

CrowdStrike CCFR-201b

CrowdStrike Certified Falcon Responder

**Thank You for Downloading CCFR-201b Updated Exam
Questions**

<https://certs4sale.com/CrowdStrike/ccfr-201b-pdf-exam-dumps>

Version: 4.0

Question: 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.

Question: 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: D

Explanation:

According to the CrowdStrike Falcon® Data Replicator (FDR) Add-on for Splunk Guide, Machine Learning Exclusions allow you to exclude files or directories from being scanned by CrowdStrike's machine learning engine, which can reduce false positives and improve performance². You can also choose whether to upload the excluded files to the CrowdStrike Cloud or not².

Question: 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.

Question: 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: B

Explanation:

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Process Timeline search returns all cloudable events associated with a given process, such as process creation, network connections, file writes, registry modifications, etc¹. This allows you to see a comprehensive view of what a process was doing on a host¹.

Question: 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.

THANK YOU FOR DOWNLOADING CCFR-201B UPDATED EXAM QUESTIONS

Note: Thanks For Trying The Demo Of Our CCFR-201b Exam Product

Visit Our Site to Purchase the Full Set of Actual CCFR-201b Exam Questions With Answers.

Money Back Guarantee



Click The Link Below

<https://certs4sale.com/CrowdStrike/ccfr-201b-pdf-exam-dumps>