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

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

Which of the following is NOT a filter available on the Detections page?

A. Severity

B. CrowdScore

C. Time

D. Triggering File

Correct Answer: D

According to the CrowdStrike Falcon?Data Replicator (FDR) Add-on for Splunk Guide, the Detections page allows you to view and manage detections generated by the CrowdStrike Falcon platform2. You can use various filters to narrow down the detections based on criteria such as severity, CrowdScore, time, tactic, technique, etc2. However, there is no filter for triggering file, which is the file that caused the detection2.

QUESTION 2

Which of the following is returned from the IP Search tool?

A. IP Summary information from Falcon events containing the given IP

B. Threat Graph Data for the given IP from Falcon sensors

C. Unmanaged host data from system ARP tables for the given IPD.IP Detection Summary information for detection events containing the given IP

Correct Answer: A

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, and geolocation of the host that communicated with that IP address1.

QUESTION 3

Sensor Visibility Exclusion patterns are written in which syntax?

A. Glob Syntax

B. Kleene Star Syntax

C. RegEx

D. SPL(Splunk)

Correct Answer: A

According to the [CrowdStrike Falcon?Data Replicator (FDR) Add-on for Splunk Guide], Sensor Visibility Exclusions allow you to exclude files or directories from being monitored by the sensor. This can reduce the amount of data sent to the CrowdStrike Cloud and improve performance. Sensor Visibility Exclusion patterns are written in Glob Syntax, which is a simple pattern matching syntax that supports wildcards, such as *, ?, and . For example, you can use *.exe to exclude all files with .exe extension.

QUESTION 4

After running an Event Search, you can select many Event Actions depending on your results. Which of the following is NOT an option for any Event Action?

A. Draw Process Explorer

B. Show a +/- 10-minute window of events

C. Show a Process Timeline for the responsible process

D. Show Associated Event Data (from TargetProcessId_decimal or ContextProcessId_decimal)

Correct Answer: A

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Event Search tool allows you to search for events based on various criteria, such as event type, timestamp, hostname, IP address, etc1. 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. However, there is no option to draw a process explorer, which is a graphical representation of the process hierarchy and activity1.

QUESTION 5

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.

Latest CCFR-201 Dumps   CCFR-201 VCE Dumps   CCFR-201 Practice Test