

Exam Questions CCFR-201

CrowdStrike Certified Falcon Responder

<https://www.2passeasy.com/dumps/CCFR-201/>



NEW QUESTION 1

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

- A. Severity
- B. CrowdScore
- C. Time
- D. Triggering File

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 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.

NEW QUESTION 2

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

- A. It contains an internal value not useful for an investigation
- B. It contains the TargetProcessId_decimal value of the child process
- C. It contains the SensorId_decimal value for related events
- D. It contains the TargetProcessId_decimal of the parent process

Answer: D

Explanation:

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the ParentProcessId_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.

NEW QUESTION 3

What information does the MITRE ATT&CK® Framework provide?

- A. It provides best practices for different cybersecurity domains, such as Identify and Access Management
- B. It provides a step-by-step cyber incident response strategy
- C. It provides the phases of an adversary's lifecycle, the platforms they are known to attack, and the specific methods they use
- D. It is a system that attributes an attack techniques to a specific threat actor

Answer: C

Explanation:

According to the [MITRE ATT&CK website], MITRE ATT&CK is a knowledge base of adversary behaviors and techniques based on real-world observations. The knowledge base is organized into tactics and techniques, where tactics are the high-level goals of an adversary, such as initial access, persistence, lateral movement, etc., and techniques are the specific ways an adversary can achieve those goals, such as phishing, credential dumping, remote file copy, etc. The knowledge base also covers different platforms that adversaries target, such as Windows, Linux, Mac, Android, iOS, etc., and different phases of an adversary's lifecycle, such as reconnaissance, resource development, execution, command and control, etc.

NEW QUESTION 4

What is the difference between a Host Search and a Host Timeline?

- A. Results from a Host Search return information in an organized view by type, while a Host Timeline returns a view of all events recorded by the sensor
- B. A Host Timeline only includes process execution events and user account activity
- C. Results from a Host Timeline include process executions and related events organized by data type
- D. A Host Search returns a temporal view of all events for the given host
- E. There is no difference - Host Search and Host Timeline are different names for the same search page

Answer: A

Explanation:

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Host Search allows you to search for hosts based on various criteria, such as hostname, IP address, OS, etc¹. The results are displayed in an organized view by type, such as detections, incidents, processes, network connections, etc¹. The Host Timeline allows you to view all events recorded by the sensor for a given host in a chronological order¹. The events include process executions, file writes, registry modifications, network connections, user logins, etc¹.

NEW QUESTION 5

Sensor Visibility Exclusion patterns are written in which syntax?

- 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.

NEW QUESTION 6

The function of Machine Learning Exclusions is to .

- 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 the CrowdStrike 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.

NEW QUESTION 7

How long are quarantined files stored on the host?

- A. 45 Days
- B. 30 Days
- C. Quarantined files are never deleted from the host
- D. 90 Days

Answer: C

Explanation:

According to the CrowdStrike 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.

NEW QUESTION 8

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 activity¹. It includes various items, such as Active Sensors, Inactive Sensors, Detections by Severity, etc¹. The item that indicates sensors running with unsupported versions is Sensors in RFM (Reduced Functionality Mode)¹. RFM is a state where a sensor has limited functionality due to various reasons, such as license expiration, network issues, tampering attempts, or unsupported versions¹. You can see the number and percentage of sensors in RFM and the reasons why they are in RFM¹.

NEW QUESTION 9

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 activities². This can reduce false positives and improve performance². IOA exclusions only apply to IOA based detections, not other types of detections such as machine learning, custom IOA, or OverWatch².

NEW QUESTION 10

Which statement is TRUE regarding the "Bulk Domains" search?

- A. It will show a list of computers and process that performed a lookup of any of the domains in your search
- B. The "Bulk Domains" search will allow you to blocklist your queried domains
- C. The "Bulk Domains" search will show IP address and port information for any associated connections
- D. You should only pivot to the "Bulk Domains" search tool after completing an investigation

Answer: A

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 domains². The summary includes the hostname, sensor ID, OS, country, city, ISP, ASN, geolocation, process name, command line, and organizational unit of the host that performed a lookup of any of the domains in your search². This can help you identify potential threats or vulnerabilities in your network².

NEW QUESTION 10

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, 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.

NEW QUESTION 12

Which is TRUE regarding a file released from quarantine?

- A. No executions are allowed for 14 days after release
- B. It is allowed to execute on all hosts
- C. It is deleted
- D. It will not generate future machine learning detections on the associated host

Answer: B

Explanation:

According to the CrowdStrike Falcon® Data Replicator (FDR) Add-on for Splunk Guide, 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.

NEW QUESTION 15

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 activities². You can set different actions for IOCs, such as Allow, No Action, or Always Block². 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 default². This action also generates a detection alert when the file is blocked².

NEW QUESTION 18

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?

- 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 the CrowdStrike 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.

NEW QUESTION 21

From a detection, what is the fastest way to see children and sibling process information?

- A. Select the Event Search option
- B. Then from the Event Actions, select Show Associated Event Data (From TargetProcessId_decimal)
- C. Select Full Detection Details from the detection
- D. Right-click the process and select "Follow Process Chain"
- E. Select the Process Timeline feature, enter the AI
- F. Target Process ID, and Parent Process ID

Answer:

B

Explanation:

According to the CrowdStrike Falcon® Data Replicator (FDR) Add-on for Splunk Guide, the Full Detection Details tool allows you to view detailed information about a detection, such as detection ID, severity, tactic, technique, description, etc¹. 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 activity¹. The process tree view provides a graphical representation of the process hierarchy and activity¹. You can see children and sibling processes information by expanding or collapsing nodes in the tree¹.

NEW QUESTION 25

Where can you find hosts that are in Reduced Functionality Mode?

- A. Event Search
- B. Executive Summary dashboard
- C. Host Search
- D. Installation Tokens

Answer: C

Explanation:

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, Reduced Functionality Mode (RFM) is a state where a host's sensor has limited functionality due to various reasons, such as license expiration, network issues, tampering attempts, etc¹. You can find hosts that are in RFM by using the Host Search tool and filtering by Sensor Status = RFM¹. You can also view details about why a host is in RFM by clicking on its hostname¹.

NEW QUESTION 26

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 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.

NEW QUESTION 27

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

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.

NEW QUESTION 32

How long does detection data remain in the CrowdStrike Cloud before purging begins?

- A. 90 Days
- B. 45 Days
- C. 30 Days
- D. 14 Days

Answer: A

Explanation:

According to the CrowdStrike Falcon® Data Replicator (FDR) Add-on for Splunk Guide, detection data is stored in the CrowdStrike Cloud for 90 days before purging begins². This means that you can access and view detections from the past 90 days using the Falcon platform or API². If you want to retain detection data for longer than 90 days, you can use FDR to replicate it to your own storage system².

NEW QUESTION 34

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CCFR-201 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CCFR-201 Product From:

<https://www.2passeasy.com/dumps/CCFR-201/>

Money Back Guarantee

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