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.certbus.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

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 2

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 3

What information is contained within a Process Timeline?

A. All cloudable process-related events within a given timeframe

B. All cloudable events for a specific host

C. Only detection process-related events within a given timeframe

D. A view of activities on Mac or Linux hosts

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, etc1. You can specify a timeframe to limit the events to a certain period1. The tool works for any host platform, not just Mac or Linux1.

QUESTION 4

The Process Activity View provides a rows-and-columns style view of the events generated in a detection. Why might this be helpful?

A. The Process Activity View creates a consolidated view of all detection events for that process that can be exported for further analysis

B. The Process Activity View will show the Detection time of the earliest recorded activity which might indicate first affected machine

C. The Process Activity View only creates a summary of Dynamic Link Libraries (DLLs) loaded by a process

D. The Process Activity View creates a count of event types only, which can be useful when scoping the event

Correct Answer: A

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Process Activity View allows you to view all events generated by a process involved in a detection in a rows-and-columns style view1. This can be helpful because it creates a consolidated view of all detection events for that process that can be exported for further analysis1. You can also sort, filter, and pivot on the events by various fields, such as event type, timestamp, file name, registry key, network destination, etc1.

QUESTION 5

From a detection, what is the fastest way to see children and sibling process information?

A. Select the Event Search option. Then from the Event Actions, select Show Associated Event Data (From TargetProcessId_decimal)

B. Select Full Detection Details from the detection

C. Right-click the process and select "Follow Process Chain"

D. Select the Process Timeline feature, enter the AID. Target Process ID, and Parent Process ID

Correct Answer: B

According to the CrowdStrike Falcon?Data Replicator (FDR) Add-on for Splunk Guide, the Full Detection Details tool allows you to view detailed information about a detection, such as detection ID, severity, tactic, technique, description, etc1. You can also view the events generated by the processes involved in the detection in different ways, such as process tree, process timeline, or process activity1. The process tree view provides a graphical representation of the

process hierarchy and activity1. You can see children and sibling processes information by expanding or collapsing nodes in the tree1.

QUESTION 6

The Falcon platform will show a maximum of how many detections per day for a single Agent Identifier (AID)?

A. 500

B. 750

C. 1000

D. 1200

Correct Answer: C

According to the CrowdStrike Falcon?Data Replicator (FDR) Add-on for Splunk Guide, the Falcon platform will show a maximum of 1000 detections per day for a single AID1. This is a limitimposed by the Falcon API, which is used to retrieve the detections from the CrowdStrike Cloud1. If there are more than 1000 detections per day for a single AID, only the first 1000 will be shown1.

QUESTION 7

What happens when a quarantined file is released?

A. It is moved into theC:\CrowdStrike\Quarantine\Releasedfolder on the host

B. It is allowed to execute on the host

C. It is deleted

D. It is allowed to execute on all hosts

Correct Answer: D

According to the CrowdStrike Falcon?Data Replicator (FDR) Add-on for Splunk Guide, 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 organization1. This action also removes the file from the quarantine list and deletes it from the CrowdStrike Cloud1.

QUESTION 8

Which of the following tactic and technique combinations is sourced from MITRE ATTandCK information?

A. Falcon Intel via Intelligence Indicator - Domain

B. Machine Learning via Cloud-Based ML

C. Malware via PUP

D. Credential Access via OS Credential Dumping

Correct Answer: D

According to the [MITRE ATTandCK website], MITRE ATTandCK is a knowledge base of adversary behaviors and techniques based on real-world observations. The knowledge base is organized into tactics and techniques, where tactics are the high-level goals of an adversary, such as initial access, persistence, lateral movement, etc., and techniques are the specific ways an adversary can achieve those goals, such as phishing, credential dumping, remote file copy, etc. Credential Access via OS Credential Dumping is an example of a tactic and technique combination sourced from MITRE ATTandCK information, which describes how adversaries can obtain credentials from operating system memory or disk storage by using tools such as Mimikatz or ProcDump.

QUESTION 9

When examining raw event data, what is the purpose of the field called ParentProcessId_decimal?

A. It contains an internal value not useful for an investigation

B. It contains the TargetProcessId_decimal value of the child process

C. It contains the SensorId_decimal value for related events

D. It contains the TargetProcessId_decimal of the parent process

Correct Answer: D

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the ParentProcessId_decimal field contains the decimal value of the process ID of the parent process that spawned or injected into the target process1. This field can be used to trace the process lineage and identify malicious or suspicious activities1.

QUESTION 10

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.