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.leads4pass.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 function of Machine Learning Exclusions is to_____.

A. stop all detections for a specific pattern ID

B. stop all sensor data collection for the matching path(s)

C. Stop all Machine Learning Preventions but a detection will still be generated and files will still be uploaded to the CrowdStrike Cloud

D. stop all ML-based detections and preventions for the matching path(s) and/or stop files from being uploaded to the CrowdStrike Cloud

Correct Answer: D

According to the CrowdStrike Falcon?Data Replicator (FDR) Add-on for Splunk Guide, Machine Learning Exclusions allow you to exclude files or directories from being scanned by CrowdStrike\\'s machine learning engine, which can reduce false positives and improveperformance2. You can also choose whether to upload the excluded files to the CrowdStrike Cloud or not2.

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 reviewing a Host Timeline, which of the following filters is available?

A. Severity

B. Event Types

C. User Name

D. Detection ID

Correct Answer: B

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Host Timeline tool allows you to view all events recorded by the sensor for a given host in a chronological order1. The events include process executions, file writes, registry modifications, network connections, user logins, etc1. You can use various filters to narrow down the events based on criteria such as event type, timestamp range, file name, registry key, network destination, etc1. However, there is no filter for severity, user name, or detection ID, as these are not attributes of the events1.

QUESTION 4

You notice that taskeng.exe is one of the processes involved in a detection. What activity should you investigate next?

A. User logons after the detection

B. Executions of schtasks.exe after the detection

C. Scheduled tasks registered prior to the detection

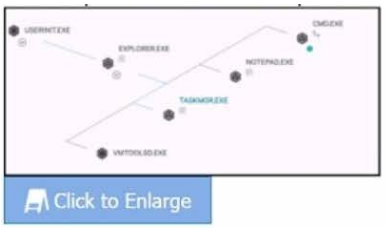
D. Pivot to a Hash search for taskeng.exe

