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

In the Hash Search tool, which of the following is listed under Process Executions?

A. Operating System

B. File Signature

C. Command Line

D. Sensor Version

Correct Answer: C

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. Under Process Executions, you can see the process name and command line for each hash execution1.

QUESTION 2

In the "Full Detection Details", which view will provide an exportable text listing of events like DNS requests. Registry Operations, and Network Operations?

A. Thedata is unable to be exported

B. View as Process Tree

C. View as Process Timeline

D. View as Process Activity

Correct Answer: D

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, 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 activity view provides a rows-andcolumns style view of the events, such as DNS requests, registry operations, network operations, etc1. You can also export this view to a CSV file for further analysis1.

QUESTION 3

Aside from a Process Timeline or Event Search, how do you export process event data from a detection in .CSV format?

A. You can\\'t export detailed event data from a detection, you have to use the Process Timeline or an Event Search

B. In Full Detection Details, you expand the nodes of the process tree you wish to expand and then click the "Export

Process Events" button

C. In Full Detection Details, you choose the "View Process Activity" option and then export from that view

D. From the Detections Dashboard, you right-click the event type you wish to export and choose CSV. JSON or XML

Correct Answer: C

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, there are three ways to export process event data from a detection in .CSV format1:

You can use the Process Timeline tool and click on "Export CSV" button at the top right corner1.

You can use the Event Search tool and select one or more events and click on "Export CSV" button at the top right corner1.

You can use the Full Detection Details tool and choose the "View Process Activity" option from any process node in the process tree view1. This will show you all events generated bythat process in a rows-and-columns style view1. You can

then click on "Export CSV" button at the top right corner1.

QUESTION 4

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.

QUESTION 5

What do IOA exclusions help you achieve?

A. Reduce false positives based on Next-Gen Antivirus settings in the Prevention Policy

B. Reduce false positives of behavioral detections from IOA based detections only

C. Reduce false positives of behavioral detections from IOA based detections based on a file hash

D. Reduce false positives of behavioral detections from Custom IOA and OverWatch detections only

Correct Answer: B

According to the CrowdStrike Falcon?Data Replicator (FDR) Add-on for Splunk Guide, IOA exclusions allow you to exclude files or directories from being detected or blocked by CrowdStrike\\'s indicators of attack (IOAs), which are behavioral rules that identify malicious activities2. This can reduce false positives and improve performance2. IOA exclusions only apply to IOA based detections, not other types of detections such as machine learning, custom IOA, or OverWatch2.