IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **CCFR-201**

Title : CrowdStrike Certified Falcon Responder

Version : DEMO

1.After pivoting to an event search from a detection, you locate the ProcessRollup2 event.
Which two field values are you required to obtain to perform a Process Timeline search so you can determine what the process was doing?
A. SHA256 and TargetProcessId_decimal
B. SHA256 and ParentProcessId_decimal
C. aid and ParentProcessId_decimal
D. aid and TargetProcessId_decimal
Answer: D
Explanation:
According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Process Timeline search requires two parameters: aid (agent ID) and TargetProcessId_decimal (the decimal value of the process ID). These fields can be obtained from the ProcessRollup2 event, which contains information about processes that have executed on a host1.

2.The function of Machine Learning Exclusions is to_____.
A. stop all detections for a specific pattern ID
B. stop all sensor data collection for the matching path(s)
C. Stop all Machine Learning Preventions but a detection will still be generated and files will still be uploaded to the CrowdStrike Cloud
D. stop all ML-based detections and preventions for the matching path(s) and/or stop files from being uploaded to the CrowdStrike Cloud
Answer: C
Explanation:
Stop all Machine Learning Preventions but a detection will still be generated and files will still be uploaded to the CrowdStrike Cloud: This option is aligned with the primary purpose of ML exclusions. It suggests that while the system will still detect and record the events (and upload files for analysis), it will not take automatic preventive actions based on machine learning decisions for the excluded paths or patterns.
This setting is useful for scenarios where certain processes or activities are known to be safe in a particular environment and should not trigger preventive actions, even though they might be flagged by ML algorithms.

3.What happens when you create a Sensor Visibility Exclusion for a trusted file path?
A. It excludes host information from Detections and Incidents generated within that file path location
B. It prevents file uploads to the CrowdStrike cloud from that file path
C. It excludes sensor monitoring and event collection for the trusted file path
D. It disables detection generation from that path, however the sensor can still perform prevention actions
Answer: C
Explanation:
According to the CrowdStrike Falcon® Data Replicator (FDR) Add-on for Splunk Guide, Sensor Visibility Exclusions allow you to exclude certain files or directories from being monitored by the CrowdStrike sensor, which can reduce noise and improve performance2. This means that no events will be collected or sent to the CrowdStrike Cloud for those files or directories2.

4.What types of events are returned by a Process Timeline?
A. Only detection events
B. All cloudable events
C. Only process events
D. Only network events
Answer: C
Explanation:
Only process events: This option suggests that the timeline focuses exclusively on events directly related to the process in question. This would typically include events like process creation, modification, interactions with other processes, and termination – essentially tracking the life cycle of the process. This ensures that the timeline provides a focused and detailed view of the specific process's activities and interactions, which is essential for thorough analysis and investigation in cybersecurity contexts.

5.What is the difference between a Host Search and a Host Timeline?
A. Results from a Host Search return information in an organized view by type, while a Host Timeline returns a view of all events recorded by the sensor
B. A Host Timeline only includes process execution events and user account activity
C. Results from a Host Timeline include process executions and related events organized by data type. A Host Search returns a temporal view of all events for the given host
D. There is no difference - Host Search and Host Timeline are different names for the same search page
Answer: A
Explanation:
According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Host Search allows you to search for hosts based on various criteria, such as hostname, IP address, OS, etc1. The results are displayed in an organized view by type, such as detections, incidents, processes, network connections, etc1. The Host Timeline allows you to view all events recorded by the sensor for a given host in a chronological order1. The events include process executions, file writes, registry modifications, network connections, user logins, etc1.