PassQueen
a.k.a dumpsqueen.com

Palo Alto Networks Certified Security Automation Engineer

Palo Alto Networks PCSAE

Version Demo

Total Demo Questions: 19

Total Premium Questions: 196

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Data Ingestion and Enrichment	28
Topic 2, Incident Investigation and Management	34
Topic 3, Automation and Orchestration	63
Topic 4, Integrations	26
Topic 5, Platform Administration	45
Total	196

QUESTION NO: 1

The XSOAR administrator is writing an automation and would like to return an error entry back into XSOAR if a particular command errors out. How can this be achieved?

A. Using the demisto_error() function

B. Using a print statement

C. Using the demisto.debug() function

D. Using the return_error() function

ANSWER: D

Explanation:

Using the `return_error()` function is the appropriate way for an XSOAR automation to send a command failure back to XSOAR as an error result. The function is intended for unrecoverable execution failures: it creates an error entry that is visible in the War Room and terminates the script's execution. An automation can call it from an exception handler, for example `except Exception as e: return_error(f"Command failed: {e}")`, so that the user receives a clear failure message rather than an incomplete or misleading result. The optional exception argument can also be supplied when available, allowing XSOAR to preserve useful error context for troubleshooting. This behavior makes `return_error()` suitable when a particular command cannot complete and the automation should explicitly report that outcome to the platform. Palo Alto Networks documents this helper in the CommonServerPython API reference, where it is described as returning an error entry to the War Room and exiting the script. See the CommonServerPython API reference and the XSOAR code conventions.

QUESTION NO: 2

Which two options are the most effective for moving content between two environments? (Choose two.)

A. Remote repository based content sharing

B. UI based content import/export button

C. Copy the content backup from one environment file system (/var/lib/demisto/backup/content-backup-*) and move it to the other environment

D. Download the content items separately and upload them to the other environment

ANSWER: A C

Explanation:

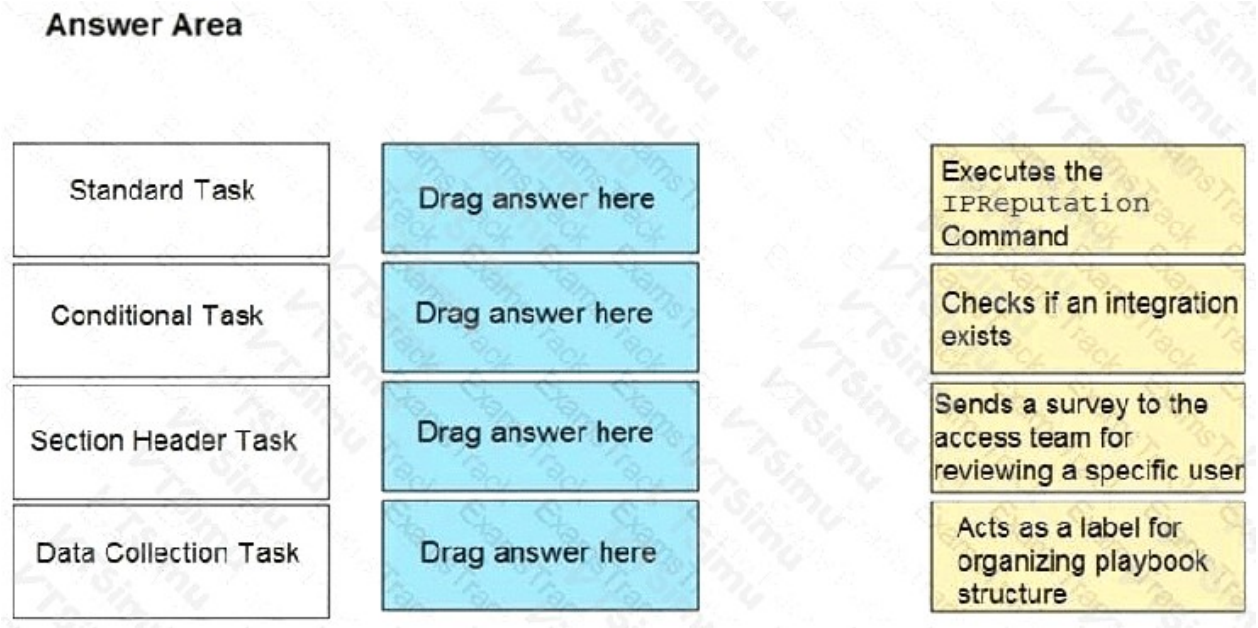
Remote repository based content sharing is an effective approach because it places custom XSOAR content under source control and provides a repeatable promotion workflow between development, test, and production environments. A remote repository can hold playbooks, integrations, scripts, layouts, incident types, classifiers, mappers, and other content as managed files. Teams can review changes, track versions, and synchronize the approved content into each target environment, which makes it particularly suitable for ongoing content-development and release processes.