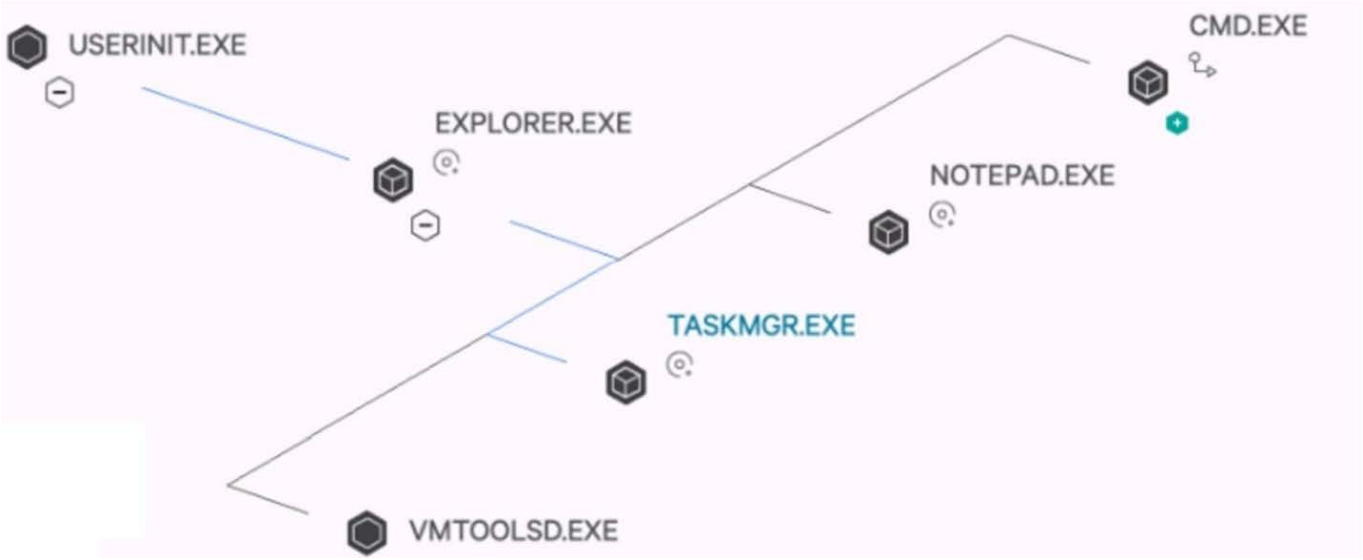
Correct Answer: C

According to the [Microsoft website], taskeng.exe is a legitimate Windows process that is responsible for running scheduled tasks. However, some malware may use this process or create a fake one to execute malicious code. Therefore, if you notice taskeng.exe involved in a detection, you should investigate whether there are any scheduled tasks registered prior to the detection that may have triggered or injected into taskeng.exe. You can use tools such as schtasks.exe or Task Scheduler to view or manage scheduled tasks.

QUESTION 5

How are processes on the same plane ordered (bottom \\'VMTOOLSD.EXE\\' to top CMD.EXE\\')?





A. Process ID (Descending, highest on bottom)

B. Time started (Descending, most recent on bottom)

C. Time started (Ascending, most recent on top)

D. Process ID (Ascending, highest on top)

Correct Answer: B

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the process tree view provides a visualization of program ancestry, which shows the parent-child and sibling relationships among the processes1. You can also see the event types and timestamps for each process1. The processes on the same plane are ordered by time started in descending order, meaning that the most recent process is at the bottom and the oldest process is at the top1. For example, in the image you sent me, CMD.EXE is the oldest process and VMTOOLSD.EXE is the most recent process on that plane1.

QUESTION 6

How long are quarantined files stored on the host?

A. 45 Days

B. 30 Days

C. Quarantined files are never deleted from the host

D. 90 Days

Correct Answer: C

According to the CrowdStrike Falcon?Data Replicator (FDR) Add-on for Splunk Guide, quarantined files are never deleted from the host unless you manually delete them or release them from quarantine2. When you release a file from quarantine, you are restoring it to its original location and allowing it to execute on any host in your organization2. This action also removes the file from the quarantine list and deletes it from the CrowdStrike Cloud2.

QUESTION 7

You found a list of SHA256 hashes in an intelligence report and search for them using the Hash Execution Search. What can be determined from the results?

A. Identifies a detailed list of all process executions for the specified hashes

B. Identifies hosts that loaded or executed the specified hashes

C. Identifies users associated with the specified hashes

D. Identifies detections related to the specified hashes

Correct Answer: B

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Hash Execution 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, and geolocation of the host that loaded or executed those hashes1. You can also see a count of detections and incidents related to those hashes1.

QUESTION 8

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 9

What is the difference between a Host Search and a Host Timeline?

A. Results from a Host Search return information in an organized view by type, while a Host Timeline returns a view of all events recorded by the sensor

B. A Host Timeline only includes process execution events and user account activity

C. Results from a Host Timeline include process executions and related events organized by data type. A Host Search returns a temporal view of all events for the given host

D. There is no difference - Host Search and Host Timeline are different names for the same search page

Correct Answer: A

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Host Search allows you to search for hosts based on various criteria, such as hostname, IP address, OS, etc1. The results are displayed in an organized view by type, such as detections, incidents, processes, network connections, etc1. The Host Timeline allows you to view all events recorded by the sensor for a given host in a chronological order1. The events include process executions, file writes, registry modifications, network connections, user logins, etc1.

QUESTION 10

How long does detection data remain in the CrowdStrike Cloud before purging begins?

A. 90 Days

B. 45 Days

C. 30 Days

D. 14 Days

Correct Answer: A

According to the CrowdStrike Falcon?Data Replicator (FDR) Add-on for Splunk Guide, detection data is stored in the CrowdStrike Cloud for 90 days before purging begins2. This means that you can access and view detections from the past 90 days using the Falcon platform or API2. If you want to retain detection data for longer than 90 days, you can use FDR to replicate it to your own storage system2.

CCFR-201 VCE Dumps CCFR-201 Exam Questions CCFR-201 Braindumps