Custom View Settings

Topic 1 - Exam A

Question #1 *Topic 1*

Phishing belongs which of the following MITRE ATT&CK tactics?

A. Initial Access, Persistence

B. Persistence, Command and Control

C. Reconnaissance, Persistence

D. Reconnaissance, Initial Access

Question #2 *Topic 1*

When creating a BIOC rule, which XQL query can be used?

A. dataset = xdr_data
| filter event_sub_type = PROCESS_START and
action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"

B. dataset = xdr_data
| filter event_type = PROCESS and
event_sub_type = PROCESS_START and
action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"

C. dataset = xdr_data
| filter action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"
| fields action_process_image

D. dataset = xdr_data
| filter event_behavior = true
event_sub_type = PROCESS_START and
action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"

Question #3 *Topic 1*

Which built-in dashboard would be the best option for an executive, if they were looking for the Mean Time to Resolution (MTTR) metric?

A. Security Manager Dashboard

B. Data Ingestion Dashboard

C. Security Admin Dashboard

D. Incident Management Dashboard

Question #4 *Topic 1*

What are two purposes of “Respond to Malicious Causality Chains” in a Cortex XDR Windows Malware profile? (Choose two.)

A. Automatically close the connections involved in malicious traffic.

B. Automatically kill the processes involved in malicious activity.

C. Automatically terminate the threads involved in malicious activity.

D. Automatically block the IP addresses involved in malicious traffic.

Question #5 *Topic 1*

When creating a custom XQL query in a dashboard, how would a user save that XQL query to the Widget Library?

A. Click the three dots on the widget and then choose “Save” and this will link the query to the Widget Library.

B. This isn’t supported, you have to exit the dashboard and go into the Widget Library first to create it.

C. Click on “Save to Action Center” in the dashboard and you will be prompted to give the query a name and description.

D. Click on “Save to Widget Library” in the dashboard and you will be prompted to give the query a name and description.

Question #6 *Topic 1*

What license would be required for ingesting external logs from various vendors?

A. Cortex XDR Pro per Endpoint

B. Cortex XDR Vendor Agnostic Pro

C. Cortex XDR Pro per TB

D. Cortex XDR Cloud per Host

Question #7 *Topic 1*

An attacker tries to load dynamic libraries on macOS from an unsecure location. Which Cortex XDR module can prevent this attack?

A. DDL Security

B. Hot Patch Protection

C. Kernel Integrity Monitor (KIM)

D. Dylib Hijacking

Question #8 *Topic 1*

What is the purpose of the Unit 42 team?

A. Unit 42 is responsible for automation and orchestration of products

B. Unit 42 is responsible for the configuration optimization of the Cortex XDR server

C. Unit 42 is responsible for threat research, malware analysis and threat hunting

D. Unit 42 is responsible for the rapid deployment of Cortex XDR agents

Question #9 *Topic 1*

Which Type of IOC can you define in Cortex XDR?

A. destination port

B. e-mail address

C. full path

D. App-ID

Question #10 *Topic 1*

When viewing the incident directly, what is the “assigned to” field value of a new Incident that was just reported to Cortex?

A. Pending

B. It is blank

C. Unassigned

D. New

Question #11 *Topic 1*

In incident-related widgets, how would you filter the display to only show incidents that were “starred”?

A. Create a custom XQL widget

B. This is not currently supported

C. Create a custom report and filter on starred incidents

D. Click the star in the widget

Question #12 *Topic 1*

Where would you view the WildFire report in an incident?