Copy the content backup from one environment file system (/var/lib/demisto/backup/content-backup-*) and move it to the other environment is also effective when migrating a broader set of existing content in bulk. XSOAR creates content-backup archives that can be transferred to another server and used during migration, avoiding the need to export and import each individual item. This approach is especially useful for moving content between environments or when establishing another tenant with comparable content.

These methods support scalable, repeatable content movement while preserving content relationships and reducing manual administration. Palo Alto Networks documents the content-backup migration process in the Cortex XSOAR migration documentation. For repository-based development practices, see the XSOAR Content Repository documentation.

QUESTION NO: 3 - (SIMULATION)

Match the corresponding action with the appropriate playbook tasks.



ANSWER: See the explanation for the answer

Explanation:

Match the tasks as follows:

A standard task runs a command or automation, a conditional task evaluates criteria to determine a flow branch, section headers organize the visual playbook, and data-collection tasks request information through a questionnaire/survey.

QUESTION NO: 4

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

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

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

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

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

E. To loop the sub-playbook over each item in a selected sub-playbook input

ANSWER: E

Explanation:

To loop the sub-playbook over each item in a selected sub-playbook input is correct. In Cortex XSOAR, a sub-playbook task can be configured to iterate when an input contains multiple values, such as a list of indicators, users, endpoints, or artifacts. The *For Each Input* setting identifies the particular input whose individual items should drive the loop. XSOAR then runs a separate iteration of the sub-playbook for each item in that selected input, passing the relevant per-item value into the execution. This lets a reusable sub-playbook process collections without requiring separate task nodes for every value. The behavior is tied to the selected input and its values; it is not an automatic iteration over the entire investigation context or every available sub-playbook input. When designing the sub-playbook, its input definitions and task logic should therefore be built to consume the individual item supplied during each iteration. Palo Alto Networks documents playbook task

configuration and sub-playbook input handling in the Cortex XSOAR Playbooks documentation and provides additional implementation guidance in the XSOAR playbook inputs and outputs guide.

QUESTION NO: 5

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

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

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

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

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

ANSWER: D

Explanation:

Settings > About > System Diagnostics, in the main host account. Each host has a System Diagnostics page. is correct because System Diagnostics is the host-level monitoring area used by a main host administrator in a Cortex XSOAR multitenant deployment. The main host account provides centralized visibility into the operational state of hosts, while the individual System Diagnostics page for each host supplies the host-specific information needed to assess health, performance, capacity, and resilience. This enables administrators to identify conditions affecting service availability or resource consumption and take the appropriate maintenance or scaling actions for the affected tenant host. Access through the About section reflects that System Diagnostics is an administrative platform-health capability rather than an account-management or general troubleshooting workflow. Palo Alto Networks documents Cortex XSOAR administrative and multitenancy operations in its official documentation portal, including system monitoring and host-management guidance. See the Palo Alto Networks Cortex documentation portal and the Cortex XSOAR community and product resources for current administrative documentation and operational guidance.

QUESTION NO: 6

Which playbook task type should be used to direct execution to different tasks according to values in the incident context?

