Free Questions for CCFR-201 by braindumpscollection

Shared by Witt on 05-09-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

What happens when you open the full detection details?

Options:

A- The process explorer opens and the detection is removed from the console

B- The process explorer opens and you're able to view the processes and process relationships

C- The process explorer opens and the detection copies to the clipboard

D- The process explorer opens and the Event Search query is run for the detection

Answer:

B

Explanation:

According to the [CrowdStrike Falcon Data Replicator (FDR) Add-on for Splunk Guide], when you open the full detection details from a detection alert or dashboard item, you are taken to a page where you can view detailed information about the detection, such as detection ID, severity, tactic, technique, description, etc. 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 activity. The process tree view is also known as the process explorer, which provides a graphical representation of the process hierarchy and activity. You can view the processes and process relationships by expanding or collapsing nodes in the tree. You can also see the event types and timestamps for each process.

Question 2

Question Type: MultipleChoice

How long are quarantined files stored in the CrowdStrike Cloud?

Options:

A- 45 Days

B- 90 Days

C- Days

D- Quarantined files are not deleted

Answer:

B

Explanation:

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 3

Question Type: **MultipleChoice**

You receive an email from a third-party vendor that one of their services is compromised, the vendor names a specific IP address that the compromised service was using. Where would you input this indicator to find any activity related to this IP address?

Options:

A- IP Addresses

B- Remote or Network Logon Activity

C- Remote Access Graph

D- Hash Executions

Answer:

A

Explanation:

According to the [CrowdStrike website], the Discover page is where you can search for and analyze various types of indicators of compromise (IOCs), such as hashes, IP addresses, or domains that are associated with malicious activities. You can use various tools, such as Hash Executions, IP Addresses, Remote or Network Logon Activity, etc., to perform different types of searches and view the results in different ways. If you want to search for any activity related to an IP address that was compromised by a third-party vendor, you can use the IP Addresses tool to do so. You can input the IP address and see a summary of information from Falcon events that contain that IP address, such as hostname, sensor ID, OS, country, city, ISP, ASN, geolocation, process name, command line, and organizational unit of the host that communicated with that IP address.

Question 4

Question Type: **MultipleChoice**

Sensor Visibility Exclusion patterns are written in which syntax?

Options:

A- Glob Syntax

B- Kleene Star Syntax

C- RegEx

D- SPL(Splunk)

Answer:

A

Explanation:

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 5

Question Type: MultipleChoice

Which of the following is NOT a valid event type?

Options:

A- StartofProcess

B- EndofProcess

C- ProcessRollup2

D- DnsRequest

Answer:

B

Explanation:

According to the [CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+], event types are categories of events that are generated by the sensor for various activities, such as process executions, file writes, registry modifications, network connections, etc. There are many valid event types, such as StartOfProcess, ProcessRollup2, DnsRequest, etc. However, EndOfProcess is not a valid event type, as there is no such event that records the end of a process.

Question 6

Question Type: **MultipleChoice**

How long are quarantined files stored on the host?

Options:

A- 45 Days

B- 30 Days

C- Quarantined files are never deleted from the host

D- 90 Days

Answer:

C

Explanation:

According to theCrowdStrike 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

Question Type: MultipleChoice

Where are quarantined files stored on Windows hosts?

Options:

A- Windows\Quarantine

B- Windows\System32\Drivers\CrowdStrike\Quarantine

C- Windows\System32\

D- Windows\temp\Drivers\CrowdStrike\Quarantine

Answer:

B

Explanation:

According to theCrowdStrike 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 executed2.The file is also encrypted and renamed with a random string of characters2.On Windows hosts, quarantined files are stored in C:\Windows\System32\Drivers\CrowdStrike\Quarantine folder2.

Question 8

Question Type: MultipleChoice

You can jump to a Process Timeline from many views, like a Hash Search, by clicking which of the following?

Options:

A- ProcessTimeline Link

B- PID

C- UTCtime

D- Process ID or Parent Process ID

Answer:

D

Explanation:

According to theCrowdStrike 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.The tool requires two parameters:aid(agent ID) andTargetProcessId_decimal(the decimal value of the process ID)1.You can jump to a Process Timeline from many views, such as Hash Search, Host Timeline, Event Search, etc., by clicking on either the Process ID or Parent Process ID fields in those views1.This will automatically populate the aid and TargetProcessId_decimal parameters for the Process Timeline tool1.

Question 9

Question Type: **MultipleChoice**

In the Hash Search tool, which of the following is listed under Process Executions?

Options:

A- Operating System

B- File Signature

C- Command Line

D- Sensor Version

Answer:

C

Explanation:

According to theCrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Hash 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, geolocation, process name, command line, and organizational unit of the host that loaded or executed those hashes1.You can also see a count of detections and incidents related to those hashes1.Under Process Executions, you can see the process name and command line for each hash execution1.