# PaloAltoNetworks.XSOAR-Engineer.v2026-05-25.q100

| | |
|---|---|
| **Exam Code:** | XSOAR-Engineer |
| **Exam Name:** | Palo Alto Networks XSOAR Engineer |
| **Certification Provider:** | Palo Alto Networks |
| **Free Question Number:** | 100 |
| **Version:** | v2026-05-25 |
| **# of views:** | 105 |
| **# of Questions views:** | 1289 |
| https://www.freecram.net/torrent/PaloAltoNetworks.XSOAR-Engineer.v2026-05-25.q100.html | |

**NEW QUESTION: 1**
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 verdict: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 reputation:Malicious sourcetimestamp:="30 days ago"
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 2**
The code snippet below is from the fetch command of an integration instance configured to run on the server.
demisto.debug(f"(len(incidents)} events fetched")
Where is the output from the snippet located when the instance runs an automatic fetch?.
**A.** Incident label.
**B.** Platform Log bundle.
**C.** Integration Logs table.
**D.** War Room entry.
**Answer: (SHOW ANSWER)**
Integration debug messages (generated using demisto.debug) are stored in the Integration Logs table, not in the War Room or incident labels.
The Admin Guide states that all logs generated by integration code are visible through the Integration Logs section for troubleshooting.

**NEW QUESTION: 3**
Given an incident with three files, how could the name of the second file be referenced?
**A.** ${File.[1].Name}
**B.** ${Files.Name.[2]}
**C.** ${Files.[2].Name}
**D.** ${File.Name.[1]}

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 4**
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.** By running the command !MarkAsEvidence
**C.** From the Notes section (mark as entry icon)
**D.** Manually from the playbook task (mark as entry icon)
**E.** Automatically from playbook tasks when the option is selected on the Advanced tab
**Answer: (SHOW ANSWER)**

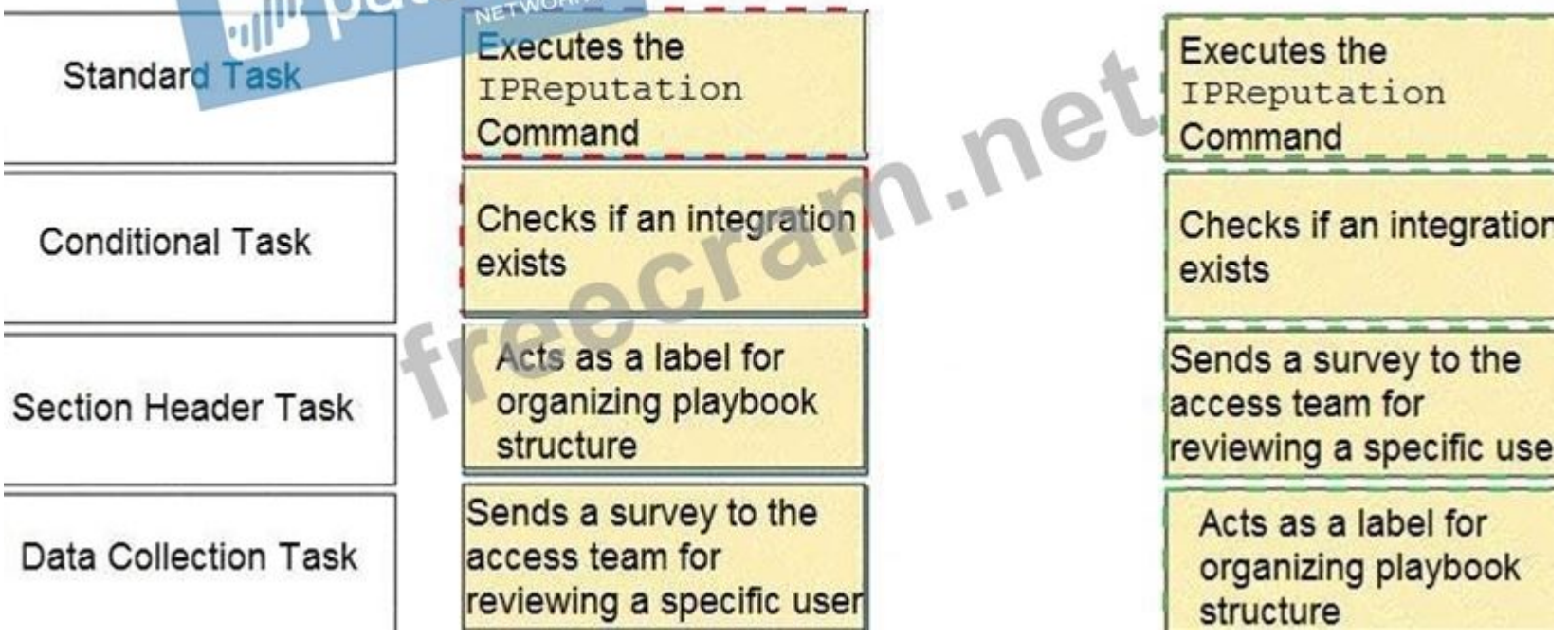
**NEW QUESTION: 5**
Which two features can be used together to automatically execute a search on a remote SIEM for extracted IP Indicators? (Choose two.).
**A.** Reputation script.
**B.** Enhancement script.
**C.** Integration command.
**D.** Feed-triggered job.
**Answer: (SHOW ANSWER)**
XSOAR automates indicator-driven actions through various trigger types. To execute a search automatically on a remote SIEM when new IP indicators are extracted, two components are needed:
* Feed-triggered job (D)- The Admin Guide explains that jobs can be triggered when a feed updates.
When new indicators are fetched, a feed-triggered job can automatically start a playbook.
* Integration command (C)- The playbook executed by the job can call SIEM integration commands (such as siem-search, query-log, or custom search commands). These commands send API queries to the remote SIEM and return event/log results.
Reputation scripts (option A) evaluate or enrich indicators but do not execute SIEM searches. Enhancement scripts (option B) add contextual data to indicators but not remote searches.
Thus, the correct pair supported by XSOAR automation architecture is:
#Integration Commandto perform the SIEM query
+
#Feed-Triggered Jobto automatically initiate the action when new IP indicators appear.
This reflects XSOAR's feed-driven automation workflow.

