

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 serverD. 1 application server, 2 main DBs, 1 node server

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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`

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

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 notC. Labels can be used in queries and fields cannot
D. Labels are indexed in the database and fields are not

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73 What is the default task type when creating an empty task?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75 In which two options can an automation script be executed? (Choose two.)

A. Engine
B. Integration
C. War room
D. Playbook

Correct Answer: CD

Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://xsoar.pan.dev/docs/tutorials/tut-integration-ui

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
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