



CrowdStrike

Exam Questions CCFR-201

CrowdStrike Certified Falcon Responder

NEW QUESTION 1

When examining a raw DNS request event, you see a field called ContextProcessId_decimal. What is the purpose of that field?

- A. It contains the TargetProcessId_decimal value for other related events
- B. It contains an internal value not useful for an investigation
- C. It contains the ContextProcessId_decimal value for the parent process that made the DNS request
- D. It contains the TargetProcessId_decimal value for the process that made the DNS request

Answer: D

Explanation:

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the ContextProcessId_decimal field contains the decimal value of the process ID of the process that generated the event¹. This field can be used to trace the process lineage and identify malicious or suspicious activities¹. For a DNS request event, this field indicates which process made the DNS request¹.

NEW QUESTION 2

You are reviewing the raw data in an event search from a detection tree. You find a FileOpenInfo event and want to find out if any other files were opened by the responsible process. Which two field values do you need from this event to perform a Process Timeline search?

- A. ParentProcessId_decimal and aid
- B. ResponsibleProcessId_decimal and aid
- C. ContextProcessId_decimal and aid
- D. TargetProcessId_decimal and aid

Answer: D

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. The tool requires two parameters: aid (agent ID) and TargetProcessId_decimal (the decimal value of the process ID)². These fields can be obtained from any event that involves the process, such as a FileOpenInfo event, which contains information about a file being opened by a process².

NEW QUESTION 3

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 4

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 5

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 6

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 7

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 8

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 9

What is the difference between Managed and Unmanaged Neighbors in the Falcon console?

- A. A managed neighbor is currently network contained and an unmanaged neighbor is uncontained
- B. A managed neighbor has an installed and provisioned sensor
- C. An unmanaged neighbor is in a segmented area of the network
- D. A managed sensor has an active prevention policy

Answer: B

Explanation:

According to the CrowdStrike Falcon® Data Replicator (FDR) Add-on for Splunk Guide, you can use the Hosts page in the Investigate tool to view information about your endpoints, such as hostname, IP address, OS, sensor version, etc². You can also see a list of managed and unmanaged neighbors for each endpoint, which are other devices that have communicated with that endpoint over the network². A managed neighbor is a device that has an installed and provisioned sensor that reports to the CrowdStrike Cloud². An unmanaged neighbor is a device that does not have an installed or provisioned sensor².

NEW QUESTION 10

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 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 14

