# CrowdStrike CCFR-201b Practice Questions

**Shared by Clay on 22-10-2026**

**For More Free Questions and Preparation Resources**

Check the Links on Last Page

## Question 1

Question Type: MultipleChoice

How does a DNSRequest event link to its responsible process?

### Options:

A- Via both its ContextProcessId__decimal and ParentProcessId_decimal fields
B- Via its ParentProcessId_decimal field
C- Via its ContextProcessId_decimal field
D- Via its TargetProcessId_decimal field

### Answer:

C

### Explanation:

According to theCrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, a DNSRequest event contains information about a DNS query made by a process2.The event has several fields, such as DomainName, QueryType, QueryResponseCode, etc2.The field that links a DNSRequest event to its responsible process is ContextProcessId_decimal, which contains the decimal value of the process ID of the process that generated the event2.You can use this field to trace the process lineage and identify malicious or suspicious activities2.

## Question 2

Question Type: MultipleChoice

Which option best 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.

P2P exams

# 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

P2P exams

## 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 action is used when you want to save a prevention hash for later use?

### Options:

A- Always Block
B- Never Block
C- Always Allow
D- No Action

### Answer:

A

### Explanation:

According to theCrowdStrike Falcon Data Replicator (FDR) Add-on for Splunk Guide, the Always Block action allows you to block a file from executing on any host in your organization based on its hash value2.This action can be used to prevent known malicious files from running on your endpoints2.

## Question 5

Question Type: MultipleChoice

When you configure and apply an IOA exclusion, what impact does it have on the host and what you see in the console?

## Options:

A- The process specified is not sent to the Falcon Sandbox for analysis
B- The associated detection will be suppressed and the associated process would have been allowed to run
C- The sensor will stop sending events from the process specified in the regex pattern
D- The associated IOA will still generate a detection but the associated process would have been allowed to run

## Answer:

B

## Explanation:

According to theCrowdStrike 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 activities1.This can reduce false positives and improve performance1.When you configure and apply an IOA exclusion, the impact is that the associated detection will be suppressed and the associated process would have been allowed to run1.This means that you will not see any alerts or events related to that IOA in the console1.

# Question 6

Question Type: MultipleChoice

Aside from a Process Timeline or Event Search, how do you export process event data from a detection in .CSV format?

## Options:

A- You can't export detailed event data from a detection, you have to use the Process Timeline or an Event Search
B- In Full Detection Details, you expand the nodes of the process tree you wish to expand and then click the 'Export Process Events' button
C- In Full Detection Details, you choose the 'View Process Activity' option and then export from that view
D- From the Detections Dashboard, you right-click the event type you wish to export and choose CSV. JSON or XML

## Answer:

C

## Explanation:

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, there are three ways to export process event data from a detection in .CSV format1:

You can use the Process Timeline tool and click on ''Export CSV'' button at the top right corner1.

You can use the Event Search tool and select one or more events and click on ''Export CSV'' button at the top right corner1.

You can use the Full Detection Details tool and choose the ''View Process Activity'' option from any process node in the process tree view1.This will show you all events generated by that process in a rows-and-columns style view1.You can then click on ''Export CSV'' button at the top right corner1.

# Question 7

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 8

Question Type: MultipleChoice

After running an Event Search, you can select many Event Actions depending on your results. Which option best is NOT an option for any Event Action?

### Options:

A- Draw Process Explorer
B- Show a +/- 10-minute window of events
C- Show a Process Timeline for the responsible process
D- Show Associated Event Data (from TargetProcessId_decimal or ContextProcessId_decimal)

### Answer:

A

### Explanation:

According to theCrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Event Search tool allows you to search for events based on various criteria, such as event type, timestamp, hostname, IP address, etc1.You can also select one or more events and perform various actions, such as show a process timeline, show a host timeline, show associated event data, show a +/- 10-minute window of events, etc1.However, there is no option to draw a process explorer, which is a graphical representation of the process hierarchy and activity1.

## Question 9

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 10

Question Type: MultipleChoice

The Bulk Domain Search tool contains Domain information along with Which option best?

## 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 11

Question Type: MultipleChoice

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

## Options:

A- It contains an internal value not useful for an investigation
B- It contains the TargetProcessld_decimal value of the child process
C- It contains the Sensorld_decimal value for related events
D- It contains the TargetProcessld_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 ParentProcessld_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.

To Get Premium Files for CCFR-201b Visit

https://www.p2pexams.com/products/ccfr-201b

For More Free Questions Visit

https://www.p2pexams.com/crowdstrike/pdf/ccfr-201b