**NEW QUESTION: 6**
Match the corresponding action with the appropriate playbook tasks.

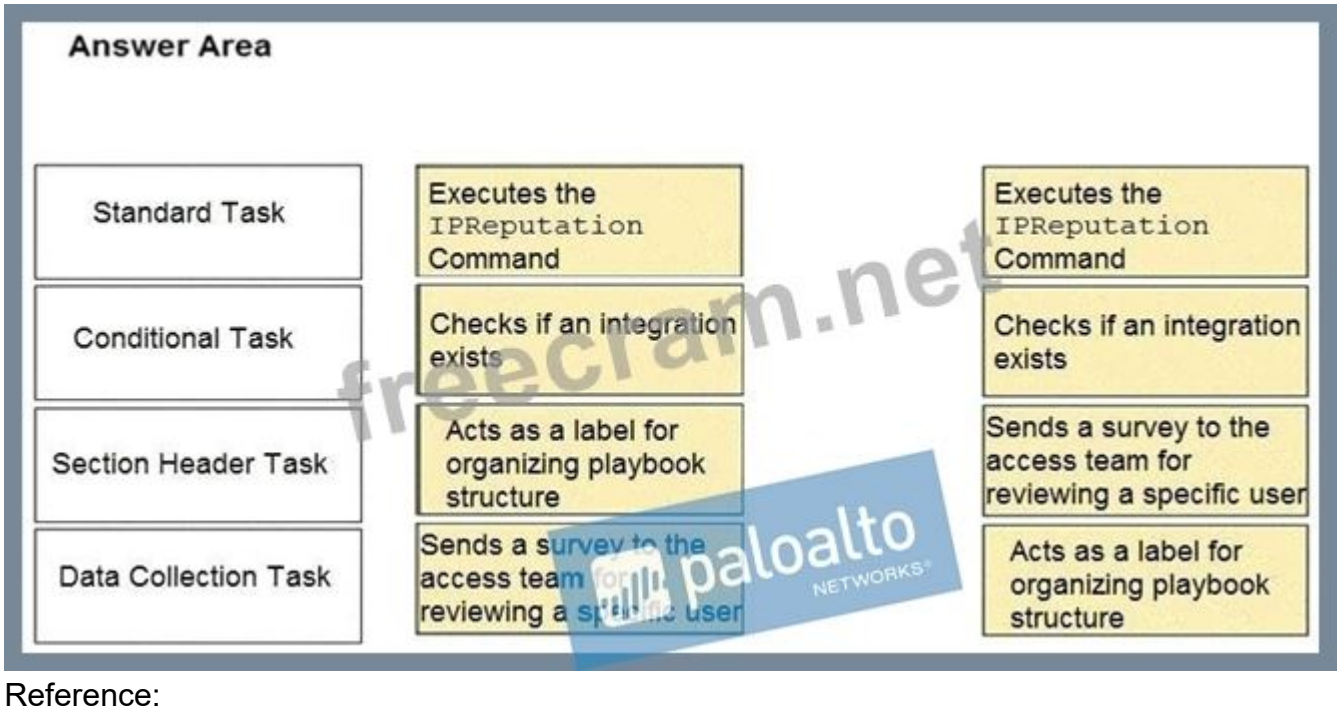
Answer Area


**Answer:**

Answer Area




paloalto NETWORKS
freecram.net




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

**NEW QUESTION: 7**
By default, automation written in which language will be executed in a Docker container?
**A.** Go
**B.** Perl
**C.** Python
**D.** JavaScript
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 8**
Which two functions in XSOAR are incident types used for? (Choose two.)
**A.** To classify indicators extracted in XSOAR incidents to their respective types
**B.** To run dedicated playbooks for different event types
**C.** To facilitate role based access to XSOAR incidents
**D.** To classify events ingested from various sources into the relevant types
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 9**
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: (SHOW ANSWER)**
Reference: https://xsoar.pan.dev/docs/integrations/fetching-incidents

**NEW QUESTION: 10**

A large number of incidents were deleted by mistake.
Which two architecture components can be used to recover the lost data? (Choose two.)

Freecram.net

**A.** Live backup
**B.** Engine
**C.** Distributed database
**D.** Local backup
**Answer: (SHOW ANSWER)**
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

**NEW QUESTION: 11**
Which field type provides an interactive and editable display of table-based data?
**A.** Grid (table)
**B.** HTML
**C.** Markdown
**D.** Multi Select
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 12**
An incident has been created in the following state:
There is no playbook attached.
The War Room is available, but no commands have been run yet.
What is the status of the incident?.
**A.** Active.
**B.** Pending.
**C.** Waiting.
**D.** In-progress.
**Answer: (SHOW ANSWER)**
The XSOAR Incident State Model defines several system statuses: Pending, Active, In-Progress, Done, and Closed. When an incident is newly created and has not yet had a playbook assigned or started-and no analyst actions (such as commands or work plan steps) have been taken-it remains in the Pending state.
Pending indicates that the incident exists in the system but has not yet begun active investigation or automated processing. The Admin Guide clarifies that an incident becomes Active only when a playbook starts or an analyst interacts with it. In-Progress is a manually applied user state indicating active human processing.
Waiting is used for blocked or paused tasks but does not apply at initial creation.
Because the War Room is available but unused, and no automation has begun, the incident fits the definition of Pending exactly. Once a playbook were attached or a command were executed, the state would transition to Active.
Therefore, the documented correct answer is B: Pending.

**NEW QUESTION: 13**
In a Dev/Prod deployment model, what is available only in the development tenant?.
**A.** Marketplace.
**B.** Content Repository page.
**C.** Custom integration instances.
**D.** "Export all custom content" feature.
**Answer: (SHOW ANSWER)**
In Cortex XSOAR's documented Dev/Prod deployment model, thedevelopment tenantis designed to be the workspace where engineers create, modify, test, and validate content before promoting it into production. As part of this workflow, the development tenant includes the"Export all custom content"feature, which generates a structured content bundle containing custom playbooks, integrations, fields, layouts, lists, and other artifacts. This bundle is then imported into the production tenant to ensure controlled, versioned, and tested promotion of content.
The Admin Guide highlights that this export capability isrestricted to the development environmentto preserve the integrity and stability of the production tenant. Production systems are intentionally limited, allowing only the import (not export) of custom content to prevent accidental overwriting, drift, or unintended modifications.
Marketplace access (A) exists in both tenants. Custom integration instances (C) can be created in either tenant. The Content Repository page (B) is also available across both environments.
Therefore, the only feature exclusive to the development tenant isD: "Export all custom content."This ensures a safe, repeatable Dev#Prod promotion model aligned with enterprise change-control requirements.

**NEW QUESTION: 14**
A playbook needs to dynamically add an email sender's address to a Cortex XSOAR list named "BlockedSenders_Email."
Which built-in command should be used within the playbook to add this email address to the specified list?.
**A.** !addToList listName="BlockedSenders_Email" listData="<email_address>".
**B.** !appendToListContext listPath="BlockedSenders Email" data="<email_address>".
**C.** !setIncident list.BlockedSenders_Emai1="<email_address>".
**D.** !createListItem listName="BlockedSenders_Email" itemValue="<email_address>".
**Answer: (SHOW ANSWER)**
XSOAR's built-inLists Servicesupports operations such as creating, updating, and appending items to lists using automation commands. The correct command for appending a value to an existing list is!addToList, which inserts the new string (in this case an email address) into the list array stored within the XSOAR Lists infrastructure.
The Admin Guide describes!addToListas the intended mechanism to add new elements to a named list while automatically handling JSON structure and avoiding duplication errors.
Option B, !appendToListContext, modifiescontext data, not persistent platform lists-therefore it will not update the BlockedSenders list. Option C misuses !setIncident, which updates incident fields only, not system lists. Option D, !createListItem, is used when an integration or automation script exposes a "create item" action, not for native XSOAR lists.
Thus, the correct and documented method of adding an email value to a persistent XSOAR list is!addToList, making optionAthe accurate choice.

**NEW QUESTION: 15**
At what stage during the incident lifecycle is an incident type assigned?
**A.** Playbook execution
**B.** Classification
**C.** Pre-processing
**D.** Incident creation
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 16**
Based on the image below, what is the output when "Test" is clicked?.


