Free Questions for CCFR-201 by certscare

Shared by Clemons on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

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

Answer:

D

Explanation:

According to theCrowdStrike 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 2

Question Type: MultipleChoice

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

Options:

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

Answer:

A

Explanation:

According to theCrowdStrike 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 3

Question Type: MultipleChoice

What types of events are returned by a Process Timeline?

Options:

A- Only detection events

B- All cloudable events

C- Only process events

D- Only network events

Answer:

B

Explanation:

According to theCrowdStrike 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

Question Type: MultipleChoice

What happens when you create a Sensor Visibility Exclusion for a trusted file path?

Options:

A- It excludes host information from Detections and Incidents generated within that file path location

B- It prevents file uploads to the CrowdStrike cloud from that file path

C- It excludes sensor monitoring and event collection for the trusted file path

D- It disables detection generation from that path, however the sensor can still perform prevention actions

Answer:

C

Explanation:

According to theCrowdStrike Falcon Data Replicator (FDR) Add-on for Splunk Guide, Sensor Visibility Exclusions allow you to exclude certain files or directories from being monitored by the CrowdStrike sensor, which can reduce noise and improve performance2.This means that no events will be collected or sent to the CrowdStrike Cloud for those files or directories2.

Question 5

Question Type: MultipleChoice

The function of Machine Learning Exclusions is to_____.

Options:

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

Answer:

D

Explanation:

According to theCrowdStrike 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 improve performance2.You can also choose whether to upload the excluded files to the CrowdStrike Cloud or not2.

Question 6

Question Type: MultipleChoice

After pivoting to an event search from a detection, you locate the ProcessRollup2 event. Which two field values are you required to obtain to perform a Process Timeline search so you can determine what the process was doing?

Options:

A- SHA256 and TargetProcessId_decimal

B- SHA256 and ParentProcessId_decimal

C- aid and ParentProcessId_decimal

D- aid and TargetProcessId_decimal

Answer:

D

Explanation:

According to theCrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Process Timeline search requires two parameters:aid(agent ID) andTargetProcessId_decimal(the decimal value of the process ID).These fields can be obtained from the ProcessRollup2 event, which contains information about processes that have executed on a host1.

Question 7

Question Type: MultipleChoice

Which is TRUE regarding a file released from quarantine?

Options:

A- No executions are allowed for 14 days after release

B- It is allowed to execute on all hosts

C- It is deleted

D- It will not generate future machine learning detections on the associated host

Answer:

B

Explanation:

According to theCrowdStrike 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 organization2.This action also removes the file from the quarantine list and deletes it from the CrowdStrike Cloud2.

Question 8

Question Type: MultipleChoice

What happens when a hash is allowlisted?

Options:

A- Execution is prevented, but detection alerts are suppressed

B- Execution is allowed on all hosts, including all other Falcon customers

C- The hash is submitted for approval to be allowed to execute once confirmed by Falcon specialists

D- Execution is allowed on all hosts that fall under the organization's CID

Answer:

D

Explanation:

According to theCrowdStrike Falcon Data Replicator (FDR) Add-on for Splunk Guide, the allowlist feature allows you to exclude files or directories from being scanned or blocked by CrowdStrike's machine learning engine or indicators of attack (IOAs)2.This can reduce false positives and improve performance2.When you allowlist a hash, you are allowing that file to execute on any host that belongs to your organization's CID (customer ID)2.This does not affect other Falcon customers or hosts outside your CID2.