CCFR-201 Q&As

CrowdStrike Certified Falcon Responder

Pass CrowdStrike CCFR-201 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/ccfr-201.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CrowdStrike Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

What happens when you open the full detection details?

A. Theprocess explorer opens and the detection is removed from the console

B. The process explorer opens and you\\'re able to view the processes and process relationships

C. The process explorer opens and the detection copies to the clipboard

D. The process explorer opens and the Event Search query is run for the detection

Correct Answer: B

According to the [CrowdStrike Falcon?Data Replicator (FDR) Add-on for Splunk Guide], when you open the full detection details from a detection alert or dashboard item, you are taken to a page where you can view detailed information about the detection, such as detection ID, severity, tactic, technique, description, etc. You can also view the events generated by the processes involved in the detection in different ways, such as process tree, process timeline, or process activity. The process tree view is also known as the process explorer, which provides a graphical representation of the process hierarchy and activity. You can view the processes and process relationships by expanding or collapsing nodes in the tree. You can also see the event types and timestamps for each process.

QUESTION 2

How long are quarantined files stored on the host?

A. 45 Days

B. 30 Days

C. Quarantined files are never deleted from the host

D. 90 Days

Correct Answer: C

According to the CrowdStrike Falcon?Data Replicator (FDR) Add-on for Splunk Guide, quarantined files are never deleted from the host unless you manually delete them or release them from quarantine2. When you release a file from quarantine, you are restoring it to its original location and allowing it to execute on any host in your organization2. This action also removes the file from the quarantine list and deletes it from the CrowdStrike Cloud2.

QUESTION 3

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

Correct Answer: D

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 4

You can jump to a Process Timeline from many views, like a Hash Search, by clicking which of the following?

A. ProcessTimeline Link

B. PID

C. UTCtime

D. Process ID or Parent Process ID

Correct Answer: D

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Process Timeline tool allows you to view all cloudable events associated with a given process, such as process creation, network connections, file writes, registry modifications, etc1. The tool requires two parameters: aid (agent ID) and TargetProcessId_decimal (the decimal value of the process ID)1. You can jump to a Process Timeline from many views, such as Hash Search, Host Timeline, Event Search, etc., by clicking on either the Process ID or Parent Process ID fields in those views1. This will automatically populate the aid and TargetProcessId_decimal parameters for the Process Timeline tool1.

QUESTION 5

The primary purpose for running a Hash Search is to:

A. determine any network connections

B. review the processes involved with a detection

C. determine the origin of the detection

D. review information surrounding a hash\\'s related activity

Correct Answer: D

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Hash Search tool allows you to search for one or more SHA256 hashes and view a summary of information from Falcon events that contain those hashes1. The summary includes the hostname, sensor ID, OS, country, city, ISP, ASN, geolocation, process name, command line, and organizational unit of the host that loaded or executed those hashes1. You can also see a count of detections and incidents related to those hashes1. The primary purpose for running a Hash Search is to review information surrounding a hash\\'s related activity, such as which hosts and processes were involved, where they were located, and whether they triggered any alerts1.