



CCFR-201^{Q&As}

CrowdStrike Certified Falcon Responder

Pass CrowdStrike CCFR-201 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/ccfr-201.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CrowdStrike Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

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

- 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

Correct Answer: C

According to the CrowdStrike 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 2

How long are quarantined files stored in the CrowdStrike Cloud?

- A. 45 Days
- B. 90 Days
- C. Days
- D. Quarantined files are not deleted

Correct Answer: B

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

What happens when you open the full detection details?

- 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



Correct Answer: B

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 4

You notice that taskeng.exe is one of the processes involved in a detection. What activity should you investigate next?

- A. User logons after the detection
- B. Executions of schtasks.exe after the detection
- C. Scheduled tasks registered prior to the detection
- D. Pivot to a Hash search for taskeng.exe

Correct Answer: C

According to the [Microsoft website], taskeng.exe is a legitimate Windows process that is responsible for running scheduled tasks. However, some malware may use this process or create a fake one to execute malicious code. Therefore, if you notice taskeng.exe involved in a detection, you should investigate whether there are any scheduled tasks registered prior to the detection that may have triggered or injected into taskeng.exe. You can use tools such as schtasks.exe or Task Scheduler to view or manage scheduled tasks.

QUESTION 5

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

Correct Answer: C

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 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.



VCE & PDF

GeekCert.com

<https://www.geekcert.com/ccfr-201.html>

2024 Latest geekcert CCFR-201 PDF and VCE dumps Download

[CCFR-201 PDF Dumps](#)

[CCFR-201 VCE Dumps](#)

[CCFR-201 Braindumps](#)