CCFR-201$^{Q\&As}$

CrowdStrike Certified Falcon Responder

Pass CrowdStrike CCFR-201 Exam with 100% Guarantee

QUESTION 1

What happens when a quarantined file is released?

A. It is moved into theC:\CrowdStrike\Quarantine\Releasedfolder on the host

B. It is allowed to execute on the host

C. It is deleted

D. It is allowed to execute on all hosts

Correct Answer: D

According to the CrowdStrike Falcon?Data Replicator (FDR) Add-on for Splunk Guide, when you release a file from quarantine, you are restoring it to its original location and allowing it to execute on any host in your organization1. This action also removes the file from the quarantine list and deletes it from the CrowdStrike Cloud1.

QUESTION 2

Which of the following is NOT a valid event type?

A. StartofProcess

B. EndofProcess

C. ProcessRollup2

D. DnsRequest

Correct Answer: B

According to the [CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+], event types are categories of events that are generated by the sensor for various activities, such as process executions, file writes, registry modifications, network connections, etc. There are many valid event types, such as StartOfProcess, ProcessRollup2, DnsRequest, etc. However, EndOfProcess is not a valid event type, as there is no such event that records the end of a process.

QUESTION 3

You are notified by a third-party that a program may have redirected traffic to a malicious domain. Which Falcon page will assist you in searching for any domain request information related to this notice?

A. Falcon X

B. Investigate

C. Discover

D. Spotlight

Correct Answer: B

According to the [CrowdStrike website], the Investigate page is where you can search for and analyze various types of data collected by the Falcon platform, such as events, hosts, processes, hashes, domains, IPs, etc1. You can use various tools, such as Event Search, Host Search, Process Timeline, Hash Search, Bulk Domain Search, etc., to perform different types of searches and view the results in different ways1. If you want to search for any domain request information related to a notice from a third-party, you can use the Investigate page to do so1. For example, you can use the Bulk Domain Search tool to search for the malicious domain and see which hosts and processes communicated with it1. You can also use the Event Search tool to search for DNSRequest events that contain the malicious domain and see more details about the query and response1.

QUESTION 4

What happens when you create a Sensor Visibility Exclusion for a trusted file path?

A. It excludes host information from Detections and Incidents generated within that file path location

B. It prevents file uploads to the CrowdStrike cloud from that file path

C. It excludes sensor monitoring and event collection for the trusted file path

D. It disables detection generation from that path, however the sensor can still perform prevention actions

Correct Answer: C

According to the CrowdStrike Falcon?Data Replicator (FDR) Add-on for Splunk Guide, Sensor Visibility Exclusions allow you to exclude certain files or directories from being monitored by the CrowdStrike sensor, which can reduce noise and improve performance2. This means that no events will be collected or sent to the CrowdStrike Cloud for those files or directories2.

QUESTION 5

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.