A. Standard task

B. Conditional task

C. Section Header task

D. Data Collection task

ANSWER: B

Explanation:

Conditional task is correct. A Conditional task evaluates one or more conditions that use incident fields, context data, task results, or other available values. Based on whether a condition evaluates as true or false, the playbook follows the corresponding connection to the next task.

This enables a playbook to make workflow decisions dynamically, such as continuing with containment when an indicator is malicious or ending an enrichment branch when no actionable data is returned. A Standard task performs an action, whereas a Conditional task determines which path the playbook should take. See the Cortex XSOAR playbooks documentation for playbook task and condition configuration guidance.

QUESTION NO: 7

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

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

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

C. Outputs are used as incident trigger for playbook

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

E. Inputs are the data fields parsed by the Classifier

ANSWER: A D E

Explanation:

In Cortex XSOAR playbook development, inputs represent the information made available to a playbook when it runs. “Inputs are data pieces that are present in the playbook” is correct because playbook inputs are defined at the playbook level and provide the values that tasks use during execution. They enable a playbook to work with incident information, context data, or values passed from a calling playbook without hard-coding those values into task logic.

“Outputs can be derived from the result of a task or command” is also correct. A task that runs an automation, integration command, or sub-playbook can produce results; those results can be mapped or exposed as outputs for subsequent workflow use. This supports modular automation, including passing useful results back to a parent playbook.

“Inputs are the data fields parsed by the Classifier” is correct in the lifecycle context because classifiers identify incoming event data and, together with mappers, make parsed incident fields available for playbook processing. Those incident values can then be consumed as playbook inputs. Palo Alto Networks documents the relationship between incoming data, classifiers, mappers, incidents, and automation in the Cortex XSOAR documentation and its playbook administration guidance.

QUESTION NO: 8

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

A. 2MB

B. 3MB

C. 1MB

D. 5MB

ANSWER: C

Explanation:

The default minimum Work Plan size classified as big is **1MB**. In Cortex XSOAR, the System Diagnostics page helps administrators identify operational conditions that can affect investigation processing and system performance. The Big Work Plans diagnostic focuses on work plans whose stored size reaches or exceeds the configured threshold, since unusually large work plans can indicate investigations with substantial task output, context data, evidence, or automation activity. By default, that threshold is set to 1MB, so a work plan at this size is included in the diagnostic results for review. This default gives administrators an early, practical signal for identifying investigations that may warrant examination or cleanup before accumulated data affects system efficiency. The threshold is a diagnostic classification setting rather than a limitation on whether an investigation can run. Palo Alto Networks documents System Diagnostics as part of the administrative monitoring and troubleshooting workflow; see the Cortex documentation portal and the Cortex XSOAR community resources for product administration guidance.

QUESTION NO: 9

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

A. setFields

B. Field mapping

C. setIncident

D. Layout inline editing

ANSWER: A C

Explanation:

`setFields` and `setIncident` are both playbook-capable mechanisms for persisting values to the current incident record. The Set Fields automation is designed to update one or more incident fields from values generated earlier in the playbook, including custom incident fields. This enables playbook tasks to retain enrichment results, classifications, ownership details, or other workflow data directly on the incident. The `setIncident` command similarly updates properties of the active incident and can assign values to built-in or custom fields. It is useful when a command task or automation needs to write incident data programmatically as part of an orchestration flow. In both cases, the saved values become part of the incident and are available to subsequent tasks, layouts, searches, and reporting. Palo Alto Networks documents the Set Fields automation in the Cortex XSOAR content reference and documents incident manipulation through the `setIncident` command. See the Set Fields automation reference and the setIncident command reference.

QUESTION NO: 10

What does the outgoing mapper support?