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

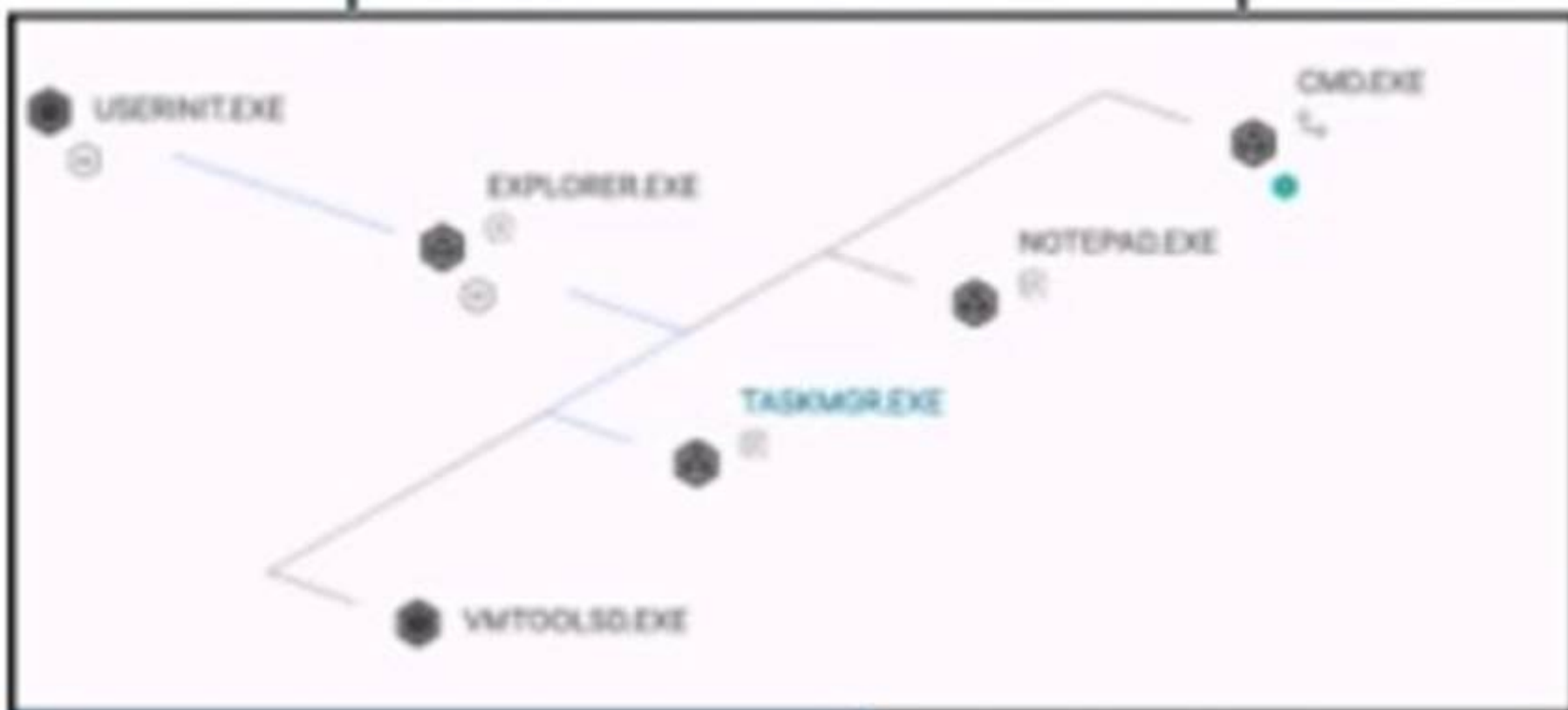
Answer: A


Explanation:

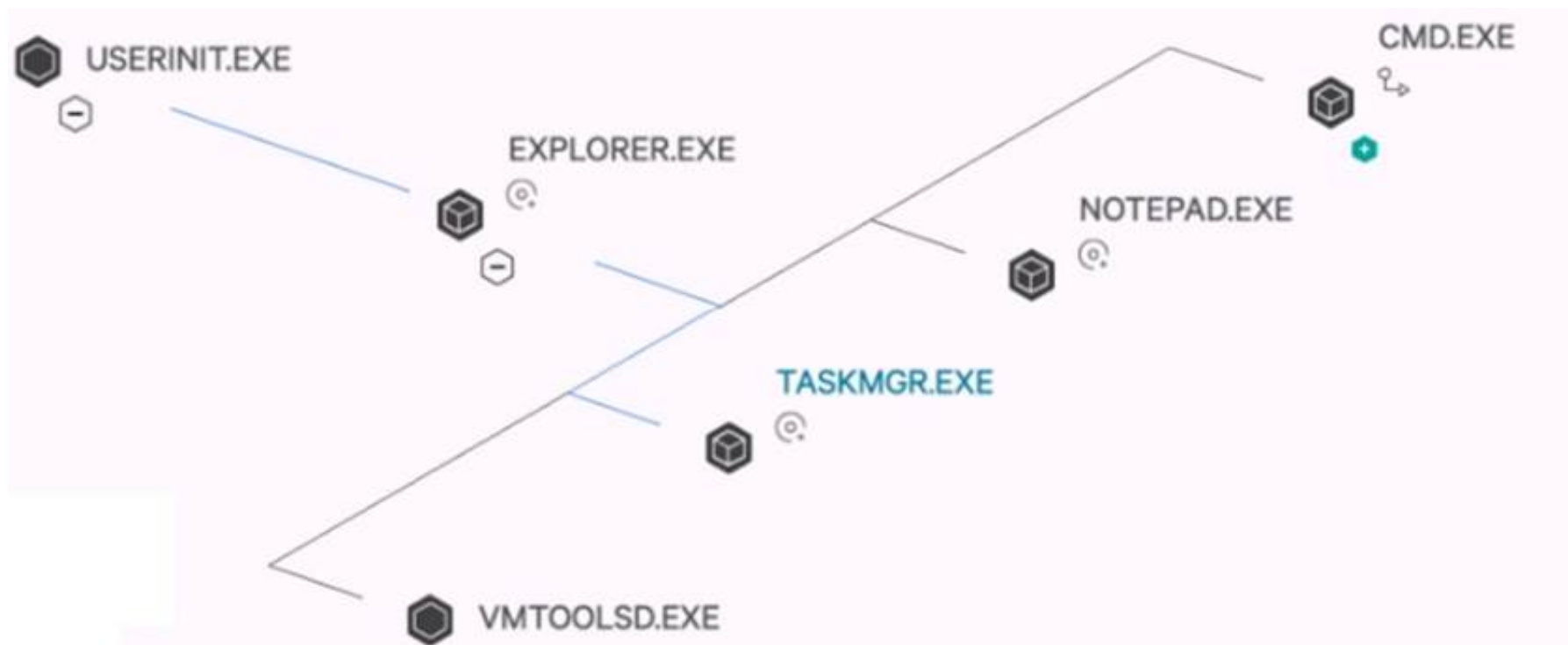
According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Process Timeline tool allows you to view all cloudable events associated with a given process, such as process creation, network connections, file writes, registry modifications, etc². You 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 18

