Custom View Settings

Topic 1 - Exam A

Question #1

Topic 1

What does the Cortex XSOAR "Saved by Dbot" widget calculate?

A. amount saved in Dollars according to actions carried out by all users in Cortex XSOAR across all incidents

B. amount saved in Dollars by using Cortex XSOAR instead of other products

C. amount of time saved by each playbook task within an incident

D. amount of time saved by Dbot's machine learning (ML) capabilities

Question #2

Topic 1

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

A. agent management

B. device control

C. agent configuration

D. device customization

Question #3

Topic 1

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

Question #4 — *Topic 1*

An adversary attempts to communicate with malware running on a network in order to control malware activities or to exfiltrate data from the network.
Which Cortex XDR Analytics alert will this activity most likely trigger?

A. uncommon local scheduled task creation

B. malware

C. new administrative behavior

D. DNS Tunneling

Question #5 — *Topic 1*

How do sub-playbooks affect the Incident Context Data?

A. When set to private, task outputs do not automatically get written to the root context.

B. When set to global, sub-playbook tasks do not have access to the root context.

C. When set to global, parallel task execution is allowed.

D. When set to private, task outputs are automatically written to the root context.

Question #6 — *Topic 1*

Which two playbook functionalities allow looping through a group of tasks during playbook execution? (Choose two.)

A. playbook functions

B. sub-playbooks

C. GenericPolling playbooks

D. playbook tasks

Question #7 — *Topic 1*

Cortex XSOAR has extracted a malicious Internet Protocol (IP) address involved in command-and-control (C2) traffic.
What is the best method to block this IP from communicating with endpoints without requiring a configuration change on the firewall?

A. Have XSOAR automatically add the IP address to a threat intelligence management (TIM) malicious IP list to elevate priority of future alerts.

B. Have XSOAR automatically add the IP address to a deny rule in the firewall.

C. Have XSOAR automatically add the IP address to an external dynamic list (EDL) used by the firewall.

D. Have XSOAR automatically create a NetOps ticket requesting a configuration change to the firewall to block the IP.

Question #8 *Topic 1*

Which integration allows searching and displaying Splunk results within Cortex XSOAR?

A. SplunkPY integration

B. Demisto App for Splunk integration

C. XSOAR REST API integration

D. Splunk integration

Question #9 *Topic 1*

Which two types of indicators of compromise (IOCs) are available for creation in Cortex XDR? (Choose two.)

A. registry

B. file path

C. hash

D. hostname

Question #10 *Topic 1*

A Cortex XSOAR customer has a phishing use case in which a playbook has been implemented with one of the steps blocking a malicious URL found in an email reported by one of the users.
What would be the appropriate next step in the playbook?

A. Email the CISO to advise that malicious email was found.

B. Disable the user's email account.

C. Email the user to confirm the reported email was phishing.

D. Change the user's password.

Question #11 *Topic 1*

What allows the use of predetermined Palo Alto Networks roles to assign access rights to Cortex XDR users?

A. role-based access control (RBAC)

B. cloud identity engine (CIE)

C. endpoint groups

D. restrictions security profile

Question #12 *Topic 1*

Which two actions are required to add indicators to the whitelist? (Choose two.)

A. Click "New Whitelisted Indicator" in the Whitelist page.

B. Upload an external file named "whitelist" to the Whitelist page.

C. Upload an external file named "whitelist" to the Indicators page.

D. Select the indicators and click "Delete and Whitelist" in the Indicators page.

Question #13 *Topic 1*

Which playbook feature allows concurrent execution of tasks?

A. parallel tasks

B. automation tasks

C. manual tasks

D. conditional tasks

Question #14 *Topic 1*

Which two Cortex XSOAR incident type features can be customized under Settings > Advanced > Incident Types? (Choose two.)

A. adding new fields to an incident type

B. setting reminders for an incident service level agreement (SLA)

C. defining whether a playbook runs automatically when an incident type is encountered

D. dropping new incidents of the same type that contain similar information

Question #15 *Topic 1*

What are two reasons incident investigation is needed in Cortex XDR? (Choose two.)