A. Mirroring

B. Classification

C. Dynamic fields

D. Pre-processing

ANSWER: A

Explanation:

Mirroring is correct. In Cortex XSOAR, an outgoing mapper is used when XSOAR sends incident data back to the remote system associated with an integration instance. Its purpose is to transform and map XSOAR incident fields into the field names and values expected by that external system. This is specifically used by incident mirroring, where updates made to an incident in XSOAR can be synchronized outward to the corresponding remote incident or ticket. For example, an outgoing mapper can map XSOAR's incident severity, status, owner, or custom fields to the appropriate fields in a ServiceNow, Jira, or other integrated platform's incident record. The mapper is selected in the integration instance configuration when enabling outbound incident mirroring, ensuring that the data sent from XSOAR conforms to the remote platform's schema. Palo Alto Networks documents outgoing mappers as part of the incident classification and mapping framework and describes their role in mapping data from XSOAR for use in mirrored incidents. See the Incident Classification and Mapping documentation and the Incident Mirroring documentation.

QUESTION NO: 11

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

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

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

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

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

E. By running the command !MarkAsEvidence

ANSWER: A B D

Explanation:

Evidence Board entries can be added through both analyst-driven and playbook-driven workflows. **Manually directly from the War Room with the Actions drop-down** is correct because an analyst can select relevant War Room entries and use the available actions to mark them as evidence, preserving investigation artifacts for later review. **From the Notes section (mark as entry icon)** is also correct because notes can be explicitly promoted to evidence using the evidence-marking control, allowing analyst observations and conclusions to be retained on the Evidence Board. **Automatically from playbook tasks when the option is selected on the Advanced tab** is correct because a task can be configured in its Advanced settings to mark its output as evidence when it runs. This enables playbook authors to consistently collect important automated findings without requiring a manual analyst step. Together, these methods support the Evidence Board's purpose of collecting notable investigation material, including War Room artifacts, analyst notes, and designated task results, into a concise evidence record for an incident. See Palo Alto Networks' Evidence Board documentation and task settings documentation.

QUESTION NO: 12

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

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

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

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

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

ANSWER: D

Explanation:

The Debugger panel to test data with one of last fifty incidents. This will not affect the incident's original incident data. This is the supported XSOAR playbook-development workflow. The Playbook Debugger lets an administrator select from the most recent incidents and execute the playbook in a separate debugging context. XSOAR uses a copy of the selected incident for the debug run, so task execution, context changes, and field updates produced while testing do not modify the source incident. This provides a safe way to validate conditional branches, task inputs and outputs, context paths, and integration-command behavior against realistic incident data before activating or changing a production playbook. The availability of the most recent fifty incidents is particularly useful because it enables selection of representative incident types and data sets without manually reproducing their contents. Administrators can inspect execution results in the debugger and iteratively adjust the playbook while preserving the original incident record and its audit history. Palo Alto Networks documents this capability in its Cortex XSOAR Administrator Guide: Debug a playbook. The broader XSOAR documentation portal is available at docs-cortex.paloaltonetworks.com.

QUESTION NO: 13

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

Explanation:

Custom widgets are appropriate when a dashboard must present data that is not adequately represented by the built-in widget types. **To visualize context data** is correct because Cortex XSOAR context contains the structured results produced during investigation and automation. A custom widget can use that context to display operationally meaningful values, such as enrichment results, indicators, task outputs, or other playbook-generated data, in a dashboard-oriented format.

To visualize a custom query is also correct because custom widgets can be based on a query that retrieves the specific incident or system data needed for a tailored dashboard visualization. This enables an engineer to select, aggregate, and present information according to an organization's reporting or operational requirements rather than relying solely on predefined dashboard views. Together, context-based visualization and query-based visualization address the primary purpose of custom widgets: surfacing customized, actionable XSOAR data for analysts and administrators.

For implementation details, see the Palo Alto Networks Cortex XSOAR Administrator's Guide and the Cortex XSOAR documentation portal.

QUESTION NO: 14

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: A B

Explanation:

When configuring an incident field in Cortex XSOAR, the Advanced section supports assigning a field trigger script and associating the field with one or more incident types. A field trigger script runs automatically when the field value changes, enabling playbook-style automation or validation logic directly in response to updates to that incident field. This lets an administrator extend incident behavior without requiring a user to manually initiate a separate action.

