TESTPASSPORT

ÜBUNGSFRAGEN

HOCHWERTIGE LERNRESSOURCEN

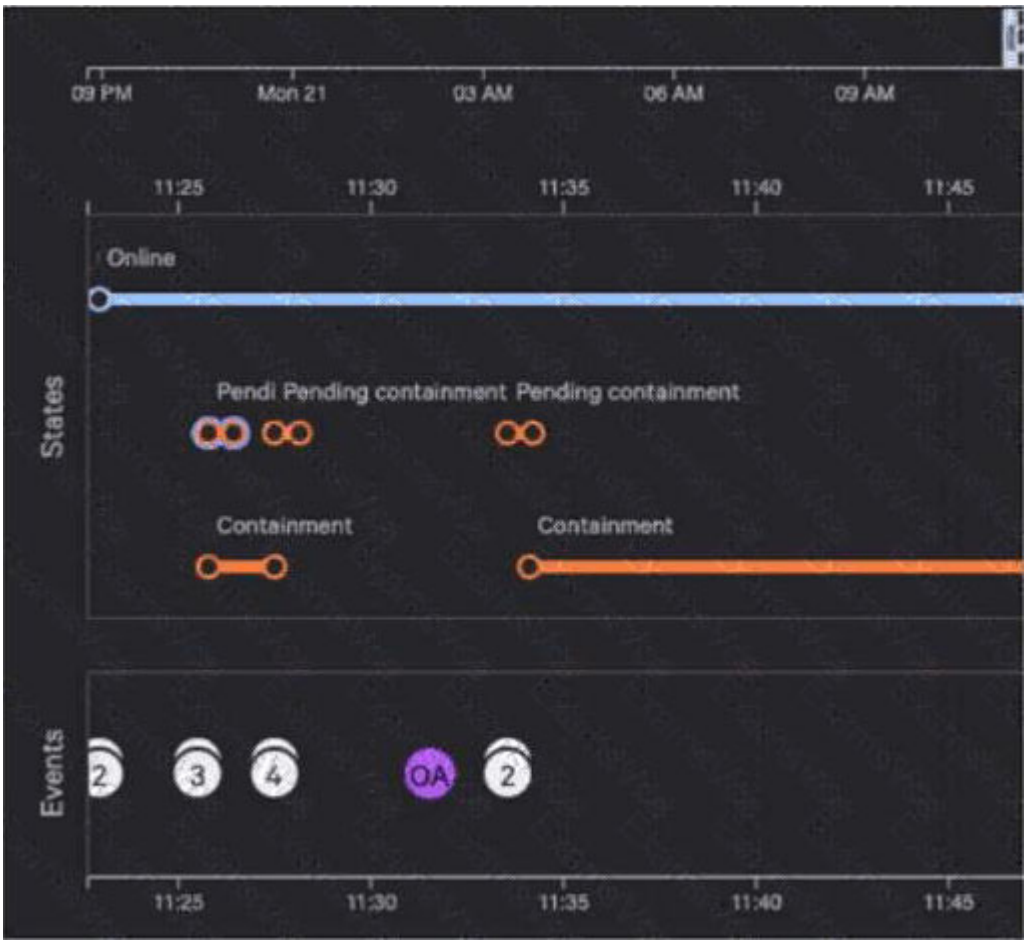
Exam : **CCFH-202b**

Title : CrowdStrike Certified Falcon Hunter

Version : DEMO

1.What can a hunter add at the end of a search string in Advanced Event Search to identify outliers when quantifying the results?
A. | groupBy()
B. | eval()
C. | sample()
D. | stats()
Answer: D
Explanation:
In the realm of Hunting Analytics, the ability to quantify data is the first step toward identifying outliers—the "needles in the haystack." The stats() function in Advanced Event Search (LogScale) is the most versatile tool for this purpose. While groupBy() is used to organize data into buckets, stats() is required to perform mathematical aggregations such as count(), sum(), avg(), or stdDev().
To identify outliers, a hunter typically wants to see which events occur with the lowest frequency (Least-Frequency Analysis) or which values deviate significantly from the mean. By appending | stats(count(), function=[...]) to a query, the analyst transforms raw event logs into a statistical summary.
For example, a hunter might use stats() to count the number of unique external IP connections per process; a process that normally connects to one IP but suddenly c onnects to 500 would stand out as a clear outlier. This quantification is what allows a hunter to move from "searching" to "analyzing." While eval() is used for calculating new fields and sample() is used for performance testing on large datasets, stats() provides the numerical foundation necessary for sophisticated behavioral baselining and the detection of anomalous activity that doesn't trigger standard signature-based alerts.

2.Refer to the image.



Why are there six pending containment events?

A. When requesting containment of a device, there is one event to contain the host by Agent ID and another event to contain by Mac Address

B. When requesting containment of a device, there is one event for checking of the current host state and another corresponding to the change request

C. When requesting containment of a device, there is one event to contain the host by Agent ID and another event to contain by Host Name

D. When requesting containment of a device, there is one event for the change request and another corresponding to the completed status of the request

Answer: B

Explanation:

In the Falcon platform's Host Investigate dashboard, the "States" timeline provides a granular visual history of administrative and system-level transitions for an endpoint. When a network containment action is initiated, the platform must track the lifecycle of that request from the console to the sensor. According to Falcon documentation, for every containment request made by an analyst, the system generates two specific sub-events that are tracked in the "Pending containment" row.