A. No solution will stop every attack requiring further investigation of activity.

B. Insider Threats may not be blocked and initial activity may go undetected.

C. Analysts need to acquire forensic artifacts of malware that has been blocked by the XDR agent.

D. Detailed reports are needed for senior management to justify the cost of XDR.

Question #16 *Topic 1*

Which process in the causality chain does the Cortex XDR agent identify as triggering an event sequence?

A. causality group owner

B. chain's alert initiator

C. adversary's remote process

D. relevant shell

Question #17 *Topic 1*

Which two statements apply to widgets? (Choose two.)

A. All widgets are customizable.

B. Dashboards cannot be shared across an organization.

C. A widget can have its own time range that is different from the rest of the dashboard.

D. Some widgets cannot be changed.

Question #18 *Topic 1*

Which source provides data for Cortex XDR?

A. VMware NSX

B. Amazon Alexa rank indicator

C. Cisco ACI

D. Linux endpoints

Question #19 *Topic 1*

Which two manual actions are allowed on War Room entries? (Choose two.)

A. mark as note

B. mark as scheduled entry

C. mark as evidence

D. mark as artifact

Question #20

Topic 1

What does DBot use to score an indicator that has multiple reputation scores?

A. most severe score

B. undefined score

C. average score

D. least severe score

Question #21

Topic 1

Which statement applies to a Cortex XSOAR engine that is part of a load-balancing group?

A. It must be in a load-balancing group with at least three additional members.

B. It must have port 443 open to allow the XSOAR server to establish a connection.

C. It does not appear in the in the engine drop-down menu when configuring an integration instance.

D. It can be used separately as an engine only if directly connected to the XSOAR server.

Question #22

Topic 1

What is the result of creating an exception from an exploit security event?

A. Administrators are exempt from generating alerts for 24 hours.

B. Process from WildFire analysis is whitelisted.

C. Triggered exploit protection module (EPM) for the host and process involved is disabled.

D. User is exempt from generating events for 24 hours.

Question #23

Topic 1

Which two filter operators are available in Cortex XDR? (Choose two.)

A. Is Contained By

B. < >

C. =

D. Contains

Question #24 *Topic 1*

Which attack method is a result of techniques designed to gain access through vulnerabilities in the code of an operating system (OS) or application?

A. exploit

B. malware

C. phishing

D. ransomware

Question #25 *Topic 1*

What are two capabilities of a War Room? (Choose two.)

A. create widgets for an investigation

B. create playbooks for orchestration

C. act as an audit trail for an investigation

D. run ad-hoc automation commands

Question #26 *Topic 1*

On a multi-tenanted v6.2 Cortex XSOAR server, which path leads to the server.log for "Tenant1"?

A. /var/log/demisto/acc_Tenant1/server.log

B. /var/log/demisto/Tenant1/server.log

C. /var/lib/demisto/acc_Tenant1/server.log

D. /var/lib/demisto/server.log

Question #27 *Topic 1*

What is used to display only file entries in a War Room?

A. !files from War Room CLI

B. incident files section in layout builder

C. files and attachments filters

D. /files from War Room CLI

Question #28 *Topic 1*

Which two areas of Cortex XDR are used for threat hunting activities? (Choose two.)

A. indicators of compromise (IOC) rules

B. query builder

C. live terminal

D. host insights module

Question #29 *Topic 1*

Where can all the relevant incidents for an indicator be viewed?

A. Related Indicators column in incident screen

B. Linked Incidents column in indicator screen

C. Linked Indicators column in incident screen

D. Related Incidents column in indicator screen

Question #30 *Topic 1*

Which statement applies to the malware protection flow in Cortex XDR Prevent?

A. Local static analysis happens before a WildFire verdict check.

B. In the final step, the block list is verified.

C. A trusted signed file is exempt from local static analysis.

D. Hash comparisons come after local static analysis.

Question #31 *Topic 1*

When initiated, which Cortex XDR capability allows immediate termination of the process or whole process tree on an anomalous process discovered during investigation of a security event?

