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.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

QUESTION 1

Which statement is TRUE regarding the "Bulk Domains" search?

A. It will show a list of computers and process that performed a lookup of any of the domains in your search

B. The "Bulk Domains" search will allow you to blocklist your queried domains

C. The "Bulk Domains" search will show IP address and port information for any associated connectionsD.You should only pivot to the "Bulk Domains" search tool after completing an investigation

Correct Answer: A

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 domains2. The summary includes the hostname, sensor ID, OS, country, city, ISP, ASN, geolocation, process name, command line, and organizational unit of the host that performed a lookup of any of the domains in your search2. This can help you identify potential threats or vulnerabilities in your network2.

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

When you configure and apply an IOA exclusion, what impact does it have on the host and what you see in the console?

A. The process specified is not sent to the Falcon Sandbox for analysis

B. The associated detection will be suppressed and the associated process would have been allowed to run

C. The sensor will stop sending events from the process specified in the regex pattern

D. The associated IOA will still generate a detection but the associated process would have been allowed to run

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 activities1. This can reduce false positives and improve performance1. When you configure and apply an IOA exclusion, the impact is that the associated detection will be suppressed and theassociated process would have been allowed to run1. This means that you will not see any alerts or events related to that IOA in the console1.

QUESTION 4

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.

QUESTION 5

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.