A. next to relevant Key Artifacts in the incidents details page

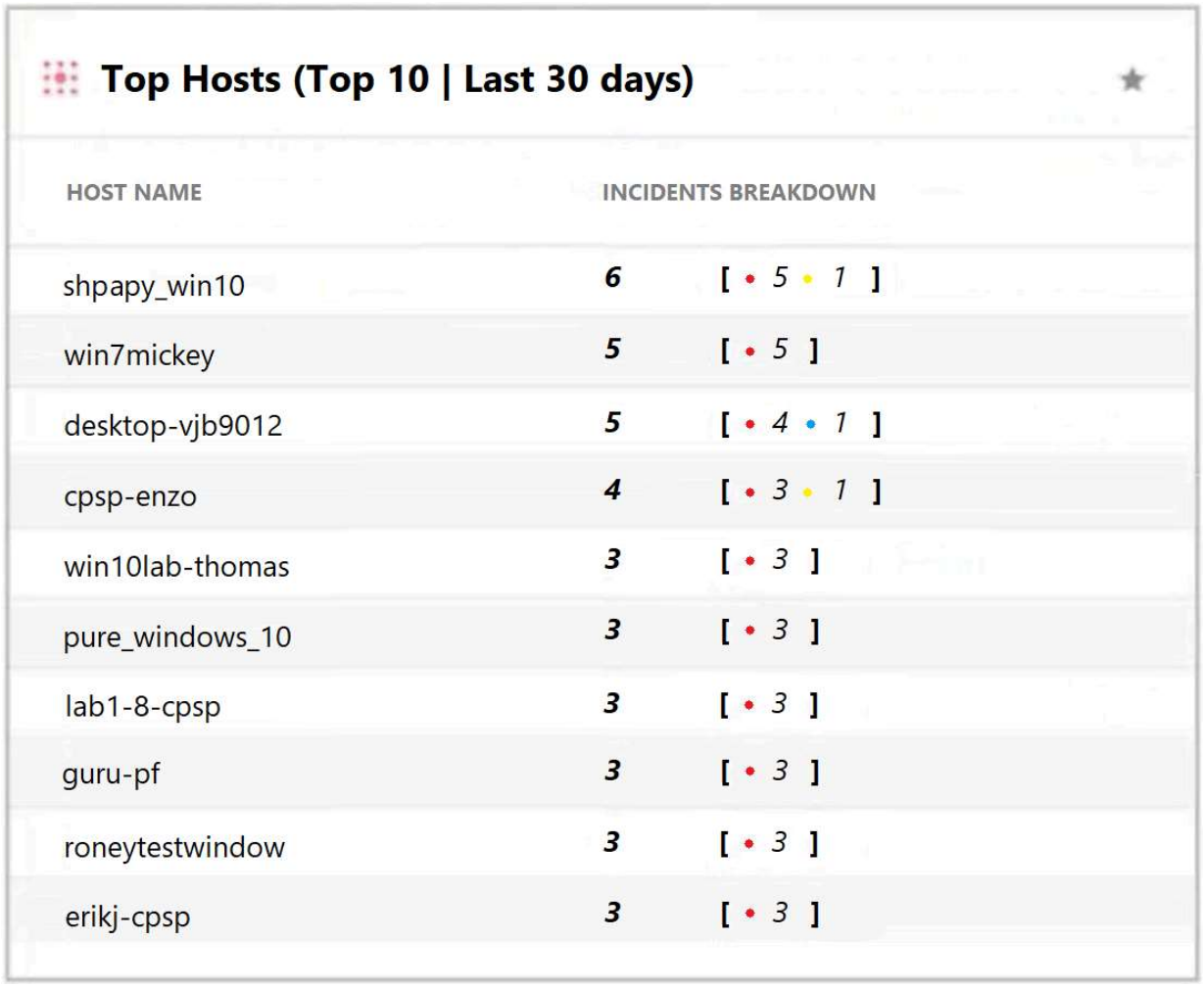
B. under Response --> Action Center

C. under the gear icon –> Agent Audit Logs

D. on the HUB page at apps.paloaltonetworks.com

Question #13 *Topic 1*

What does the following output tell us?



A. There is one low severity incident.

B. Host shpapy_win10 had the most vulnerabilities.

C. There is one informational severity alert.

D. This is an actual output of the Top 10 hosts with the most malware.

Question #14 *Topic 1*

Which engine, of the following, in Cortex XDR determines the most relevant artifacts in each alert and aggregates all alerts related to an event into an incident?

A. Sensor Engine

B. Causality Analysis Engine

C. Log Stitching Engine

D. Causality Chain Engine

Question #15 *Topic 1*

Which type of BIOC rule is currently available in Cortex XDR?

