# Free Questions for CCFR-201 by dumpssheet

## Shared by Nixon on 29-01-2024

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

**Question Type:** MultipleChoice

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

## Options:

**A-** 500

**B-** 750

**C-** 1000

**D-** 1200

## Answer:

C

## Explanation:

According to theCrowdStrike 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 limit imposed 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 2

**Question Type:** MultipleChoice

The Bulk Domain Search tool contains Domain information along with which of the following?

## Options:

**A-** Process Information

**B-** Port Information

**C-** IP Lookup Information

**D-** Threat Actor Information

## Answer:

C

## Explanation:

According to theCrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Bulk Domain Search tool allows you to search for one or more domains and view a summary of information from Falcon events that contain those domains1.The summary includes the domain name, IP address, country, city, ISP, ASN, geolocation, hostname, sensor ID, OS, process name, command line, and organizational unit of the host that communicated with those domains1.This means that the tool contains domain information along with IP lookup information1.

# Question 3

**Question Type:** MultipleChoice

Within the MITRE-Based Falcon Detections Framework, what is the correct way to interpret Keep Access > Persistence > Create Account?

## Options:

**A-** An adversary is trying to keep access through persistence by creating an account

**B-** An adversary is trying to keep access through persistence using browser extensions

**C-** An adversary is trying to keep access through persistence using external remote services

**D-** adversary is trying to keep access through persistence using application skimming

## Answer:

A

## Explanation:

According to the [CrowdStrike website], the MITRE-Based Falcon Detections Framework is a way of categorizing and describing detections based on the MITRE ATT&CK knowledge base of adversary behaviors and techniques. The framework uses three levels of granularity: category, tactic, and technique. The category is the highest level and represents the main objective of an adversary, such as initial access, execution, credential access, etc. The tactic is the second level and represents the sub-objective of an adversary within a category, such as persistence, privilege escalation, defense evasion, etc. The technique is the lowest level and represents the specific way an adversary can achieve a tactic, such as create account, modify registry, obfuscated files or information, etc. Therefore, the correct way to interpret Keep Access > Persistence > Create Account is that an adversary is trying to keep access through persistence by creating an account.

# Question 4

**Question Type:** MultipleChoice

What is an advantage of using the IP Search tool?

## Options:

**A-** IP searches provide manufacture and timezone data that can not be accessed anywhere else

**B-** IP searches allow for multiple comma separated IPv6 addresses as input

**C-** IP searches offer shortcuts to launch response actions and network containment on target hosts

**D-** IP searches provide host, process, and organizational unit data without the need to write a query

## Answer:

D

## Explanation:

According to theCrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the IP Search tool allows you to search for an IP address and view a summary of information from Falcon events that contain that IP address1.The summary includes the hostname, sensor ID, OS, country, city, ISP, ASN, geolocation, process name, command line, and organizational unit of the host that communicated with that IP address1.This is an advantage of using the IP Search tool because it provides host, process, and organizational unit data without the need to write a query1.

# Question 5

**Question Type:** MultipleChoice

What is the difference between Managed and Unmanaged Neighbors in the Falcon console?

## Options:

**A-** A managed neighbor is currently network contained and an unmanaged neighbor is uncontained

**B-** A managed neighbor has an installed and provisioned sensor

**C-** An unmanaged neighbor is in a segmented area of the network

**D-** A managed sensor has an active prevention policy

## Answer:

B

## Explanation:

According to theCrowdStrike Falcon Data Replicator (FDR) Add-on for Splunk Guide, you can use the Hosts page in the Investigate tool to view information about your endpoints, such as hostname, IP address, OS, sensor version, etc2.You can also see a list of managed and unmanaged neighbors for each endpoint, which are other devices that have communicated with that endpoint over the network2.A managed neighbor is a device that has an installed and provisioned sensor that reports to the CrowdStrike Cloud2.An unmanaged neighbor is a device that does not have an installed or provisioned sensor2.

# Question 6

**Question Type:** MultipleChoice

Which of the following is NOT a filter available on the Detections page?

## Options:

**A-** Severity

**B-** CrowdScore

**C-** Time

**D-** Triggering File

## Answer:

D

## Explanation:

According to theCrowdStrike Falcon Data Replicator (FDR) Add-on for Splunk Guide, the Detections page allows you to view and manage detections generated by the CrowdStrike Falcon platform2.You can use various filters to narrow down the detections based on criteria such as severity, CrowdScore, time, tactic, technique, etc2.However, there is no filter for triggering file, which is the file that

caused the detection2.

# Question 7

**Question Type:** MultipleChoice

What information is contained within a Process Timeline?

## Options:

**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

## Answer:

A

### 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.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 8

**Question Type:** MultipleChoice

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?

### Options:

**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

## Answer:

B

## Explanation:

According to theCrowdStrike 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.