Associating a field with an incident type controls where the field is applicable and available. This is useful when different categories of incidents require different data, such as malware-analysis incidents versus phishing incidents. Limiting a field to relevant incident types helps keep incident forms focused while ensuring that the necessary contextual information is collected for each workflow. These advanced field settings are part of XSOAR's incident-field configuration and support customization of incident data collection and automation. See the Palo Alto Networks documentation for incident fields and the incident type configuration guidance.

QUESTION NO: 15

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

ANSWER: A D

Explanation:

Conditional tasks in Cortex XSOAR evaluate conditions against available incident and context data, then control how a playbook proceeds. They are used for branching paths in a playbook because the task can direct execution to different downstream tasks according to the condition result. This enables a single playbook to handle differing incident characteristics, confidence levels, enrichment results, or containment requirements without requiring separate playbooks for every scenario.

They are also used for sending a specific question to a person or team. A conditional task can determine that additional human input is required and route the relevant question or approval request based on the matching condition. For example, an escalation path can request validation from a particular analyst group only when the incident meets defined criteria. This combines automated decision logic with targeted analyst engagement while retaining the playbook's execution context. Palo Alto Networks describes conditional tasks as a mechanism for creating conditional branches in playbooks and for determining the appropriate next action based on evaluated conditions. See the Cortex XSOAR Conditional Task documentation and the Cortex XSOAR playbooks documentation.

QUESTION NO: 16

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: B D

Explanation:

In Cortex XSOAR, filters and transformers are data-processing tools that can be applied where information is passed into or handled by automation logic. **Playbook Tasks** is a primary location for their use: task inputs can be filtered to select relevant context values, and transformers can format, extract, combine, or otherwise modify those values before a task runs. This lets playbook authors ensure that automations and subsequent tasks receive data in the expected structure.

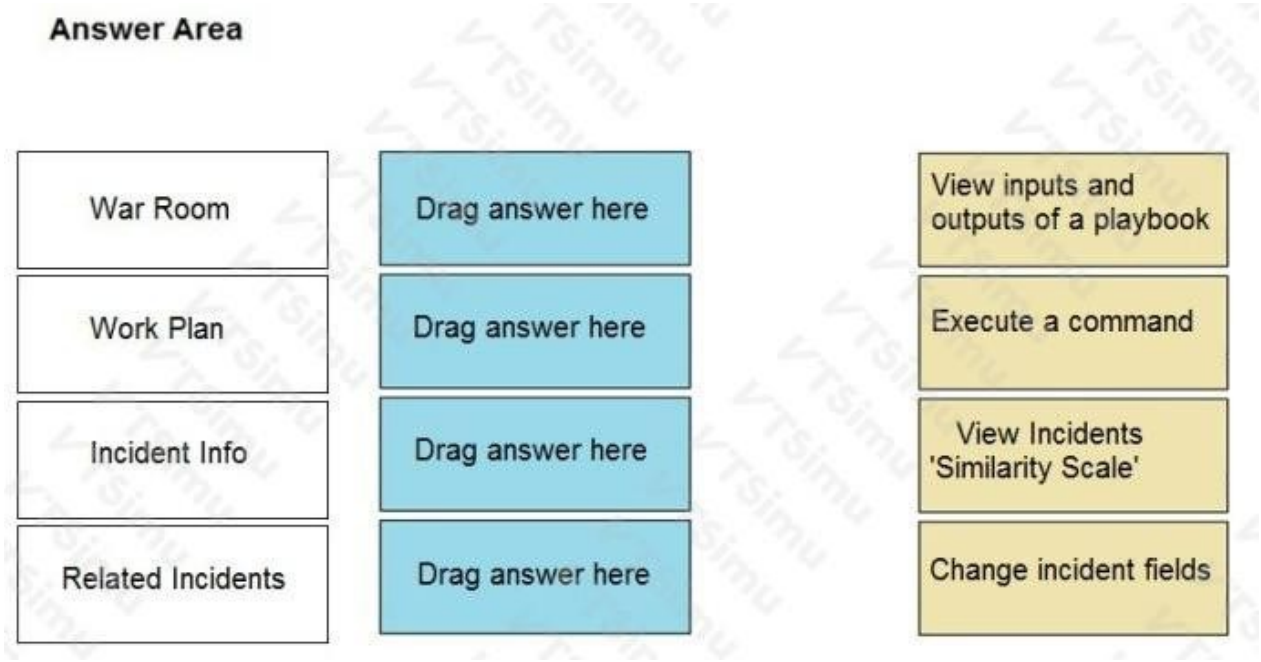
Incident Fields also supports filters and transformers. When configuring a field, these operations can control which values are populated and can transform the available context data into the form required by that incident field. This is useful for enriching incident records with normalized values, extracting specific indicators or attributes, and presenting investigation-relevant information consistently to analysts. Palo Alto Networks documents filters and transformers as mechanisms for filtering and transforming context data in both playbook task configuration and incident-field configuration. See the Cortex XSOAR Filters and Transformers documentation and the Cortex XSOAR context and outputs documentation.

