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.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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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 2

What is an advantage of using the IP Search tool?

A. IP searches provide manufacture and timezone data that can not be accessed anywhere else

B. IP searches allow for multiple comma separated IPv6 addresses as input

C. IP searches offer shortcuts to launch response actions and network containment on target hosts

D. IP searches provide host, process, and organizational unit data without the need to write a query

Correct Answer: D

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, geolocation, process name, command line, and organizational unit of the host that communicated with that IP address1. This is an advantage of using the IP Search tool because it provides host, process, and organizational unit data without the need to write a query1.

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

When looking at the details of a detection, there are two fields called Global Prevalence and Local Prevalence. Which answer best defines Local Prevalence?

A. Local prevalence is the frequency with which the hash of the triggering file is seen across the entire Internet

B. Local Prevalence tells you how common the hash of the triggering file is within your environment (CID)

C. Local Prevalence is the Virus Total score for the hash of the triggering file

D. Local prevalence is the frequency with which the hash of the triggering file is seen across all CrowdStrike customer environments

Correct Answer: B

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, Global Prevalence and Local Prevalence are two fields that provide information about how common or rare a file is based on its hash value2. Global Prevalence tells you how frequently the hash of the triggering file is seen across all CrowdStrike customer environments2. Local Prevalence tells you how frequently the hash of the triggering file is seen within your environment (CID)2. These fields can help you assess the risk and impact of a detection2.

QUESTION 5

What is the difference between Managed and Unmanaged Neighbors in the Falcon console?

A. A managed neighbor is currently network contained and an unmanaged neighbor is uncontained

B. A managed neighbor has an installed and provisioned sensor

C. An unmanaged neighbor is in a segmented area of the network

D. A managed sensor has an active prevention policy

Correct Answer: B

According to the CrowdStrike Falcon?Data Replicator (FDR) Add-on for Splunk Guide, you can use the Hosts page in the Investigate tool to view information about your endpoints, such as hostname, IP address, OS, sensor version, etc2. You can also see a list of managed and unmanaged neighbors for each endpoint, which are other devices that have

communicated with that endpoint over the network2. A managed neighbor is a device that has an installed and provisioned sensor that reports to the CrowdStrike Cloud2. An unmanaged neighbor is a device that does not have an installed or provisioned sensor2.