



CrowdStrike

Exam Questions CCFR-201

CrowdStrike Certified Falcon Responder

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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

After pivoting to an event search from a detection, you locate the ProcessRollup2 event. Which two field values are you required to obtain to perform a Process Timeline search so you can determine what the process was doing?

- A. SHA256 and TargetProcessId_decimal
- B. SHA256 and ParentProcessId_decimal
- C. aid and ParentProcessId_decimal
- D. aid and TargetProcessId_decimal

Answer: D

Explanation:

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Process Timeline search requires two parameters: aid (agent ID) and TargetProcessId_decimal (the decimal value of the process ID). These fields can be obtained from the ProcessRollup2 event, which contains information about processes that have executed on a host¹.

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

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 order¹. The events include process executions, file writes, registry modifications, network connections, user logins, etc¹. 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, etc¹. However, there is no filter for severity, user name, or detection ID, as these are not attributes of the events¹.

NEW QUESTION 5

You are notified by a third-party that a program may have redirected traffic to a malicious domain. Which Falcon page will assist you in searching for any domain request information related to this notice?

- A. Falcon X
- B. Investigate
- C. Discover
- D. Spotlight

Answer: B

Explanation:

According to the [CrowdStrike website], the Investigate page is where you can search for and analyze various types of data collected by the Falcon platform, such as events, hosts, processes, hashes, domains, IPs, etc¹. You can use various tools, such as Event Search, Host Search, Process Timeline, Hash Search, Bulk Domain Search, etc., to perform different types of searches and view the results in different ways¹. If you want to search for any domain request information related to a notice from a third-party, you can use the Investigate page to do so¹. For example, you can use the Bulk Domain Search tool to search for the malicious domain and see which hosts and processes communicated with it¹. You can also use the Event Search tool to search for DNSRequest events that contain the malicious domain and see more details about the query and response¹.

NEW QUESTION 6

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

- 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 CS
- E. 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.

NEW QUESTION 7

Which option indicates a hash is allowlisted?

- A. No Action
- B. Allow
- C. Ignore
- D. Always Block

Answer: B

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)². This can reduce false positives and improve performance². When you allowlist a hash, you are allowing that file to execute on any host that belongs to your organization's CID (customer ID)². The option to indicate that a hash is allowlisted is "Allow"².

NEW QUESTION 8

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, etc¹. This allows you to see a comprehensive view of what a process was doing on a host¹.

NEW QUESTION 9

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

Answer: C

Explanation:

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.

NEW QUESTION 10

What happens when a quarantined file is released?

- A. It is moved into the C:\CrowdStrike\Quarantine\Released folder on the host
- B. It is allowed to execute on the host
- C. It is deleted

D. It is allowed to execute on all hosts

Answer: D

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 organization¹. This action also removes the file from the quarantine list and deletes it from the CrowdStrike Cloud¹.

NEW QUESTION 10

When looking at the details of a detection, there are two fields called Global Prevalence and Local Prevalence. Which answer best defines Local Prevalence?

- A. Local prevalence is the frequency with which the hash of the triggering file is seen across the entire Internet
- B. Local Prevalence tells you how common the hash of the triggering file is within your environment (CID)
- C. Local Prevalence is the Virus Total score for the hash of the triggering file
- D. Local prevalence is the frequency with which the hash of the triggering file is seen across all CrowdStrike customer environments

Answer: B

Explanation:

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, Global Prevalence and Local Prevalence are two fields that provide information about how common or rare a file is based on its hash value². Global Prevalence tells you how frequently the hash of the triggering file is seen across all CrowdStrike customer environments². Local Prevalence tells you how frequently the hash of the triggering file is seen within your environment (CID)². These fields can help you assess the risk and impact of a detection².

NEW QUESTION 13

What is an advantage of using the IP Search tool?

- 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 the CrowdStrike 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.

NEW QUESTION 17

What does pivoting to an Event Search from a detection do?

- A. It gives you the ability to search for similar events on other endpoints quickly
- B. It takes you to the raw Insight event data and provides you with a number of Event Actions
- C. It takes you to a Process Timeline for that detection so you can see all related events
- D. It allows you to input an event type, such as DNS Request or ASEP write, and search for those events within the detection

Answer: B

Explanation:

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, pivoting to an Event Search from a detection takes you to the raw Insight event data and provides you with a number of Event Actions¹. Insight events are low-level events that are generated by the sensor for various activities, such as process executions, file writes, registry modifications, network connections, etc¹. You can view these events in a table format and use various filters and fields to narrow down the results¹. 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. These actions can help you investigate and analyze events more efficiently and effectively¹.

NEW QUESTION 19

What is an advantage of using a Process Timeline?

- A. Process related events can be filtered to display specific event types
- B. Suspicious processes are color-coded based on their frequency and legitimacy over time
- C. Processes responsible for spikes in CPU performance are displayed overtime
- D. A visual representation of Parent-Child and Sibling process relationships is provided

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, etc². You can also filter the events by various criteria, such as event type, timestamp range, file name, registry key, network destination, etc². This is an advantage of using the Process Timeline tool because it allows you to focus on specific events that are relevant to your investigation².