**A.** Blue.
**B.** Orange.
**C.** Yellow.
**D.** Red.
**Answer: D (LEAVE A REPLY)**

**Valid XSOAR-Engineer Dumps** shared by EduDump.com for Helping Passing XSOAR-Engineer Exam! EduDump.com now offer the **newest XSOAR-Engineer exam dumps**, the EduDump.com XSOAR-Engineer exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com XSOAR-Engineer dumps with Test Engine here: https://www.edudump.com/exams/Palo-Alto-Networks/XSOAR-Engineer/premium/ (**206** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

**NEW QUESTION: 17**
When using the playbook debugger, what may be the cause of a starred incident missing from the Test Data selections?.
**A.** Closed incidents are not visible in the debugger.

**B.** Starred incidents are not visible in the debugger.
**C.** The incident type is set incorrectly.
**D.** The incident has been restricted.
**Answer: (SHOW ANSWER)**
The XSOAR Playbook Debugger documentation states that only open incidents can be selected as Test Data.
Closed incidents do not appear in the debugger's incident selection list.
Starring an incident does not override this limitation; if it is closed, it will not appear.

**NEW QUESTION: 18**
Threat Intel search queries can be shared with which of the following? (Select 1)
**A.** Users outside XSOAR via email invite
**B.** Other organizations via the Marketplace
**C.** Users defined in the platform (email or username)
**D.** Roles defined in the platform
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 19**
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: (SHOW ANSWER)**
Reference: https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.6/Cortex-XSOAR-Administrator- Guide/Configure-the-HTML-Field

**NEW QUESTION: 20**
In which two options can an automation script be executed? (Choose two.)
**A.** Engine
**B.** Integration
**C.** War room
**D.** Playbook
**Answer: (SHOW ANSWER)**
Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar-admin/playbooks/ automations.html

**NEW QUESTION: 21**
What is the correct way to install different engines on the same Ubuntu machine for a Dev/Prod setup?.
**A.** Use Shell installer and create a custom JSON configuration file.
**B.** Use different docker instances in the machine to install each engine.

**C.** Use Shell installer with "Allow running multiple engines.".
**D.** Create a DEB installer and modify in the JSON configuration.
**Answer: (SHOW ANSWER)**
The XSOAR Engine Installation Guide explains that a single Linux host can run multiple engines using the Shell Installer with the "Allow running multiple engines" option enabled. This method is specifically intended for Dev/Prod, HA, and multi-tenant scenarios. When this option is selected, the installer configures separate engine services and directories, preventing conflicts in ports, logs, or runtime environments.
Using Docker containers (option B) is not an officially supported or documented deployment method for running multiple XSOAR engines. Creating custom JSON or DEB installers (options A and D) applies to advanced engine deployments but doesnotenable multiple engines on the same host.
The Admin Guide explicitly states that the Shell Installer includes a built-in prompt allowing multiple engines to coexist safely, and this is the approved and supported mechanism provided by Palo Alto Networks.
Therefore, the correct answer isC.

**NEW QUESTION: 22**
A SOC team must send a notification email to specific teams based on the severity of an incident.
Which feature will accomplish this task each time the severity escalates?.
**A.** SLA script.
**B.** Post-processing rule.
**C.** Field-change trigger script.
**D.** Server config.
**Answer: (SHOW ANSWER)**
The XSOAR Admin Guide specifies that field-change trigger scripts allow automations to run whenever a designated incident field changes. Severity is a standard incident field, and when its value increases due to analyst action, a playbook, enrichment script, or correlation event, a field-change trigger can automatically run a script to notify teams.
Post-processing rules only run after an incident closes, making them unsuitable for real-time severity escalation alerts. SLA scripts respond to timer conditions, not field changes, and are used for SLA violations or deadline tracking. Server configuration does not provide automation behavior tied to field modifications.
Field-change triggers are explicitly documented as the mechanism to automate workflows for "reacting to changes in incident fields such as owner, severity, status, or custom fields." When severity is updated, XSOAR evaluates matching triggers and runs the associated automation immediately.
Thus, only a field-change trigger script can reliably detect a severity escalation and execute a notification action the moment the field changes, making option C the correct and documented solution.

**NEW QUESTION: 23**
What are two primary uses of standard tasks? (Choose two.)
**A.** To generate new widgets for a dashboard
**B.** To create an incident or escalate an existing incident
**C.** To highlight different paths in a playbook
**D.** To automate tasks such as parsing a file or enriching indicators
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 24**
Inside the Incidents table view, which actions can be performed on the selected incidents? (Choose two.)
**A.** Run Command for all selected incidents having Active status
**B.** Run Command, Export, and Close and Delete for all selected incidents regardless of their status
**C.** Assign, Edit, and Mark as Duplicate for all selected incidents regardless of their status
**D.** Export incidents as JSON and change incident status
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 25**
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 custom integration will not be maintained and updated by XSOAR content team
**B.** The commands must return a proper result to the war room for the analysts to understand
**C.** The integrations are locked and cannot be edited with additional commands
**D.** The code may not be written to XSOAR standards
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 26**
Previous playbook tasks have built out the context in the image below.

paloalto
freecram.net

When specifying ${User.Name} as an input for a sub playbook task which has the default loop configuration, how many times will the sub-playbook be executed?.

**A.** 4.

**B.** 1.

**C.** 3.

**D.** 0.

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 27**

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

**A.** Inputs are data pieces that are present in the task

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

**C.** Inputs are data pieces that are present in the playbook

**D.** Inputs are the data fields parsed by the Classifier

**E.** Outputs are used as incident trigger for playbook

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 28**

Which feature is used to convert event data values into incident fields when an integration fetches an event?.

**A.** Classification.

**B.** Mapping.

**C.** Field configuration.

**D.** Layout configuration.

**Answer: (SHOW ANSWER)**

XSOAR's ingestion pipeline defines a strict order in which raw fetched data is processed, and the Admin Guide explains that Classification determines the incident type based on incoming fields, while Mapping performs the actual transformation of event data into structured incident fields. Mapping profiles define how each field from the integration's raw JSON (for example, source_ip, username, alert_id) is converted into standard or custom incident fields.

The Mapping Editor allows administrators to select specific fields from the incoming event data and bind them to incident fields used throughout playbooks, layouts, and reports. This ensures normalization of data and consistent schema usage across the SOC.

The documentation makes clear that Mapping is responsible for populating incident field values, whereas Classification only chooses the incident type. Field configuration defines field metadata but does not map values. Layout configuration controls visual presentation only and does not populate fields.

Thus, option B (Mapping) is the function that converts event data into incident field values and is the correct answer according to the ingestion architecture documented in the XSOAR Admin Guide.

**NEW QUESTION: 29**

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

**NEW QUESTION: 30**
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?
Freecram.net
**A.** Add the !startinvestigation automation to the beginning of the playbook
**B.** Select 'Run playbook automatically' from the integration settings
**C.** Select 'Run playbook automatically' from the incident type settings
**D.** Add the playbook to the integration's settings
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 31**
A breakpoint is added to a saved playbook to ensure that it pauses before running the task "ad-delete-user." However, it is later discovered that an Active Directory account was deleted by this playbook, and the playbook did not pause at the breakpoint.
What is the cause of this issue?.
**A.** The playbook does not stop at the breakpoint when run from an incident.
**B.** The task was not set to "skip.".
**C.** The task was not configured to override input.
**D.** The playbook was not set to "quiet mode.".
**Answer: (SHOW ANSWER)**
The XSOAR Playbook Debugger documentation states that breakpoints only apply when the playbook is run in Debug mode, not when an incident triggers the playbook normally.
Running from an incident executes the playbook without debugger controls, so breakpoints are ignored- leading to the deletion task running normally.