A. Threat Actor

B. Discovery

C. Network

D. Dropper

Question #16 *Topic 1*

In Windows and macOS you need to prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer. What is one way to add an exception for the singer?

A. In the Restrictions Profile, add the file name and path to the Executable Files allow list.

B. Create a new rule exception and use the singer as the characteristic.

C. Add the signer to the allow list in the malware profile.

D. Add the signer to the allow list under the action center page.

Question #17 *Topic 1*

As a Malware Analyst working with Cortex XDR you notice an alert suggesting that there was a prevented attempt to download Cobalt Strike on one of your servers. Days later, you learn about a massive ongoing supply chain attack. Using Cortex XDR you recognize that your server was compromised by the attack and that Cortex XDR prevented it. What steps can you take to ensure that the same protection is extended to all your servers?

A. Create Behavioral Threat Protection (BTP) rules to recognize and prevent the activity.

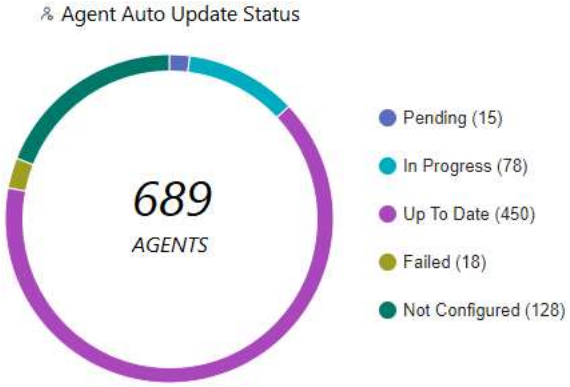
B. Enable DLL Protection on all servers but there might be some false positives.

C. Create IOCs of the malicious files you have found to prevent their execution.

D. Enable Behavioral Threat Protection (BTP) with cytool to prevent the attack from spreading.

Question #18 *Topic 1*

Which statement is true based on the following Agent Auto Upgrade widget?



A. There are a total of 689 Up To Date agents.

B. Agent Auto Upgrade was enabled but not on all endpoints.

C. Agent Auto Upgrade has not been enabled.

D. There are more agents in Pending status than In Progress status.

Question #19 *Topic 1*

What is the purpose of targeting software vendors in a supply-chain attack?

A. to take advantage of a trusted software delivery method.

B. to steal users' login credentials.

C. to access source code.

D. to report Zero-day vulnerabilities.

Question #20 *Topic 1*

What is the standard installation disk space recommended to install a Broker VM?

A. 1GB disk space

B. 2GB disk space

C. 512GB disk space

D. 256GB disk space

Question #21 *Topic 1*

Where can SHA256 hash values be used in Cortex XDR Malware Protection Profiles?

A. in the macOS Malware Protection Profile to indicate allowed signers

B. in the Linux Malware Protection Profile to indicate allowed Java libraries

C. SHA256 hashes cannot be used in Cortex XDR Malware Protection Profiles

D. in the Windows Malware Protection Profile to indicate allowed executables

Question #22 *Topic 1*

How does Cortex XDR agent for Windows prevent ransomware attacks from compromising the file system?

A. by encrypting the disk first.

B. by utilizing decoy Files.

C. by retrieving the encryption key.

D. by patching vulnerable applications.

Question #23 *Topic 1*

What functionality of the Broker VM would you use to ingest third-party firewall logs to the Cortex Data Lake?

A. Netflow Collector

B. Syslog Collector

C. DB Collector

D. Pathfinder

Question #24 *Topic 1*

In the deployment of which Broker VM applet are you required to install a strong cipher SHA256-based SSL certificate?

A. Agent Proxy

B. Agent Installer and Content Caching

C. Syslog Collector

D. CSV Collector

Question #25 *Topic 1*

When is the wss (WebSocket Secure) protocol used?

A. when the Cortex XDR agent downloads new security content

B. when the Cortex XDR agent uploads alert data

C. when the Cortex XDR agent connects to WildFire to upload files for analysis

D. when the Cortex XDR agent establishes a bidirectional communication channel

Question #26 *Topic 1*

With a Cortex XDR Prevent license, which objects are considered to be sensors?

