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

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.

QUESTION 3

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 4

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.

QUESTION 5

What action is used when you want to save a prevention hash for later use?

A. Always Block

B. Never Block

C. Always Allow

D. No Action

Correct Answer: A

According to the CrowdStrike Falcon?Data Replicator (FDR) Add-on for Splunk Guide, the Always Block action allows you to block a file from executing on any host in your organization based on its hash value2. This action can be used to prevent known malicious files from running on your endpoints2.