**Valid XSOAR-Engineer Dumps** shared by EduDump.com for Helping Passing XSOAR-Engineer Exam! EduDump.com now offer the **newest XSOAR-Engineer exam dumps**, the EduDump.com XSOAR-Engineer exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com XSOAR-Engineer dumps with Test Engine here: https://www.edudump.com/exams/Palo-Alto-Networks/XSOAR-Engineer/premium/ (**206** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

**NEW QUESTION: 32**
A playbook task is set up to run an integration command that takes no input and which outputs information to the context. The integration has several instances configured.
Which action will ensure the integration command only runs once?.

**A.** Specify the using- parameter to target a specific integration instance to run.
**B.** Click on Advanced Options # Limits to specify the minimum / maximum run limits for a command.
**C.** Click on Performance # Run Limits to specify the maximum run count before the task exits.
**D.** Specify the runlimit= parameter to limit the number of times a specific command will run.
**Answer: (SHOW ANSWER)**
When an integration has multiple instances configured, XSOAR's playbook engine attempts to execute the command once per available instance unless directed otherwise. This behavior is described in the Playbook Task Execution Model within the Admin Guide. To prevent multiple executions, the engineer must explicitly specify which integration instance the command should use. Playbook tasks include a "Using" drop-down (the "using=" parameter in CLI form), which binds the task to a particular instance. Once set, XSOAR will run the command only on that selected instance, ensuring it does not loop through all available instances.
The limits settings in Advanced Options or Performance sections control retry behavior or error handling, not instance selection. The "runlimit" parameter is used for limiting iterative loops or repeated command execution inside playbooks, not for controlling multi-instance execution.
Thus, to ensure the integration command executes only once, the engineer must specify the using=instance_name, making option A the correct answer.

**NEW QUESTION: 33**
What is the default configuration for indicator auto-extraction when incidents are created?
**A.** Inline
**B.** None
**C.** Inband
**D.** Out of band
**Answer: (SHOW ANSWER)**

**NEW 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.** 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
**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.** 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

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 35**

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: (SHOW ANSWER)**

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

**NEW QUESTION: 36**

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

**A.** ${incident.UserMail}

**B.** ${incident.usermail}

**C.** ${usermail}

**D.** ${incident.User Mail}

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 37**

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

**A.** Section Header task

**B.** Data Collection task

**C.** Standard task

**D.** Conditional task

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 38**

## Context


freecram.net


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

**A.** 1E56733826E5035233A097FCEA2046AF96EC616C

**B.** e6ef5142e2553c1e442a0ffac07636eac61e6edd

**C.** E6EF5142E2553C1E442A0FFAC07636EAC61E6EDD

**D.** 8D193FA162A305E4859BA8C45F5121F7265E3ABB

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 39**

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: (SHOW ANSWER)**

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

**NEW QUESTION: 40**

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?

Freecram.net

**A.** status=="Pending"andandcategory!="job"andandseverity=="High"andandowner=="None" andandtype=="Phishing"andandemailsubject=="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: (SHOW ANSWER)**
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

**NEW QUESTION: 41**
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.** Run the command !findIndicators in CLI with the query firstSeen:>="90 days ago" and export to CSV.
**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.** SSH into the server and copy the indicator's database.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 42**
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.** Contribute through the XSOAR UI
**B.** Create a pull request directly on Github
**C.** Open a ticket with the XSOAR support team
**D.** Send an email to contributions@xsoar.com
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 43**
Which set of trigger options is available to start a job when a new instance is created?.
**A.** "Mapping" and "Classification"
**B.** "Time" and "By delta in feed"
**C.** "Cron View" and "Human View"
**D.** "Script Start" and "CLI"
**Answer: (SHOW ANSWER)**
Cortex XSOAR jobs are automated scheduled tasks used for running playbooks or scripts on a recurring basis.
According to the Jobs documentation within the XSOAR Admin Guide, the available job trigger mechanisms includeTime-based triggersandDelta-based feed triggers.
ATimetrigger enables execution at scheduled intervals using either predefined frequency settings or a cron expression. This allows running jobs hourly, daily, weekly, etc.
ABy delta in feedtrigger launches a job when a connected feed detects changes (new, updated, or removed indicators). This is

commonly used in threat-intelligence workflows to perform enrichment, normalization, or distribution when new indicator data arrives.
The other options listed do not exist within XSOAR's job trigger configuration. "Mapping and Classification" are ingestion components, not job triggers. "Cron View and Human View" are simply formatting options for viewing scheduling expressions-not trigger types.
"Script Start and CLI" describe execution methods for scripts, not job-initialization triggers.
Thus, optionBis the accurate and documented set of job trigger types available when creating a new job in XSOAR.

**NEW QUESTION: 44**
A temporary integration issue causes a scheduled job to fail continuously.
Which action will ensure the job continues to run after future failures?.
**A.** Edit Queue Handling settings of the job.
**B.** Verify that the "Continue on Error" box is checked in the job.
**C.** Adjust the Role-Based Access Control (RBAC) of the incident type.
**D.** Ensure the last playbook task runs closeInvestigation.
**Answer: (SHOW ANSWER)**
Jobs in XSOAR run playbooks or scripts automatically at scheduled intervals. According to the Job Execution section of the Admin Guide, if a job encounters an error during playbook execution, its continued operation depends on whether"Continue on Error"is enabled. When this checkbox is selected, the job will not terminate due to an exception or integration failure. Instead, it logs the error and proceeds to the next scheduled execution as normal.
Queue handling settings (A) apply to indicators/job queues within feeds, not job failure behavior. RBAC changes (C) do not influence job execution continuity. Ensuring the last task closes the investigation (D) is unrelated and may even disrupt job workflows, since jobs often do not require incident-based models.
By contrast, enablingContinue on Erroris the documented mechanism that prevents scheduled jobs from halting due to transient or recurring errors. It ensures operational resilience, especially during integration outages or API rate limits.
Thus, optionBis the correct and fully documented answer.

**NEW QUESTION: 45**
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: (SHOW ANSWER)**

**NEW QUESTION: 46**
Where is a custom layout for an incident configured?.
**A.** Pre-process rule.
**B.** Incident playbook.
**C.** Integration instance settings.
**D.** Incident type.
**Answer: (SHOW ANSWER)**
The Admin Guide states that layouts-representing how analysts view incident data, evidence, fields, and work plans-are attached

directly toincident types. When configuring an incident type, the administrator can specify the layout for the "New," "Editing," and "Preview" modes. This ensures consistent presentation of data across the SOC, tailored to each use case (e.g., phishing, endpoint alerts, malware investigations).
Pre-process rules (option A) operate before incident creation and do not control the user interface layout.
Incident playbooks (option B) automate response actions but have no effect on how the incident UI is presented. Integration instance settings (option C) define connection details and ingestion parameters but do not control UI layouts.
Only theIncident Type configuration pageincludes fields for selecting or assigning custom layouts. This aligns with XSOAR's design principle: incident types define schema, workflows, and UI behavior, including which layout is displayed to analysts.
Thus, the correct answer isD, as incident layouts are configured and bound within theIncident Typesettings.