A. Syslog servers

B. Third-Party security devices

C. Cortex XDR agents

D. Palo Alto Networks Next-Generation Firewalls

Question #27 *Topic 1*

Which license is required when deploying Cortex XDR agent on Kubernetes Clusters as a DaemonSet?

A. Cortex XDR Pro per TB

B. Host Insights

C. Cortex XDR Pro per Endpoint

D. Cortex XDR Cloud per Host

Question #28 *Topic 1*

What kind of the threat typically encrypts user files?

A. ransomware

B. SQL injection attacks

C. Zero-day exploits

D. supply-chain attacks

Question #29 *Topic 1*

When using the “File Search and Destroy” feature, which of the following search hash type is supported?

A. SHA256 hash of the file

B. AES256 hash of the file

C. MD5 hash of the file

D. SHA1 hash of the file

Question #30 *Topic 1*

If you have an isolated network that is prevented from connecting to the Cortex Data Lake, which type of Broker VM setup can you use to facilitate the communication?

A. Broker VM Pathfinder

B. Local Agent Proxy

C. Local Agent Installer and Content Caching

D. Broker VM Syslog Collector

Question #31 *Topic 1*

What is by far the most common tactic used by ransomware to shut down a victim’s operation?

A. preventing the victim from being able to access APIs to cripple infrastructure

B. denying traffic out of the victims network until payment is received

C. restricting access to administrative accounts to the victim

D. encrypting certain files to prevent access by the victim

Question #32 *Topic 1*

Cortex XDR Analytics can alert when detecting activity matching the following MITRE ATT&CKTM techniques.

A. Exfiltration, Command and Control, Collection

B. Exfiltration, Command and Control, Privilege Escalation

C. Exfiltration, Command and Control, Impact

D. Exfiltration, Command and Control, Lateral Movement

Question #33 *Topic 1*

When selecting multiple Incidents at a time, what options are available from the menu when a user right-clicks the incidents? (Choose two.)

A. Assign incidents to an analyst in bulk.

B. Change the status of multiple incidents.

C. Investigate several Incidents at once.

D. Delete the selected Incidents.

Question #34 *Topic 1*

A file is identified as malware by the Local Analysis module whereas WildFire verdict is Benign, Assuming WildFire is accurate. Which statement is correct for the incident?

A. It is true positive.

B. It is false positive.

C. It is a false negative.

D. It is true negative.

Question #35 *Topic 1*

What is the outcome of creating and implementing an alert exclusion?

A. The Cortex XDR agent will allow the process that was blocked to run on the endpoint.

B. The Cortex XDR console will hide those alerts.

C. The Cortex XDR agent will not create an alert for this event in the future.

D. The Cortex XDR console will delete those alerts and block ingestion of them in the future.

Question #36 *Topic 1*

Which statement is true for Application Exploits and Kernel Exploits?

A. The ultimate goal of any exploit is to reach the application.

B. Kernel exploits are easier to prevent then application exploits.

C. The ultimate goal of any exploit is to reach the kernel.

D. Application exploits leverage kernel vulnerability.

Question #37 *Topic 1*

To create a BIOC rule with XQL query you must at a minimum filter on which field in order for it to be a valid BIOC rule?

A. causality_chain

B. endpoint_name

C. threat_event

D. event_type

Question #38 *Topic 1*

Which of the following is an example of a successful exploit?

A. connecting unknown media to an endpoint that copied malware due to Autorun.

B. a user executing code which takes advantage of a vulnerability on a local service.

C. identifying vulnerable services on a server.

D. executing a process executable for well-known and signed software.

Question #39 *Topic 1*

Which of the following represents the correct relation of alerts to incidents?

A. Only alerts with the same host are grouped together into one Incident in a given time frame.

B. Alerts that occur within a three hour time frame are grouped together into one Incident.

C. Alerts with same causality chains that occur within a given time frame are grouped together into an Incident.

D. Every alert creates a new Incident.

Question #40 *Topic 1*

Which of the following protection modules is checked first in the Cortex XDR Windows agent malware protection flow?

