

# CrowdStrike

## Exam Questions CCFR-201

CrowdStrike Certified Falcon Responder



#### NEW QUESTION 1

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

- A. Severity
- B. Event Types
- C. User Name
- D. Detection ID

**Answer: B**

#### Explanation:

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 order<sup>1</sup>. The events include process executions, file writes, registry modifications, network connections, user logins, etc<sup>1</sup>. 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, etc<sup>1</sup>. However, there is no filter for severity, user name, or detection ID, as these are not attributes of the events<sup>1</sup>.

#### NEW QUESTION 2

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

- 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.

#### NEW QUESTION 3

Which Executive Summary dashboard item indicates sensors running with unsupported versions?

- A. Detections by Severity
- B. Inactive Sensors
- C. Sensors in RFM
- D. Active Sensors

**Answer: C**

#### Explanation:

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Executive Summary dashboard provides an overview of your sensor health and activity<sup>1</sup>. It includes various items, such as Active Sensors, Inactive Sensors, Detections by Severity, etc<sup>1</sup>. The item that indicates sensors running with unsupported versions is Sensors in RFM (Reduced Functionality Mode)<sup>1</sup>. RFM is a state where a sensor has limited functionality due to various reasons, such as license expiration, network issues, tampering attempts, or unsupported versions<sup>1</sup>. You can see the number and percentage of sensors in RFM and the reasons why they are in RFM<sup>1</sup>.

#### NEW QUESTION 4

What do IOA exclusions help you achieve?

- A. Reduce false positives based on Next-Gen Antivirus settings in the Prevention Policy
- B. Reduce false positives of behavioral detections from IOA based detections only
- C. Reduce false positives of behavioral detections from IOA based detections based on a file hash
- D. Reduce false positives of behavioral detections from Custom IOA and OverWatch detections only

**Answer: B**

#### Explanation:

According to the CrowdStrike Falcon® Data Replicator (FDR) Add-on for Splunk Guide, IOA exclusions allow you to exclude files or directories from being detected or blocked by CrowdStrike's indicators of attack (IOAs), which are behavioral rules that identify malicious activities<sup>2</sup>. This can reduce false positives and improve performance<sup>2</sup>. IOA exclusions only apply to IOA based detections, not other types of detections such as machine learning, custom IOA, or OverWatch<sup>2</sup>.

#### NEW QUESTION 5

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

**Answer: B**

**Explanation:**

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, etc<sup>1</sup>. This allows you to see a comprehensive view of what a process was doing on a host<sup>1</sup>.

**NEW QUESTION 6**

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

**Answer:** A

**Explanation:**

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, etc<sup>1</sup>. You can specify a timeframe to limit the events to a certain period<sup>1</sup>. The tool works for any host platform, not just Mac or Linux<sup>1</sup>.

**NEW QUESTION 7**

What happens when a hash is set to Always Block through IOC Management?

- A. Execution is prevented on all hosts by default
- B. Execution is prevented on selected host groups
- C. Execution is prevented and detection alerts are suppressed
- D. The hash is submitted for approval to be blocked from execution once confirmed by Falcon specialists

**Answer:** A

**Explanation:**

According to the CrowdStrike Falcon® Data Replicator (FDR) Add-on for Splunk Guide, IOC Management allows you to manage indicators of compromise (IOCs), which are artifacts such as hashes, IP addresses, or domains that are associated with malicious activities<sup>2</sup>. You can set different actions for IOCs, such as Allow, No Action, or Always Block<sup>2</sup>. When you set a hash to Always Block through IOC Management, you are preventing that file from executing on any host in your organization by default<sup>2</sup>. This action also generates a detection alert when the file is blocked<sup>2</sup>.

**NEW QUESTION 8**

From the Detections page, how can you view 'in-progress' detections assigned to Falcon Analyst Alex?

- A. Filter on 'Analyst: Alex'
- B. Alex does not have the correct role permissions as a Falcon Analyst to be assigned detections
- C. Filter on 'Hostname: Alex' and 'Status: In-Progress'
- D. Filter on 'Status: In-Progress' and 'Assigned-to: Alex\*'

**Answer:** D

**Explanation:**

According to the CrowdStrike Falcon® Data Replicator (FDR) Add-on for Splunk Guide, the Detections page allows you to view and manage detections generated by the CrowdStrike Falcon platform<sup>2</sup>. You can use various filters to narrow down the detections based on criteria such as status, severity, tactic, technique, etc<sup>2</sup>. To view 'in-progress' detections assigned to Falcon Analyst Alex, you can filter on 'Status: In-Progress' and 'Assigned-to: Alex\*'<sup>2</sup>. The asterisk (\*) is a wildcard that matches any characters after Alex<sup>2</sup>.

**NEW QUESTION 9**

The primary purpose for running a Hash Search is to:

- A. determine any network connections
- B. review the processes involved with a detection
- C. determine the origin of the detection
- D. review information surrounding a hash's related activity

**Answer:** D

**Explanation:**

According to the CrowdStrike 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 hashes<sup>1</sup>. 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 hashes<sup>1</sup>. You can also see a count of detections and incidents related to those hashes<sup>1</sup>. The primary purpose for running a Hash Search is to review information surrounding a hash's related activity, such as which hosts and processes were involved, where they were located, and whether they triggered any alerts<sup>1</sup>.

**NEW QUESTION 10**

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?

- 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.

**NEW QUESTION 10**

In the "Full Detection Details", which view will provide an exportable text listing of events like DNS requests. Registry Operations, and Network Operations?

- A. The data is unable to be exported
- B. View as Process Tree
- C. View as Process Timeline
- D. View as Process Activity

**Answer:** D

**Explanation:**

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Full Detection Details tool allows you to view detailed information about a detection, such as detection ID, severity, tactic, technique, description, etc<sup>1</sup>. 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<sup>1</sup>. The process activity view provides a rows-and-columns style view of the events, such as DNS requests, registry operations, network operations, etc<sup>1</sup>. You can also export this view to a CSV file for further analysis<sup>1</sup>.

**NEW QUESTION 14**

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

- A. Process Information
- B. Port Information
- C. IP Lookup Information
- D. Threat Actor Information

**Answer:** C

**Explanation:**

According to the CrowdStrike 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 domains<sup>1</sup>. 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 domains<sup>1</sup>. This means that the tool contains domain information along with IP lookup information<sup>1</sup>.

**NEW QUESTION 15**

What happens when a hash is allowlisted?

- 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 the CrowdStrike 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)<sup>2</sup>. This can reduce false positives and improve performance<sup>2</sup>. When you allowlist a hash, you are allowing that file to execute on any host that belongs to your organization's CID (customer ID)<sup>2</sup>. This does not affect other Falcon customers or hosts outside your CID<sup>2</sup>.

**NEW QUESTION 16**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### CCFR-201 Practice Exam Features:

- \* CCFR-201 Questions and Answers Updated Frequently
- \* CCFR-201 Practice Questions Verified by Expert Senior Certified Staff
- \* CCFR-201 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* CCFR-201 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The CCFR-201 Practice Test Here](#)**