NEW QUESTION 22

The Process Activity View provides a rows-and-columns style view of the events generated in a detection. Why might this be helpful?

- A. The Process Activity View creates a consolidated view of all detection events for that process that can be exported for further analysis
- B. The Process Activity View will show the Detection time of the earliest recorded activity which might indicate first affected machine
- C. The Process Activity View only creates a summary of Dynamic Link Libraries (DLLs) loaded by a process
- D. The Process Activity View creates a count of event types only, which can be useful when scoping the event

Answer: A

Explanation:

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Process Activity View allows you to view all events generated by a process involved in a detection in a rows-and-columns style view¹. This can be helpful because it creates a consolidated view of all detection events for that process that can be exported for further analysis¹. You can also sort, filter, and pivot on the events by various fields, such as event type, timestamp, file name, registry key, network destination, etc¹.

NEW QUESTION 24

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

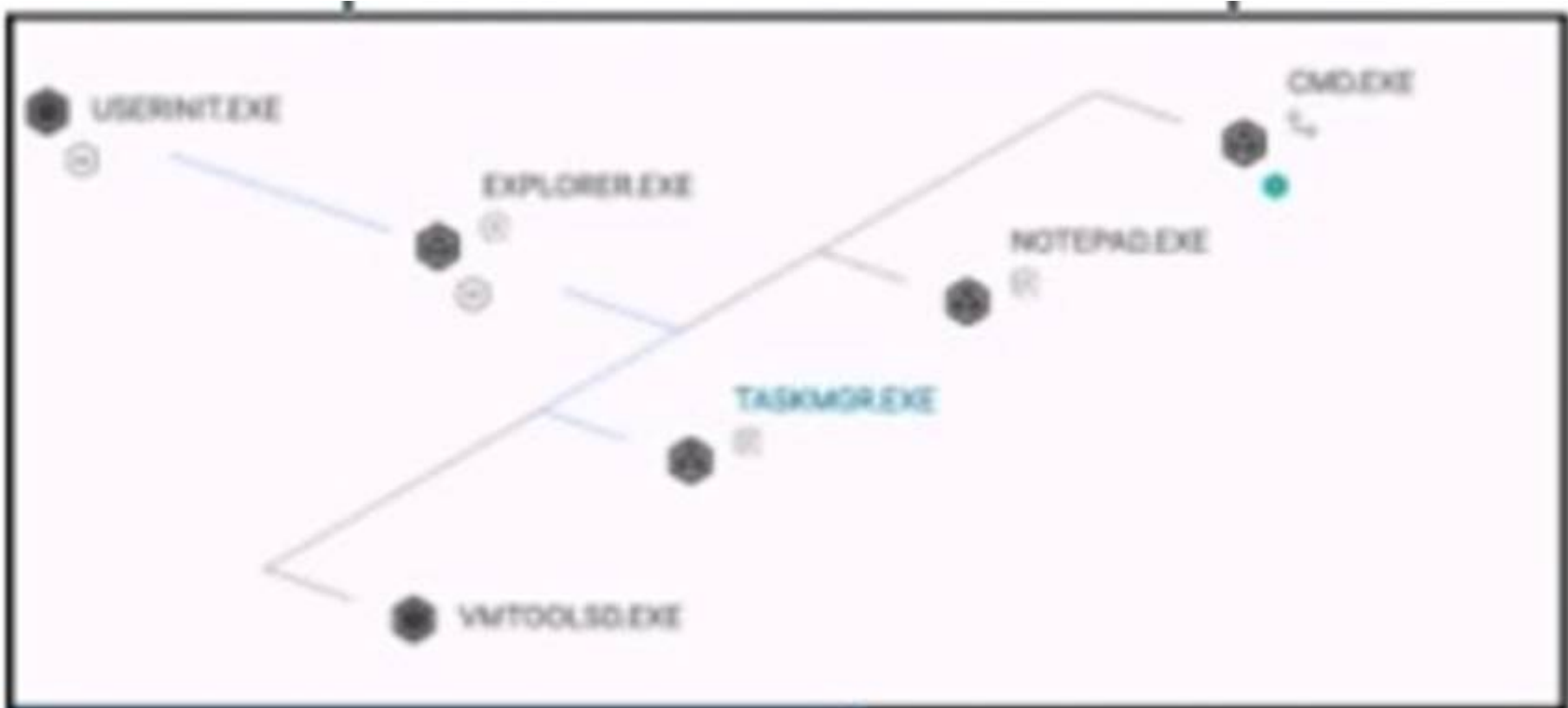
Answer: A


Explanation:

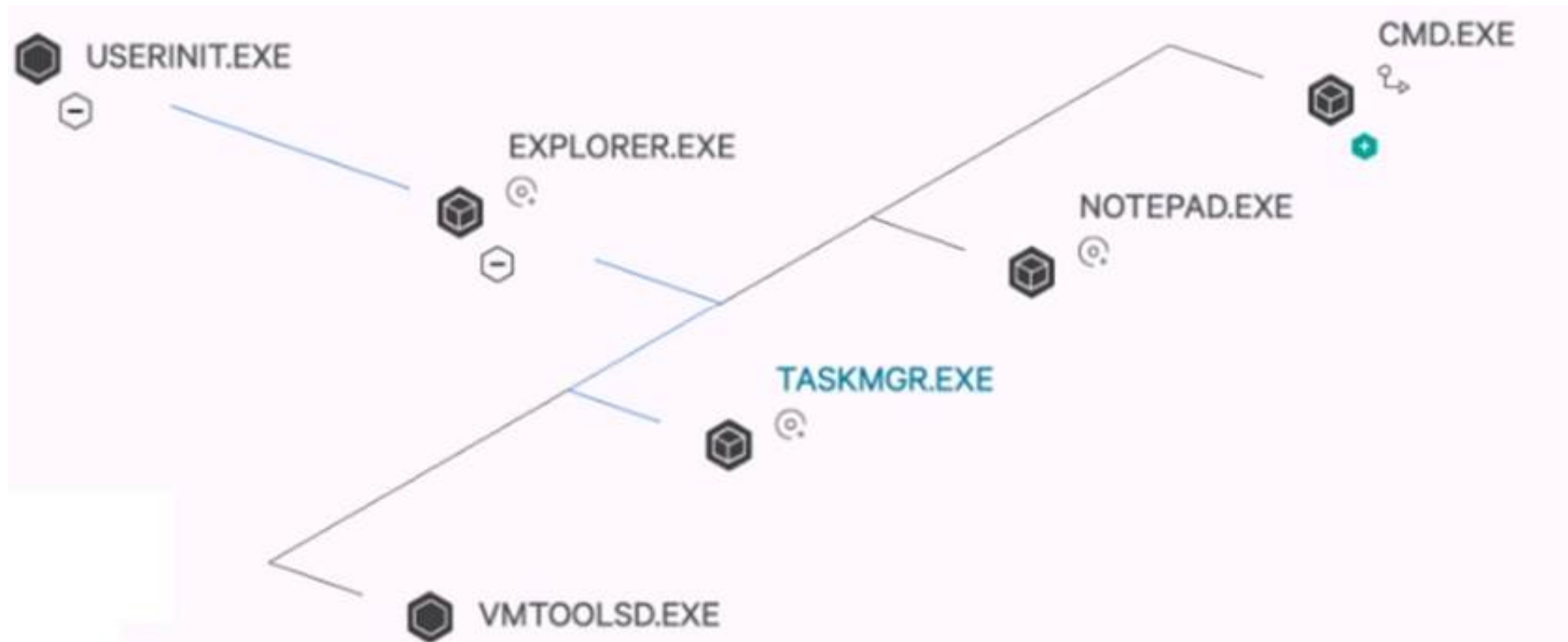
According to the CrowdStrike Falcon® Data Replicator (FDR) Add-on for Splunk Guide, IOC Management allows you to manage indicators of compromise (IOCs), which are artifacts such as hashes, IP addresses, or domains that are associated with malicious activities². You can set different actions for IOCs, 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 26

How are processes on the same plane ordered (bottom 'VMTOOLS.DEXE' to top CMD.EXE')?



 Click to Enlarge



- A. Process ID (Descending, highest on bottom)
- B. Time started (Descending, most recent on bottom)
- C. Time started (Ascending, most recent on top)
- D. Process ID (Ascending, highest on top)

Answer: B

Explanation:

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the process tree view provides a visualization of program ancestry, which shows the parent-child and sibling relationships among the processes¹. You can also see the event types and timestamps for each process¹. The processes on the same plane are ordered by time started in descending order, meaning that the most recent process is at the bottom and the oldest process is at the top¹. For example, in the image you sent me, CMD.EXE is the oldest process and VMTOOLSD.EXE is the most recent process on that plane¹.

NEW QUESTION 27

What does the Full Detection Details option provide?

- A. It provides a visualization of program ancestry via the Process Tree View
- B. It provides a visualization of program ancestry via the Process Activity View
- C. It provides detailed list of detection events via the Process Table View
- D. It provides a detailed list of detection events via the Process Tree View

Answer: A

Explanation:

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Full Detection Details option 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 visualization of program ancestry, which shows the parent-child and sibling relationships among the processes¹. You can also see the event types and timestamps for each process¹.

NEW QUESTION 28

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

- 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 the CrowdStrike 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.

NEW QUESTION 33

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

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

Answer: A

Explanation:

According to the CrowdStrike 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.

NEW QUESTION 36

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)². This can reduce false positives and improve performance². When you allowlist a hash, you are allowing that file to execute on any host that belongs to your organization's CID (customer ID)². This does not affect other Falcon customers or hosts outside your CID².

NEW QUESTION 39

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 43

.....

Relate Links

100% Pass Your CCFR-201 Exam with Examible Prep Materials

<https://www.exambible.com/CCFR-201-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>