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

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 2

What information is contained within a Process Timeline?

A. All cloudable process-related events within a given timeframe

B. All cloudable events for a specific host

C. Only detection process-related events within a given timeframe

D. A view of activities on Mac or Linux hosts

Correct Answer: A

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Process Timeline tool allows you to view all cloudable events associated with a given process, such as process creation, network connections, file writes, registry modifications, etc1. You can specify a timeframe to limit the events to a certain period1. The tool works for any host platform, not just Mac or Linux1.

QUESTION 3

Where can you find hosts that are in Reduced Functionality Mode?

A. Event Search

B. Executive Summary dashboard

C. Host Search

D. Installation Tokens

Correct Answer: C

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, Reduced Functionality Mode (RFM) is a state where a host\\'s sensor has limited functionality due to various reasons, such as license expiration, network issues, tampering attempts, etc1. You can find hosts that are in RFM by using the Host Search tool and filtering by Sensor Status = RFM1. You can also view details about why a host is in RFM by clicking on its hostname1.

QUESTION 4

What types of events are returned by a Process Timeline?

A. Only detection events

B. All cloudable events

C. Only process events

D. Only network events

Correct Answer: B

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Process Timeline search returns all cloudable events associated with a given process, such as process creation, network connections, file writes, registry modifications, etc1. This allows you to see a comprehensive view of what a process was doing on a host1.

QUESTION 5

The primary purpose for running a Hash Search is to:

A. determine any network connections

B. review the processes involved with a detection

C. determine the origin of the detection

D. review information surrounding a hash\\'s related activity

Correct Answer: D

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. The primary purpose for running a Hash Search is to review information surrounding a hash\\'s related activity, such as which hosts and processes were involved, where they were located, and whether they triggered any alerts1.