A. Hash Verdict Determination

B. Behavioral Threat Protection

C. Restriction Policy

D. Child Process Protection

Question #41 *Topic 1*

While working the alerts involved in a Cortex XDR incident, an analyst has found that every alert in this incident requires an exclusion. What will the Cortex XDR console automatically do to this incident if all alerts contained have exclusions?

A. mark the incident as Unresolved

B. create a BIOC rule excluding this behavior

C. create an exception to prevent future false positives

D. mark the incident as Resolved – False Positive

Question #42 *Topic 1*

Network attacks follow predictable patterns. If you interfere with any portion of this pattern, the attack will be neutralized. Which of the following statements is correct?

A. Cortex XDR Analytics allows to interfere with the pattern as soon as it is observed on the firewall.

B. Cortex XDR Analytics does not interfere with the pattern as soon as it is observed on the endpoint.

C. Cortex XDR Analytics does not have to interfere with the pattern as soon as it is observed on the endpoint in order to prevent the attack.

D. Cortex XDR Analytics allows to interfere with the pattern as soon as it is observed on the endpoint.

Question #43 *Topic 1*

After scan, how does file quarantine function work on an endpoint?

A. Quarantine takes ownership of the files and folders and prevents execution through access control.

B. Quarantine disables the network adapters and locks down access preventing any communications with the endpoint.

C. Quarantine removes a specific file from its location on a local or removable drive to a protected folder and prevents it from being executed.

D. Quarantine prevents an endpoint from communicating with anything besides the listed exceptions in the agent profile and Cortex XDR.

Question #44 *Topic 1*

Which two types of exception profiles you can create in Cortex XDR? (Choose two.)

A. exception profiles that apply to specific endpoints

B. agent exception profiles that apply to specific endpoints

C. global exception profiles that apply to all endpoints

D. role-based profiles that apply to specific endpoints

Question #45 *Topic 1*

Which profiles can the user use to configure malware protection in the Cortex XDR console?

A. Malware Protection profile

B. Malware profile

C. Malware Detection profile

D. Anti-Malware profile

Question #46 *Topic 1*

Which module provides the best visibility to view vulnerabilities?

A. Live Terminal module

B. Device Control Violations module

C. Host Insights module

D. Forensics module

Question #47 *Topic 1*

Which of the following is NOT a precanned script provided by Palo Alto Networks?

A. delete_file

B. quarantine_file

C. process_kill_name

D. list_directories

Question #48 *Topic 1*

Live Terminal uses which type of protocol to communicate with the agent on the endpoint?

A. NetBIOS over TCP

B. WebSocket

C. UDP and a random port

D. TCP, over port 80

Question #49 *Topic 1*

You can star security events in which two ways? (Choose two.)

A. Create an alert-starring configuration.

B. Create an Incident-starring configuration.

C. Manually star an alert.

D. Manually star an Incident.

Question #50 *Topic 1*

Where would you go to add an exception to exclude a specific file hash from examination by the Malware profile for a Windows endpoint?

A. Find the Malware profile attached to the endpoint, Under Portable Executable and DLL Examination add the hash to the allow list.

B. From the rules menu select new exception, fill out the criteria, choose the scope to apply it to, hit save.

C. Find the exceptions profile attached to the endpoint, under process exceptions select local analysis, paste the hash and save.

D. In the Action Center, choose Allow list, select new action, select add to allow list, add your hash to the list, and apply it.

Question #51 *Topic 1*

As a Malware Analyst working with Cortex XDR you notice an alert suggesting that there was a prevented attempt to open a malicious Word document. You learn from the WildFire report and AutoFocus that this document is known to have been used in Phishing campaigns since 2018. What steps can you take to ensure that the same document is not opened by other users in your organization protected by the Cortex XDR agent?

A. Enable DLL Protection on all endpoints but there might be some false positives.

B. Create Behavioral Threat Protection (BTP) rules to recognize and prevent the activity.

C. No step is required because Cortex shares IOCs with our fellow Cyber Threat Alliance members.

D. No step is required because the malicious document is already stopped.

Question #52 *Topic 1*

When investigating security events, which feature in Cortex XDR is useful for reverting the changes on the endpoint?

