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

What does the Full Detection Details option provide?

A. It provides a visualization of program ancestry via the Process Tree View

B. It provides a visualization of program ancestry via the Process Activity View

C. It provides detailed list of detection events via the Process Table View

D. It provides a detailed list of detection events via the Process Tree View

Correct Answer: A

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Full Detection Details option 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 visualization of program ancestry, which shows the parent-child and sibling relationships among the processes1. You can also see the event types and timestamps for each process1.

QUESTION 2

What does pivoting to an Event Search from a detection do?

A. It gives you the ability to search for similar events on other endpoints quickly

B. It takes you to the raw Insight event data and provides you with a number of Event Actions

C. It takes you to a Process Timeline for that detection so you can see all related events

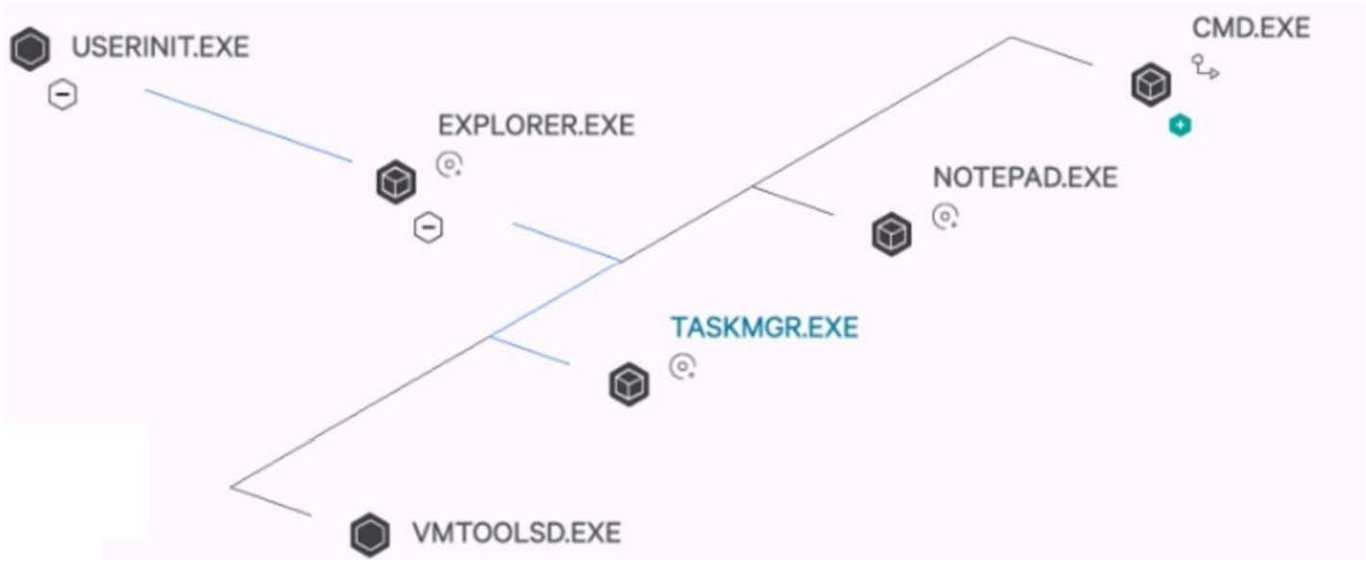
D. It allows you to input an event type, such as DNS Request or ASEP write, and search for those events within the detection

Correct Answer: B

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, pivoting to an Event Search from a detection takes you to the raw Insight event data and provides you with a number of Event Actions1. Insight events are low-level events that are generated by the sensor for various activities, such as process executions, file writes, registry modifications, network connections, etc1. You can view these events in a table format and use various filters and fields to narrow down the results1. You can also select one or more events and perform various actions, such as show a process timeline, show a host timeline, show associated event data, show a +/- 10-minute window of events, etc1. These actions can help you investigate and analyze events more efficiently and effectively1.

QUESTION 3

How are processes on the same plane ordered (bottom \\'VMTOOLSD.EXE\\' to top CMD.EXE\\')?



A. Process ID (Descending, highest on bottom)

B. Time started (Descending, most recent on bottom)

C. Time started (Ascending, most recent on top)

D. Process ID (Ascending, highest on top)

Correct Answer: B

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the process tree view provides a visualization of program ancestry, which shows the parent-child and sibling relationships among the processes1. You can also see the event types and timestamps for each process1. The processes on the same plane are ordered by time started in descending order, meaning that the most recent process is at the bottom and the oldest process is at the top1. For example, in the image you sent me, CMD.EXE is the oldest process and VMTOOLSD.EXE is the most recent process on that plane1.

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

You found a list of SHA256 hashes in an intelligence report and search for them using the Hash Execution Search. What can be determined from the results?

A. Identifies a detailed list of all process executions for the specified hashes

B. Identifies hosts that loaded or executed the specified hashes

C. Identifies users associated with the specified hashes

D. Identifies detections related to the specified hashes

Correct Answer: B

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Hash Execution 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, and geolocation of the host that loaded or executed those hashes1. You can also see a count of detections and incidents related to those hashes1.

QUESTION 6

What is an advantage of using the IP Search tool?

A. IP searches provide manufacture and timezone data that can not be accessed anywhere else

B. IP searches allow for multiple comma separated IPv6 addresses as input

C. IP searches offer shortcuts to launch response actions and network containment on target hosts

D. IP searches provide host, process, and organizational unit data without the need to write a query

Correct Answer: D

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the IP Search tool allows you to search for an IP address and view a summary of information from Falcon events that contain that IP address1. The summary includes the hostname, sensor ID, OS, country, city, ISP, ASN, geolocation, process name, command line, and organizational unit of the host that communicated with that IP address1. This is an advantage of using the IP Search tool because it provides host, process, and organizational unit data without the need to write a query1.

QUESTION 7

The Bulk Domain Search tool contains Domain information along with which of the following?

A. Process Information

B. Port Information

C. IP Lookup Information

D. Threat Actor Information

Correct Answer: C

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Bulk Domain Search tool allows you to search for one or more domains and view a summary of information from Falcon events that contain those domains1. The summary includes the domain name, IP address, country, city, ISP, ASN, geolocation, hostname, sensor ID, OS, process name, command line, and organizational unit of the host that communicated with those domains1. This means that the tool contains domain information along with IP lookup information1.

QUESTION 8

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 9

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 10

Which Executive Summary dashboard item indicates sensors running with unsupported versions?

A. Detections by Severity

B. Inactive Sensors

C. Sensors in RFM

D. Active Sensors

Correct Answer: C

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Executive Summary dashboard provides an overview of your sensor health and activity1. It includes various items, such as Active Sensors, Inactive Sensors, Detections by Severity, etc1. The item that indicates sensors running with unsupported versions is Sensors in RFM (Reduced Functionality Mode)1. RFM is a state where a sensor has limited functionality due to various reasons, such as license expiration, network issues, tampering attempts, or unsupported versions1. You can see the number and percentage of sensors in RFM and the reasons why they are in RFM1.

CCFR-201 VCE Dumps CCFR-201 Practice Test CCFR-201 Braindumps