How are processes on the same plane ordered (bottom 'VMTOOLSD.EXE' 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 22

What are Event Actions?

- A. Automated searches that can be used to pivot between related events and searches
- B. Pivotal hyperlinks available in a Host Search
- C. Custom event data queries bookmarked by the currently signed in Falcon user
- D. Raw Falcon event data

Answer: A

Explanation:

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, Event Actions are automated searches that can be used to pivot between related events and searches¹. They are available in various tools, such as Event Search, Process Timeline, Host Timeline, etc¹. You can 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 23

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 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 hashes¹. 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 hashes¹. You can also see a count of detections and incidents related to those hashes¹. 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 alerts¹.

NEW QUESTION 30

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, 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 activity view provides a rows-and-columns style view of the events, such as DNS requests, registry operations, network operations, etc¹. You can also export this view to a CSV file for further analysis¹.

NEW QUESTION 33

When analyzing an executable with a global prevalence of common; but you do not know what the executable is. what is the best course of action?

- A. Do nothing, as this file is common and well known
- B. From detection, click the VT Hash button to pivot to VirusTotal to investigate further
- C. From detection, use API manager to create a custom blocklist
- D. From detection, submit to FalconX for deep dive analysis

Answer: B

Explanation:

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, global prevalence is a field that indicates how frequently the hash of a file is seen across all CrowdStrike customer environments¹. A global prevalence of common means that the file is widely distributed and likely benign¹. However, if you do not know what the executable is, you may want to investigate it further to confirm its legitimacy and functionality¹. One way to do that is to click the VT Hash button from the detection, which will pivot you to VirusTotal, a service that analyzes files and URLs for viruses, malware, and other threats¹. You can then see more information about the file, such as its name, size, type, signatures, detections, comments, etc¹.

NEW QUESTION 34

You can jump to a Process Timeline from many views, like a Hash Search, by clicking which of the following?

- A. ProcessTimeline Link
- B. PID
- C. UTCtime
- D. Process ID or Parent Process ID

Answer: D

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. The tool requires two parameters: aid (agent ID) and TargetProcessId_decimal (the decimal value of the process ID)¹. You can jump to a Process Timeline from many views, such as Hash Search, Host Timeline, Event Search, etc., by clicking on either the Process ID or Parent Process ID fields in those views¹. This will automatically populate the aid and TargetProcessId_decimal parameters for the Process Timeline tool¹.

NEW QUESTION 35

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 38

Which of the following is returned from the IP Search tool?

- A. IP Summary information from Falcon events containing the given IP
- B. Threat Graph Data for the given IP from Falcon sensors
- C. Unmanaged host data from system ARP tables for the given IP
- D. IP Detection Summary information for detection events containing the given IP

Answer:

A

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, and geolocation of the host that communicated with that IP address¹.

NEW QUESTION 40

.....

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 First Try
- * CCFR-201 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

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