A. Remediation Automation

B. Machine Remediation

C. Automatic Remediation

D. Remediation Suggestions

Question #53 *Topic 1*

What is the purpose of the Cortex Data Lake?

A. a local storage facility where your logs and alert data can be aggregated

B. a cloud-based storage facility where your firewall logs are stored

C. the interface between firewalls and the Cortex XDR agents

D. the workspace for your Cortex XDR agents to detonate potential malware files

Question #54 *Topic 1*

When creating a scheduled report which is not an option?

A. Run weekly on a certain day and time.

B. Run quarterly on a certain day and time.

C. Run monthly on a certain day and time.

D. Run daily at a certain time (selectable hours and minutes).

Question #55 *Topic 1*

Which statement regarding scripts in Cortex XDR is true?

A. Any version of Python script can be run.

B. The level of risk is assigned to the script upon import.

C. Any script can be imported including Visual Basic (VB) scripts.

D. The script is run on the machine uploading the script to ensure that it is operational.

Question #56 *Topic 1*

What is the function of WildFire for Cortex XDR?

A. WildFire runs in the cloud and analyses alert data from the XDR agent to check for behavioural threats.

B. WildFire is the engine that runs on the local agent and determines whether behavioural threats are occurring on the endpoint.

C. WildFire accepts and analyses a sample to provide a verdict.

D. WildFire runs entirely on the agent to quickly analyse samples and provide a verdict.

Question #57 *Topic 1*

A Linux endpoint with a Cortex XDR Pro per Endpoint license and Enhanced Endpoint Data enabled has reported malicious activity, resulting in the creation of a file that you wish to delete. Which action could you take to delete the file?

A. Manually remediate the problem on the endpoint in question.

B. Open X2go from the Cortex XDR console and delete the file via X2go.

C. Initiate Remediate Suggestions to automatically delete the file.

D. Open an NFS connection from the Cortex XDR console and delete the file.

Question #58 *Topic 1*

Which of the following best defines the Windows Registry as used by the Cortex XDR agent?

A. a hierarchical database that stores settings for the operating system and for applications

B. a system of files used by the operating system to commit memory that exceeds the available hardware resources. Also known as the "swap"

C. a central system, available via the internet, for registering officially licensed versions of software to prove ownership

D. a ledger for maintaining accurate and up-to-date information on total disk usage and disk space remaining available to the operating system

Question #59 *Topic 1*

Which statement best describes how Behavioral Threat Protection (BTP) works?

A. BTP injects into known vulnerable processes to detect malicious activity.

B. BTP runs on the Cortex XDR and distributes behavioral signatures to all agents.

C. BTP matches EDR data with rules provided by Cortex XDR.

D. BTP uses machine Learning to recognize malicious activity even if it is not known.

Question #60 *Topic 1*

Which of the following paths will successfully activate Remediation Suggestions?

A. Alerts Table > Right-click on a process node > Remediation Suggestions

B. Incident View > Actions > Remediation Suggestions

C. Causality View > Actions > Remediation Suggestions

D. Alerts Table > Right-click on an alert > Remediation Suggestions

Question #61 *Topic 1*

In Cortex XDR management console scheduled reports can be forwarded to which of the following applications/services?

A. Service Now

B. Slack

C. Salesforce

D. Jira

Question #62 *Topic 1*

Which type of IOC can you define in Cortex XDR?

A. Source port

B. Destination IP Address

C. Destination IP Address:Destination

D. Source IP Address

Question #63 *Topic 1*

What is the action taken out by Managed Threat Hunting team for Zero Day Exploits?

A. MTH runs queries and investigative actions and no further action is taken.

B. MTH researches for threats in the logs and reports to engineering.

C. MTH researches for threats in the tenant and generates a report with the findings.

D. MTH pushes content updates to prevent against the zero day exploits.

Question #64 *Topic 1*

What is an example of an attack vector for ransomware?

A. A URL filtering feature enabled on a firewall

B. Phishing emails containing malicious attachments

C. Performing DNS queries for suspicious domains

D. Performing SSL Decryption on an endpoint