QUESTION NO: 17 - (DRAG DROP)

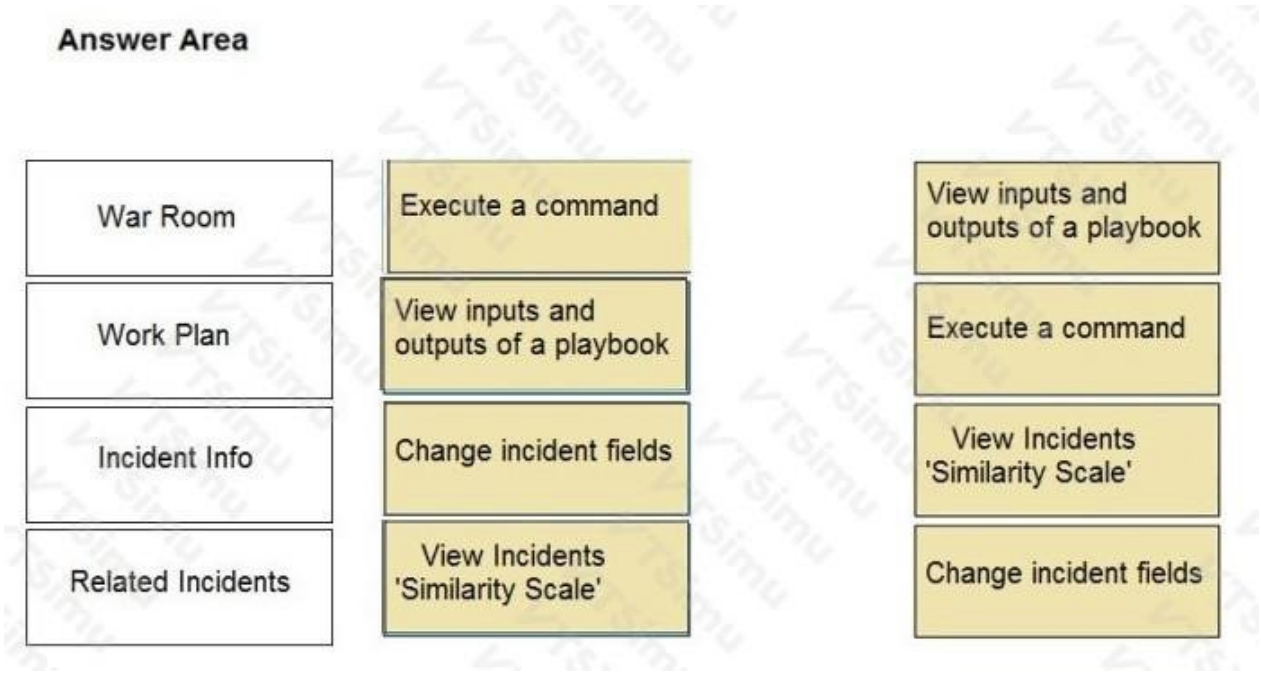
DRAG DROP

Match the appropriate action to the layout type.