A. file explorer

B. log stitching

C. live sensors

D. live terminal

Question #32 *Topic 1*

What is the size of the free Cortex Data Lake instance provided to a customer who has activated a TMS tenant, but has not purchased a Cortex Data Lake instance?

A. 10 GB

B. 1 TB

C. 10 TB

D. 100 GB

Question #33 *Topic 1*

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.

Question #34 *Topic 1*

Which two types of indicators of compromise (IOCs) are available for creation in Cortex XDR? (Choose two.)

A. registry entry

B. Internet Protocol (IP)

C. domain

D. endpoint hostname

Question #35 *Topic 1*

What is a benefit offered by Cortex XSOAR?

A. It has the ability to customize the extensible platform to scale to business needs.

B. It allows the consolidation of multiple point products into a single integrated service.

C. It provides holistic protection across hosts and containers throughout the application lifecycle.

D. It enables an end-to-end view of everything in the customer environment that affects digital employee productivity.

Question #36 *Topic 1*

Which action allows Cortex XSOAR to access Docker in an air-gapped environment where the Docker page was manually installed after the Cortex XSOAR installation?

A. Create a "docker" group and add the "Cortex XSOAR" or "demisto" user to this group.

B. Create a "Cortex XSOAR" or "demisto" group and add the "docker" user to this group.

C. Enable the Docker service.

D. Disable the Cortex XSOAR service.

Question #37 *Topic 1*

The Cortex XDR management service requires which other Palo Alto Networks product?

A. Directory Sync

B. Cortex Data Lake

C. Panorama

D. Cortex XSOAR

Question #38 *Topic 1*

Which command-line interface (CLI) query would retrieve the last three Splunk events?

A. !search using=splunk_instance_1 query="* | last 3"

B. !search using=splunk_instance_1 query="* | 3"

C. !query using=splunk_instance_1 query="* | last 3"

D. !search using=splunk_instance_1 query="* | head 3"

Question #39 *Topic 1*

Which Linux OS command will manually load Docker images onto the Cortex XSOAR server in an air-gapped environment?

A. sudo repoquery -a --installed

B. sudo demistoserver-x.x-xxxx.sh -- -tools=load

C. sudo docker ps load

D. sudo docker load -i YOUR_DOCKER_FILE.tar

Question #40 *Topic 1*

Which solution profiles network behavior metadata, not payloads and files, allowing effective operation regardless of encrypted or unencrypted communication protocols, like HTTPS?

A. endpoint protection platform (EPP)

B. Security Information and Event Management (SIEM)

C. endpoint detection and response (EDR)

D. Network Detection and Response (NDR)

Question #41 *Topic 1*

A customer wants the main Cortex XSOAR server installed in one site and wants to integrate with three other technologies in a second site.
What communications are required between the two sites if the customer wants to install a Cortex XSOAR engine in the second site?

A. The Cortex XSOAR server at the first site must be able to initiate a connection to the Cortex XSOAR engine at the second site.

B. All connectivity is initiated from the Cortex XSOAR server on the first site via a managed cloud proxy.

C. Dedicated site-to-site virtual private network (VPN) is required for the Cortex XSOAR server at the first site to initiate a connection to the Cortex XSOAR engine at the second site.

D. The Cortex XSOAR engine at the first site must be able to initiate a connection to the Cortex XSOAR server at the second site.

Question #42 *Topic 1*

Which two methods does the Cortex XDR agent use to identify malware during a scheduled scan? (Choose two.)

A. WildFire hash comparison

B. heuristic analysis

C. signature comparison

D. dynamic analysis

Question #43 *Topic 1*

Why is reputation scoring important in the Threat Intelligence Module of Cortex XSOAR?

A. It allows for easy comparison between open-source intelligence and paid services.

B. It deconflicts prioritization when two vendors give different scores for the same indicator.

C. It provides a mathematical model for combining scores from multiple vendors.

D. It helps identify threat intelligence vendors with substandard content.