The first event involves the cloud's process of checking the current host state to verify the baseline connectivity and sensor status. The second event corresponds to the actual change request, which is the command sent to the Falcon sensor to apply the network isolation filters (blocking all traffic except for communication with the CrowdStrike cloud).

As seen in the provided image, there are three distinct "bundles" or attempts of containment activity

shown. Because each of these three attempts is comprised of these two mandatory sub-events (the check and the request), the timeline displays a total of six icons. This level of detail allows a hunter to troubleshoot containment issues; for instance, if the check event succeeds but the change request remains pending, it could indicate a communication lag or a tamper-protection mechanism on the endpoint. Once the sensor successfully applies the isolation and sends an acknowledgment back to the cloud, the state transitions from "Pending" to the solid "Containment" line seen lower in the timeline.

3.You have an Advanced Event Search query created to identify suspicious PowerShell usage and want to display the results in a dashboard.
How can this query be displayed in a dashboard?
A. Save the query as a dashboard widget
B. Create a scheduled workflow to execute the query
C. Save the query as a saved search
D. Configure a scheduled search with the query
Answer: A
Explanation:
Within the Falcon platform's Reports and References ecosystem, the transition from a live investigation to a persistent monitoring view is handled through the dashboarding engine. When a hunter crafts a high-fidelity query in Advanced Event Search (powered by LogScale), the primary method for visual persistence is to "Save as Dashboard Widget." This process allows the analyst to take the live telemetry results and pin them to a new or existing dashboard, choosing a visualization type (such as a table, line chart, or gauge) that best represents the data.
While "Saved Searches" are useful for quickly re-running a specific query manually, they do not provide the real-time visual "at-a-glance" capability that a dashboard offers. Scheduled searches and workflows are more aligned with automated alerting or external data exports rather than internal visualization. By saving the query as a widget, the hunter ensures that the suspicious PowerShell activity is tracked continuously. This is essential for maintaining situational awareness across the environment. Once a widget is created, it can be filtered by time or host group, allowing different teams to utilize the same underlying logic to monitor their specific areas of responsibility. This workflow is a core component of building a custom SOC (Security Operations Center) visibility layer tailored to the unique threats of an organization.

4.An attacker created a scheduled task which executes a remote management application.
Which MITRE ATT
& CK Matrix for Enterprise stage is this an example of?
A. Persistence
B. Lateral Movement
C. Privilege Escalation
D. Gaining Access
Answer: A
Explanation:
In the context of the MITRE ATT & CK Framework, the creation of a scheduled task is a quintessential technique within the Persistence tactic (specifically T1053). Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions

that could cut off their flow. By scheduling a task to execute a remote management application, the attacker ensures that their connection to the compromised host is maintained automatically without requiring manual re-exploitation.
Within the Falcon platform, hunters monitor for this behavior by analyzing events such as ScheduledTaskRegistered or process executions originating from taskeng.exe or schtasks.exe. While scheduled tasks can occasionally be used for Privilege Escalation (if the task runs with SYSTEM privileges) or Execution, the primary goal of creating a permanent task for a management application is to ensure long-term, stable access to the environment. Effective hunting methodology involves pivoting from the detection of a new scheduled task to identifying the source process that created it. This allows the analyst to determine if the task was part of a legitimate administrative action or an unauthorized persistence mechanism designed to facilitate further malicious activity, such as data exfiltration or internal reconnaissance.

5.You identify an instance of a user in your environment utilizing a Cloudflared tunnel daemon, resulting in unusual command line activity.
What steps would you take to determine if the unusual activity is malicious or legitimate?
A. Block all instances of Cloudflared in your environment and perform a forensic investigation into the host
B. Create a forensic image of the hard drive and analyze it for indicators of compromise
C. Immediately network contain the host and perform a forensic investigation into the host
D. Review the specific commands associated and compare them with known legitimate use cases to confirm if patterns align with normal operations
Answer: D
Explanation:
When a hunter encounters a "dual-use" tool like Cloudflared, the investigation must be approached with nuance. Cloudflared (and similar tunneling tools) can be used legitimately by DevOps or IT teams for secure remote access, but they are also frequently used by adversaries for Command and Control (C2) and data exfiltration because they can bypass traditional firewall rules by tunneling traffic over HTTPS. The first step in Detection Analysis should always be to gather context before taking disruptive actions like network containment or blocking (which could break legitimate business processes). By reviewing the CommandLine arguments in the Falcon Process Timeline, the hunter can see how the tunnel was configured. Are the commands consistent with documented IT procedures? Is the tunnel connecting to a known corporate Cloudflare account, or an anonymous one? Comparing this activity against a baseline of "normal operations" for that specific user or department is essential. If the commands show the tunnel being used to expose a sensitive local port (like RDP or SSH) to the public internet under a non-IT account, the suspicion level increases. This measured approach—investigating the "What" and "Why" before reacting—ensures that the hunter provides accurate triage and avoids unnecessary downtime while still maintaining a high security posture.