Select and Place:



ANSWER:



Explanation:

Cortex XSOAR layouts divide incident activity into focused work areas, so the displayed mappings correctly align each action with the area designed for it. The War Room is the interactive investigation and response workspace. Analysts use it to run automation, query integrations, inspect command results, and continue an investigation, so executing a command belongs in the War Room. Palo Alto Networks describes the War Room as the incident's working area for commands and automation activity in the Cortex XSOAR War Room documentation.

The Work Plan presents the incident's playbook execution. It provides the operational view of playbook tasks and the information associated with their execution, including the inputs supplied to tasks and the results they produce. Therefore, viewing the inputs and outputs of a playbook correctly belongs in the Work Plan.

Incident Info is the layout section for the incident record itself. It displays the incident's configured fields and lets an analyst update the values that describe the case, such as status, severity, owner, classification, and organization-specific fields. Changing incident fields is consequently the intended action for Incident Info. Layouts can be configured to organize these fields and incident-context views, as described in the Cortex XSOAR layouts documentation.

Related Incidents is intended to help analysts identify other cases that may be connected to the active incident. Its similarity scale communicates how closely other incidents match based on the configured incident-similarity criteria. Viewing incidents through the similarity scale therefore belongs in Related Incidents. Together, these placements follow the normal investigation flow: issue commands in the War Room, track playbook execution in the Work Plan, maintain case data in Incident Info, and assess potentially connected cases in Related Incidents.

QUESTION NO: 18

Reliability scores in XSOAR range from A through F. What do A and F stand for?

A. F - Reliability cannot be judged, A - Completely Reliable

B. F - Not reliable, A - Usually Reliable

C. F - Not usually reliable, A - Fairly Reliable

D. F - Unreliable, A - Completely Reliable

ANSWER: A

Explanation:

F - Reliability cannot be judged, A - Completely Reliable is correct because XSOAR uses the standard source-reliability scale when assessing incident information and indicators. This scale expresses confidence in the source itself, independently of any separate assessment of the credibility of a specific report or piece of intelligence. “Completely Reliable” is the highest source-reliability designation and is appropriate for a source that has consistently proven dependable. At the other end of the scale, “Reliability cannot be judged” is used where there is insufficient history or corroborating evidence to make a defensible assessment of the source’s reliability. This distinction is important in investigations and automation: a source that cannot yet be assessed is not automatically considered deceptive or inaccurate; rather, XSOAR records that its reliability is unknown. Analysts can use this reliability metadata, together with credibility and contextual evidence, to prioritize triage and make better-informed decisions. Palo Alto Networks documents incident-information assessment and the reliability/credibility model in the Cortex XSOAR Administrator Guide. The underlying source-reliability terminology also follows the established NATO standardization framework used in intelligence reporting.

QUESTION NO: 19

Which component can be part of a load balancing group?

A. Distributed database

B. D2 agent

C. Engine

D. Load balancing server

ANSWER: C

Explanation:

An Engine can be part of a load balancing group in Cortex XSOAR. Engines are lightweight services installed in a customer environment that enable Cortex XSOAR to communicate with resources that are not directly accessible from the Cortex XSOAR tenant, such as internal network devices, systems, and applications. When multiple Engines have the same configuration and are assigned to a load balancing group, Cortex XSOAR can distribute integration commands and automation tasks among the available Engines in that group.

This design provides both scalability and resilience for integrations that require access to internal resources. The platform selects an eligible Engine from the group to execute a task; if an Engine is unavailable, another suitable Engine in the load balancing group can handle subsequent work. To participate effectively, the Engines need compatible connectivity and configuration for the integrations and network destinations they serve. Palo Alto Networks documents Engine deployment,

communication, and load-balancing behavior in the Cortex XSOAR administration documentation: Understand Engines and Configure Engine Groups.