**Valid XSOAR-Engineer Dumps** shared by EduDump.com for Helping Passing XSOAR-Engineer Exam! EduDump.com now offer the **newest XSOAR-Engineer exam dumps**, the EduDump.com XSOAR-Engineer exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com XSOAR-Engineer dumps with Test Engine here: https://www.edudump.com/exams/Palo-Alto-Networks/XSOAR-Engineer/premium/ (**206** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

**NEW QUESTION: 47**
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: (SHOW ANSWER)**
Reference: https://xsoar.pan.dev/docs/integrations/context-and-outputs#:~:text=The%20main%20use%20of%20the,the%20Context%20and%20uses%20it.

**NEW QUESTION: 48**
Which playbook will a job run by default?
**A.** The playbook assigned by the integration
**B.** The playbook assigned during pre-processing
**C.** The playbook assigned to the incident type
**D.** The playbook assigned to the indicator type
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 49**
Which tag must be applied to an Automation Script in order for it to be available when configuring an Indicator Type?
**A.** reputationScript
**B.** reputation
**C.** enrich

**D.** reputation-script
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 50**
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 - Unreliable, A - Completely Reliable
**C.** F - Not reliable, A - Usually Reliable
**D.** F - Not usually reliable, A - Fairly Reliable
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 51**
Two feed integrations with the same source reliability (B - Usually reliable) fetch the same indicator with the following verdicts:
Integration A - Malicious
Integration B - Benign
Indicator data from Integration B was fetched after Integration A.
What will be the values of the fields associated with the indicator?.
**A.** Verdict: Malicious
Other Fields: Values from Integration A.
**B.** Verdict: Malicious
Other Fields: Values from Integration B.
**C.** Verdict: Benign
Other Fields: Values from Integration A.
**D.** Verdict: Benign
Other Fields: Values from Integration B.
**Answer: (SHOW ANSWER)**
According to the Threat Intelligence section of the XSOAR Admin Guide, indicatorverdict resolutionuses two key rules:
* If multiple sources have different reliability levels, the verdict from the highest-reliability source wins.
* If multiple sources share the same reliability, XSOAR selects the "worst" (most severe) verdict among them.
Because both integrations have equal reliability (B - Usually reliable), XSOAR selects the more severe verdict. "Malicious" is more severe than "Benign," so the resulting indicator verdict will beMalicious.
However, indicatorfield valuesfollow a different rule:
When multiple sources share the same reliability score,the most recently updated source overwrites the indicator fields, except for the verdict field.
Integration B updated the indicator after Integration A, so its field values overwrite Integration A's fields. But its verdict does not override the malicious verdict because severity resolution rules take precedence.
Therefore, the correct combined logic yields:
* Verdict: Benign? No # Because Malicious is the highest severity.
* Other Fields: From the most recently updated feed # Integration B.
But the verdict is strictly the "worst" verdict, so:
Correct answer: C.

**NEW QUESTION: 52**
What can be added to offload integration instance processing from the main server?
**A.** Engine
**B.** Development server
**C.** Application server
**D.** Database node
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 53**
What is the correct expression to use when filtering only PDF files?
**A.** Use File.Extension equals (string comparison) PDF
**B.** Use File.Name contains PDF
**C.** Use File.Extension that does not equal (string comparison) PDF
**D.** Use File.Extension contains (general) PDF
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 54**
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: (SHOW ANSWER)**
Reference: https://www.paloaltonetworks.com/resources/datasheets/cortex-xsoar-overview

**NEW QUESTION: 55**
What is the unique identifier for a note in the incident War Room?.
**A.** Incident ID.
**B.** Entry ID.
**C.** Field ID.
**D.** Note ID.
**Answer: (SHOW ANSWER)**
In XSOAR, every entry in the War Room (commands, notes, outputs, files) is stored with a unique Entry ID.
Notes do not have a separate "Note ID"; they are War Room entries, and therefore their unique ID is the Entry ID.

**NEW QUESTION: 56**
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: (SHOW ANSWER)**

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

**NEW QUESTION: 57**

When using the playbook debugger, what may be the cause of a starred incident missing from the Test Data selections?.

**A.** Closed incidents are not visible in the debugger.

**B.** The incident has been restricted.

**C.** Starred incidents are not visible in the debugger.

**D.** The incident type is set incorrectly.

**Answer: A (LEAVE A REPLY)**

The XSOAR Playbook Debugger allows engineers to simulate playbook behavior using existing incidents as sample data. The documentation explicitly states that onlyopen incidentsappear within the debugger's Test Data selection list. Closed incidents are removed from the selectable list because the debugger cannot execute against non-active incident states.

Starring an incident does not affect debugger availability; the star is a user-level convenience for bookmarking. RBAC restrictions (B) could hide an incident in general UI contexts but not selectively from the debugger. Incorrect incident type (D) also does not prevent selection as long as the incident is open.

Therefore, if a starred incident does not appear as a debugging option, the most common and documented reason is that the incident has beenclosed, and closed incidents cannot be used as debugger input. This aligns with optionA.

**NEW QUESTION: 58**

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

**A.** Automation

**B.** Built-in

**C.** Data collection

**D.** For-each

**E.** Conditional

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 59**

Where is a custom layout for an incident configured?.

**A.** Integration instance settings.

**B.** Incident type.

**C.** Incident playbook.

**D.** Pre-process rule.

**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 60**

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: (SHOW ANSWER)**
Reference: https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.6/Cortex-XSOAR-Administrator- Guide/Customize-Incident-Layouts

**NEW QUESTION: 61**
While testing a custom integration, an XSOAR engineer noticed that the incident fetch interval is missing.
How can this be fixed?
**A.** 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.
**B.** Define the Incident Fetch Interval when running the integration's commands.
**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: (SHOW ANSWER)**

**Valid XSOAR-Engineer Dumps** shared by EduDump.com for Helping Passing XSOAR-Engineer Exam! EduDump.com now offer the **newest XSOAR-Engineer exam dumps**, the EduDump.com XSOAR-Engineer exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com XSOAR-Engineer dumps with Test Engine here: https://www.edudump.com/exams/Palo-Alto-Networks/XSOAR-Engineer/premium/ (**206** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

**NEW QUESTION: 62**
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: (SHOW ANSWER)**
Reference: https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.5/Cortex-XSOAR-Threat-Intel- Management-Guide/Indicator-Expiration

**NEW QUESTION: 63**
Which component can be part of a load balancing group?
**A.** Distributed database
**B.** D2 agent

**C.** Engine

**D.** Load balancing server

**Answer: (SHOW ANSWER)**

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

**NEW QUESTION: 64**

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

**Answer: (SHOW ANSWER)**

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

**NEW QUESTION: 65**

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: (SHOW ANSWER)**

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

**NEW QUESTION: 66**

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

**A.** Which tabs appear and in which order

**B.** Which users have permissions to view the tabs

**C.** Which roles have permissions to view the tabs

**D.** Which dashboard settings are applied

**E.** The information and how is it displayed

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 67**

What can be used as integration parameters?

