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.pass4itsure.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

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 2

When examining raw event data, what is the purpose of the field called ParentProcessId_decimal?

A. It contains an internal value not useful for an investigation

B. It contains the TargetProcessId_decimal value of the child process

C. It contains the SensorId_decimal value for related events

D. It contains the TargetProcessId_decimal of the parent process

Correct Answer: D

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the ParentProcessId_decimal field contains the decimal value of the process ID of the parent process that spawned or injected into the target process1. This field can be used to trace the process lineage and identify malicious or suspicious activities1.

QUESTION 3

How long are quarantined files stored in the CrowdStrike Cloud?

A. 45 Days

B. 90 Days

C. Days

D. Quarantined files are not deleted

Correct Answer: B

According to the [CrowdStrike Falcon?Data Replicator (FDR) Add-on for Splunk Guide], when you quarantine a file from a host using IOC Management or Real Time Response (RTR), you are moving it from its original location to a secure location on the host where it cannot be executed. The file is also encrypted and renamed with a random string of characters. A copy of the file is also uploaded to the CrowdStrike Cloud for further analysis. Quarantined files are stored in the CrowdStrike Cloud for 90 days before they are deleted.

QUESTION 4

From a detection, what is the fastest way to see children and sibling process information?

A. Select the Event Search option. Then from the Event Actions, select Show Associated Event Data (From TargetProcessId_decimal)

B. Select Full Detection Details from the detection

C. Right-click the process and select "Follow Process Chain"

D. Select the Process Timeline feature, enter the AID. Target Process ID, and Parent Process ID

Correct Answer: B

According to the CrowdStrike Falcon?Data Replicator (FDR) Add-on for Splunk Guide, the Full Detection Details tool allows you to view detailed information about a detection, such as detection ID, severity, tactic, technique, description, etc1. 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 activity1. The process tree view provides a graphical representation of the process hierarchy and activity1. You can see children and sibling processes information by expanding or collapsing nodes in the tree1.

QUESTION 5

When examining a raw DNS request event, you see a field called ContextProcessId_decimal. What is the purpose of that field?

A. It contains the TargetProcessId_decimal value for other related events

B. It contains an internal value not useful for an investigation

C. It contains the ContextProcessId_decimal value for the parent process that made the DNS request

D. It contains the TargetProcessId_decimal value for the process that made the DNS request

Correct Answer: D

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the ContextProcessId_decimal field contains the decimal value of the process ID of the process that generated the event1. This field can be used to trace the process lineage and identify malicious or suspicious activities1. For a DNS request event, this field indicates which process made the DNS request1.