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

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 2

What is an advantage of using a Process Timeline?

A. Process related events can be filtered to display specific event types

B. Suspicious processes are color-coded based on their frequency and legitimacy over time

C. Processes responsible for spikes in CPU performance are displayed overtime

D. A visual representation of Parent-Child and Sibling process relationships is provided

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, etc2. You can also filter the events by various criteria, such as event type, timestamp range, file name, registry key, network destination, etc2. This is an advantage of using the Process Timeline tool because it allows you to focus on specific events that are relevant to your investigation2.

QUESTION 3

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 4

How long are quarantined files stored in the CrowdStrike Cloud?

A. 45 Days

B. 90 Days

C. Days

D. Quarantined files are not deleted

Correct Answer: B

According to the [CrowdStrike Falcon?Data Replicator (FDR) Add-on for Splunk Guide], when you quarantine a file from a host using IOC Management or Real Time Response (RTR), you are moving it from its original location to a secure location on the host where it cannot be executed. The file is also encrypted and renamed with a random string of characters. A copy of the file is also uploaded to the CrowdStrike Cloud for further analysis. Quarantined files are stored in the CrowdStrike Cloud for 90 days before they are deleted.

QUESTION 5

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.