**A.** User-password, csv file, query

**B.** URL, certificate, image

**C.** URL, API key, port

**D.** Token, query, playbook

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 68**
Which two options may be added when a content pack is being installed? (Choose two.)
**A.** Indicator layouts
**B.** Roles
**C.** Other content packs
**D.** Lists
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 69**
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 [as value]
**D.** Get csvList.value where csvList.value equals test {}[from previous tasks]
**E.** Get csvList.value where csvList.value equals ${test} [as value]
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 70**
What is an outcome of using sections within a tab when customizing an incident layout?.
**A.** Triggering specific automations or playbooks when data within that section is modified during an investigation.
**B.** Enforcing mandatory fields that must be completed before an incident can be closed.
**C.** Grouping related fields and information logically, improving readability and data entry efficiency.
**D.** Restricting access to sensitive fields based on user roles, ensuring data privacy within the specific incident type.
**Answer: (SHOW ANSWER)**
The Layout customization section of the XSOAR Admin Guide explains that incident layouts control how analysts view and interact with fields, evidence, and metadata. Within a layout tab, sections exist purely for the purpose of organizing related fields into structured blocks, improving clarity, readability, and workflow efficiency. This is essential in complex incident types where numerous fields must be grouped logically (e.g.,
"User Details," "Endpoint Information," "Alert Metadata").
Sections do not trigger automations or playbooks; automation triggers are defined through playbooks, field- change scripts, or incident type settings. They also do not enforce field mandatory requirements-mandatory fields are defined in the incident type configuration, not within layout sections. Likewise, RBAC does not operate at the section level; access restrictions apply to fields or entire incident types, not layout sections.
Therefore, the only correct and documented result of using sections within tabs is enhanced logical grouping of fields, improving analyst usability and data-entry organization. This aligns with option C, matching the intended purpose described in the layout configuration documentation.

**NEW QUESTION: 71**
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 ReadandEdit 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: (SHOW ANSWER)**
Reference: https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.5/Cortex-XSOAR-Administrator- Guide/Create-the-Read-Only-Dashboard

**NEW QUESTION: 72**
Which action will resolve the issue when an analyst upgrades a content pack from the Marketplace, and the new version has a code error?.
**A.** Revert the content pack to a previous version.
**B.** Uninstall and reinstall the content pack.
**C.** Upgrade the dependencies of the content pack.
**D.** Export and manually upload the content pack.
**Answer: (SHOW ANSWER)**
The Marketplace section states that administrators can revert any installed content pack to a previous version via the Version History # Revert to this version option.
This is the recommended method when a new release introduces a bug.
Reinstalling the same version does not fix the code error.

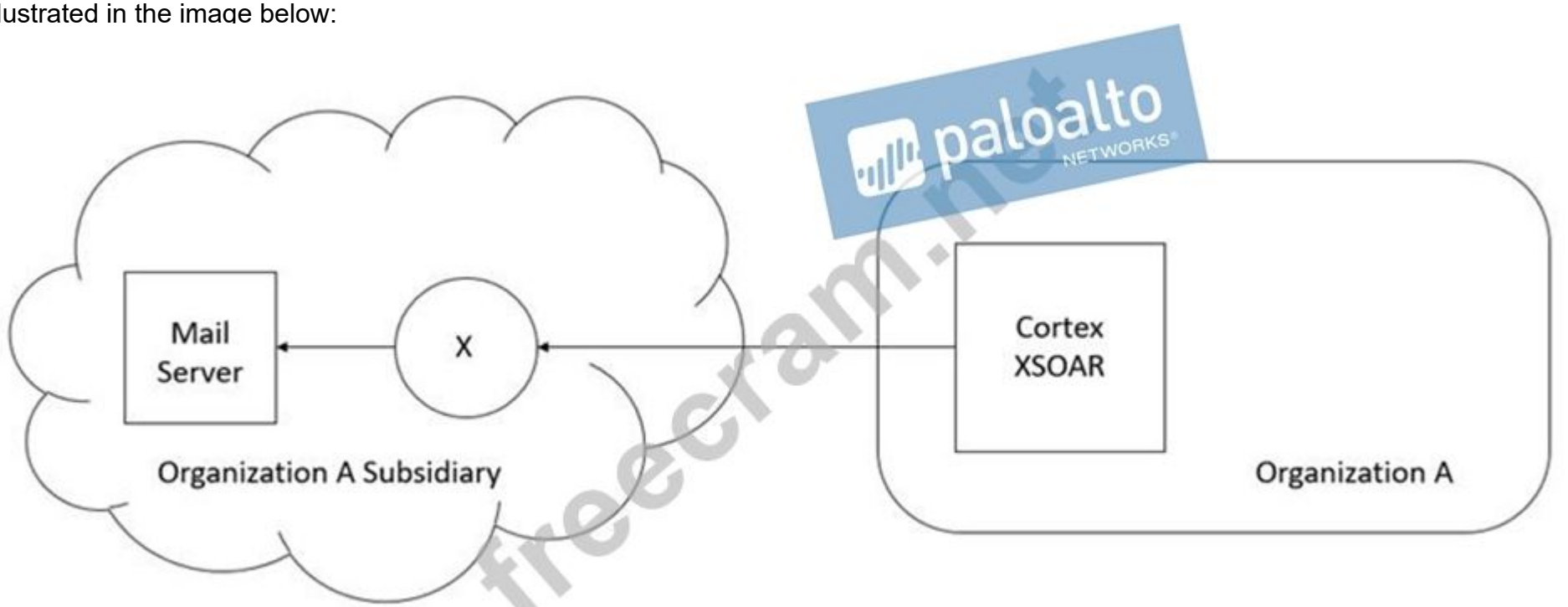
**NEW QUESTION: 73**
When uploading content, which two options could the upload include? (Choose two.)
**A.** Reports
**B.** Fields
**C.** Indicators
**D.** Incidents
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 74**
Which investigation element is best suited for collaboration among users?
**A.** Work Plan
**B.** Related Incidents
**C.** War Room
**D.** Context Data
**Answer: (SHOW ANSWER)**
Reference: https://blog.paloaltonetworks.com/2020/01/cortex-security-operations/

**NEW QUESTION: 75**
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: (SHOW ANSWER)**
Reference: https://xsoar.pan.dev/docs/incidents/incident-classification-mapping

**NEW QUESTION: 76**
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.** A Linux server connected with an XSOAR server using SSH integration. Commands can be run remotely to access the mail server.
**B.** An XSOAR engine that is downloaded from the XSOAR server and installed within the subsidiary.
**C.** XSOAR D2 Agents, to send the required emails.
**D.** Another XSOAR server that uses the same license as their primary XSOAR server.
**Answer: A (LEAVE A REPLY)**

**Valid XSOAR-Engineer Dumps** shared by EduDump.com for Helping Passing XSOAR-Engineer Exam! EduDump.com now offer the **newest XSOAR-Engineer exam dumps**, the EduDump.com XSOAR-Engineer exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com XSOAR-Engineer dumps with Test Engine here: https://www.edudump.com/exams/Palo-Alto-Networks/XSOAR-Engineer/premium/ (**206** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

**NEW QUESTION: 77**

What must happen before a pre-process rule can be applied to a potential incident?.

**A.** Mapping.

**B.** Playbook execution.

**C.** Ingestion.

**D.** Classification.

**Answer: (SHOW ANSWER)**

The XSOAR event-to-incident pipeline is clearly defined in the admin documentation:Ingestion # Classification # Pre-Processing # Incident Creation # Playbook Execution. Classification must occur beforepre-process rules because the system must determine an incident type (or classification result) before evaluating any pre-process logic that may drop, merge, link, or modify the incoming incident.

Pre-process rules use fields created during the classification stage-including incident type, normalized values, and extracted fields-to determine whether an incident should be suppressed, modified, or related to an existing incident. Without classification completing first, the rule engine would not have the necessary structured data.

