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

The Process Activity View provides a rows-and-columns style view of the events generated in a detection. Why might this be helpful?

A. The Process Activity View creates a consolidated view of all detection events for that process that can be exported for further analysis

B. The Process Activity View will show the Detection time of the earliest recorded activity which might indicate first affected machine

C. The Process Activity View only creates a summary of Dynamic Link Libraries (DLLs) loaded by a process

D. The Process Activity View creates a count of event types only, which can be useful when scoping the event

Correct Answer: A

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Process Activity View allows you to view all events generated by a process involved in a detection in a rows-and-columns style view1. This can be helpful because it creates a consolidated view of all detection events for that process that can be exported for further analysis1. You can also sort, filter, and pivot on the events by various fields, such as event type, timestamp, file name, registry key, network destination, etc1.

QUESTION 2

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 3

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 4

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 5

What happens when a hash is allowlisted?

A. Execution is prevented, but detection alerts are suppressed

B. Execution is allowed on all hosts, including all other Falcon customers

C. The hash is submitted for approval to be allowed to execute once confirmed by Falcon specialists

D. Execution is allowed on all hosts that fall under the organization\\'s CID

Correct Answer: D

According to the CrowdStrike Falcon?Data Replicator (FDR) Add-on for Splunk Guide, the allowlist feature allows you to exclude files or directories from being scanned or blocked by CrowdStrike\\'s machine learning engine or indicators of attack (IOAs)2. This can reduce false positives and improve performance2. When you allowlist a hash, you are allowing that file to execute on any host that belongs to your organization\\'s CID (customer ID)2. This does not affect other Falcon customers or hosts outside your CID2.