Mapping, which transforms raw event fields into incident fields, occursafterclassification but during incident creation, meaning it also precedes playbook execution but not pre-process evaluation.

Therefore, optionD (Classification)is the only correct prerequisite. Pre-process rules cannot run at ingestion time (option C). Playbook execution (option B) happensafterthe incident is created. Mapping (option A) is not a prerequisite for pre-process rules.

**NEW QUESTION: 78**

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

**A.** Standard (Manual)

**B.** Conditional

**C.** Section header

**D.** Standard (Automated)

**Answer: (SHOW ANSWER)**

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

**NEW QUESTION: 79**

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

**A.** The output of the previous task automatically becomes the input of the subplaybook.

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

**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: (SHOW ANSWER)**

**NEW QUESTION: 80**

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: A,D,E (LEAVE A REPLY)**

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

**NEW QUESTION: 81**

What happens when an integration is deprecated?

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

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

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

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

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 82**

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: (SHOW ANSWER)**

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

**NEW QUESTION: 83**

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: (SHOW ANSWER)**

**NEW QUESTION: 84**

An engineer adds a new "Forensics" tab that includes several sections for detailed artifact analysis to the "Malware Incident" layout. However, junior analysts report they cannot see this tab, while senior analysts can.

Which configuration setting is the most likely reason for this discrepancy?.

**A.** The underlying fields within the tab sections was incorrectly mapped.

**B.** The tab was not added to the junior analyst role group.

**C.** The tab was marked as read-only in the layout configuration for the junior analyst roles.

**D.** A display filter was applied to the tab in the layout editor.

**Answer: (SHOW ANSWER)**

According to the Cortex XSOAR Admin Guide, visibility of layout tabs is controlled byrole-based access permissions (RBAC). When customizing layouts, administrators can assign tabs, fields, and components to specific user roles. If the "Forensics" tab appears for senior analysts but not junior analysts, this indicates that the tab has been assigned only to certain roles through the "Roles" field in the layout editor.
XSOAR does not hide layout tabs due to incorrect field mappings (option A). If a field is unmapped, it simply appears empty, not invisible. Likewise, marking a tab as "read-only" (option C) still makes it visible; it only restricts editing. Display filters (option D) apply to list widgets, dashboards, and incidents-not layout tab visibility.
The documentation clearly states thata tab will not appear to a user unless their assigned role is included in the tab's role permissions. Therefore, junior analysts cannot view the tab becausethe tab was not assigned to their role, making optionBthe correct explanation based on XSOAR's RBAC-controlled layout behavior.

**NEW QUESTION: 85**
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: (SHOW ANSWER)**
Reference: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar-admin/installation/install- demisto-on-a-physical-or-virtual-server.html

**NEW QUESTION: 86**
Based on the integration and classifier configuration images below,


which incident type will be created for incidents ingested using this integration when the incoming "type" field is set to "url allowed"?.
**A.** Access.

**B.** XSOAR ENGINEER- URL Alerts.

**C.** URL Allowed.

**D.** Case.

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 87**

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:jobandtype:Phishing created:<="30 days ago"

**C.** status:closed -category:jobandtype:Phishing created:>="30 days ago"

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

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 88**

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: D,E (LEAVE A REPLY)**

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

**NEW QUESTION: 89**

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

**A.** Settings > About > Troubleshooting > Set Log Level to Debug > Download Logs

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

**C.** Settings > About > System Diagnostics

**D.** DashboardsandReports > System Health

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 90**

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

**A.** setIncident

**B.** Layout inline editing

**C.** Field mapping

**D.** setFields

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 91**
Where would you look to find a personalized view of your own incidents and tasks?
**A.** My Incidents
**B.** Incident Summary View
**C.** My Dashboard
**D.** My Threat Landscape
**Answer: (SHOW ANSWER)**

**Valid XSOAR-Engineer Dumps** shared by EduDump.com for Helping Passing XSOAR-Engineer Exam! EduDump.com now offer the **newest XSOAR-Engineer exam dumps**, the EduDump.com XSOAR-Engineer exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com XSOAR-Engineer dumps with Test Engine here: https://www.edudump.com/exams/Palo-Alto-Networks/XSOAR-Engineer/premium/ (**206** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

**NEW QUESTION: 92**
Which of these would be the most operationally efficient repository for moving XSOAR custom content from a development server to a production environment?
**A.** The development server's default repository
**B.** Remote git repository specified in the dev-prod configuration parameters
**C.** A content repository specified in the Marketplace
**D.** Cortex XSOAR public content repository
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 93**
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.** /setIncident description=Confirmed Phishing
**B.** /incidentSet description=Confirmed Phishing
**C.** !setIncident description="Confirmed Phishing"
**D.** !incidentSet description="Confirmed Phishing"
**Answer: D (LEAVE A REPLY)**

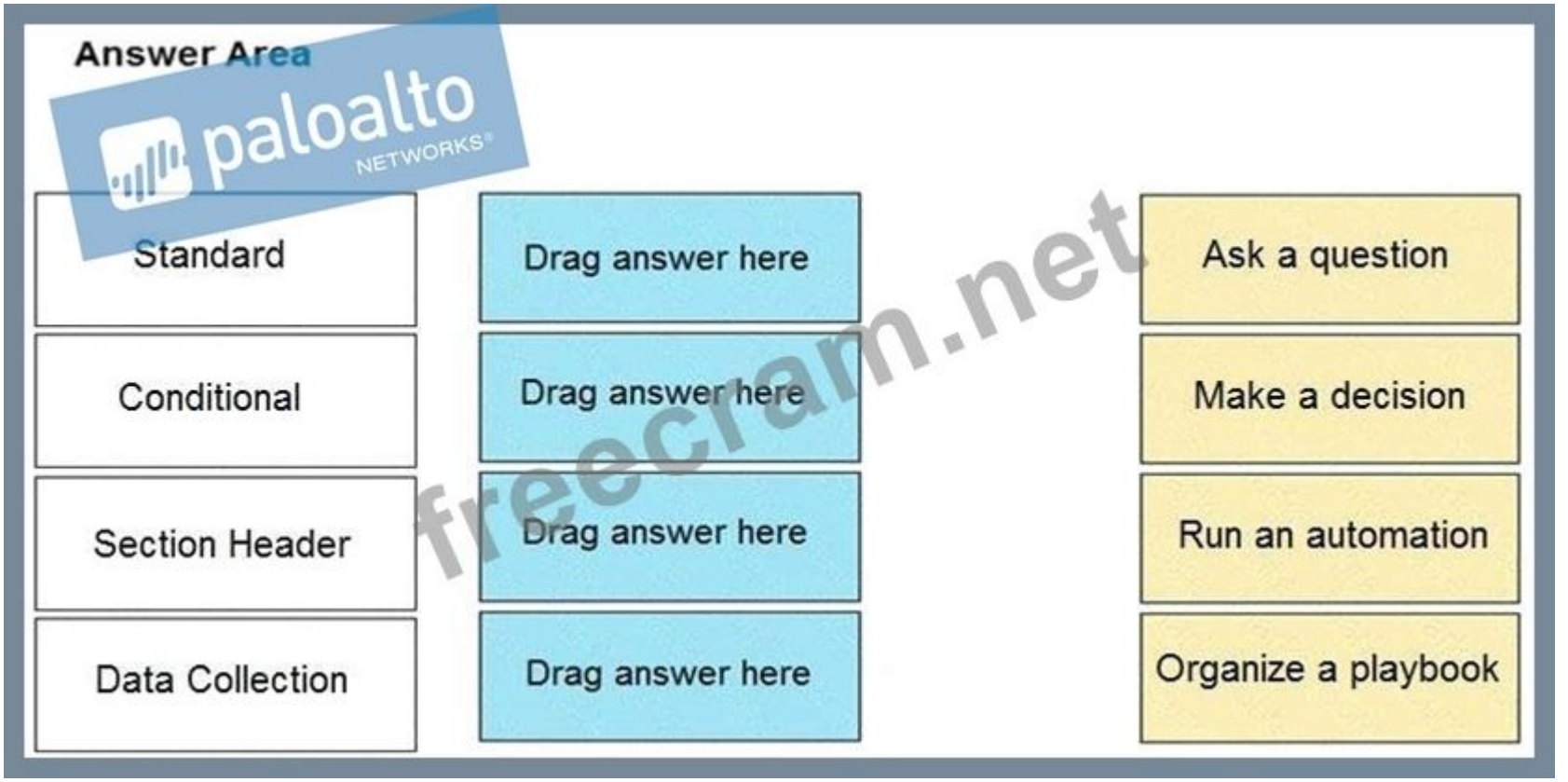
**NEW QUESTION: 94**
An administrator wants to send an email via the Mail Sender integration. Which of the following out of the box methods would be used for that?
**A.** common automation script
**B.** XSOAR shared agent
**C.** XSOAR D2 agent
**D.** external integration command

**Answer: (SHOW ANSWER)**

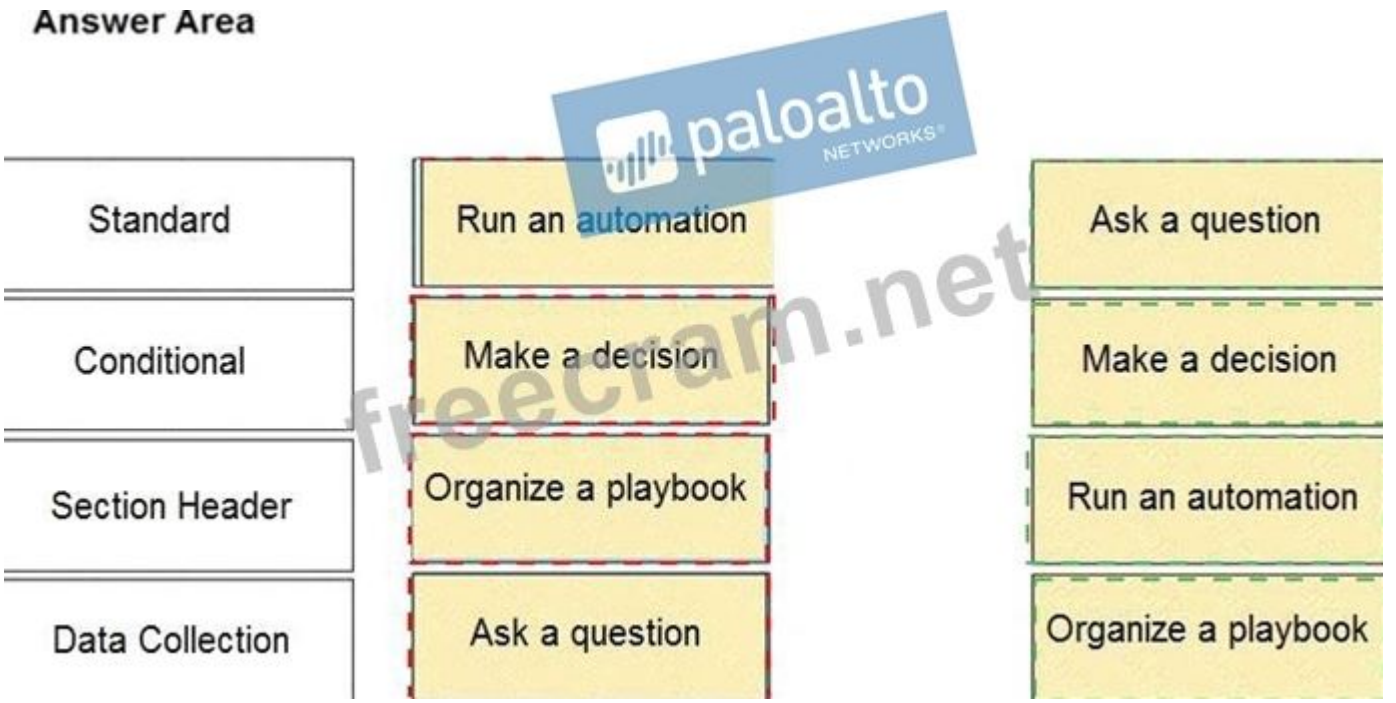
**NEW QUESTION: 95**
Assuming an incident type configuration runs the associated playbook automatically, which pre-process rule action can preserve matching incidents without triggering the playbook?.
**C.** Drop.
**A.** Close.
**D.** Link.
**B.** Update.
**Answer: (SHOW ANSWER)**
Pre-process rules allow XSOAR to evaluate incoming events before they are fully created as incidents. These rules can suppress, modify, or relate events based on defined criteria. According to the Admin Guide, when a pre-process rule uses theLinkaction, XSOAR links the incoming event to an existing incident without triggering the standard incident creation process or subsequent playbook execution. This preserves the data for correlation and investigation while preventing duplicate or unnecessary playbook runs.
TheCloseaction (A) suppresses incidents completely and is used to auto-close unwanted events; this prevents preservation of the event and does not trigger the playbook. TheDropaction (C) discards incoming events entirely, removing them from the system and not preserving them. TheUpdateaction (B) modifies or enriches existing incidents but does not stop the playbook from running on newly created incidents of that type.
Because the requirement is topreserve the incident while also preventing automatic playbook execution, the Link action is the only workflow that fulfills both requirements according to XSOAR's pre-process rule architecture. Thus, optionDis correct.

**NEW QUESTION: 96**
What happens if both a Classifier and Incident Type are configured in an integration instance's settings?
**A.** The Classifier will be ignored, and incoming incidents will be classified according to the Incident Type.
**B.** Both the Classifier and Incident Type will classify incoming incidents.
**C.** The administrator will receive a notification that there is both a Classifier and Incident Type set for that integration instance.
**D.** The Incident Type will be ignored, and incoming incidents will be classified according to the Classifier.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 97**
Match the action with the most appropriate playbook task type.




**Answer:**




Explanation:

**Answer Area**


paloalto NETWORKS
freecram.net

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

**NEW QUESTION: 98**

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 questions to a person or team

**Answer: (SHOW ANSWER)**

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

**NEW QUESTION: 99**

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

**A.** Export and import custom content

**B.** View and modify server configuration settings

**C.** Download the debug log bundle

**D.** Put the XSOAR server in maintenance mode

**E.** View a list of server administrators

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 100**

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: (SHOW ANSWER)**

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

**Valid XSOAR-Engineer Dumps** shared by EduDump.com for Helping Passing XSOAR-Engineer Exam! EduDump.com now offer the **newest XSOAR-Engineer exam dumps**, the EduDump.com XSOAR-Engineer exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com XSOAR-Engineer dumps with Test Engine here: https://www.edudump.com/exams/Palo-Alto-Networks/XSOAR-Engineer/premium/ (**206** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)