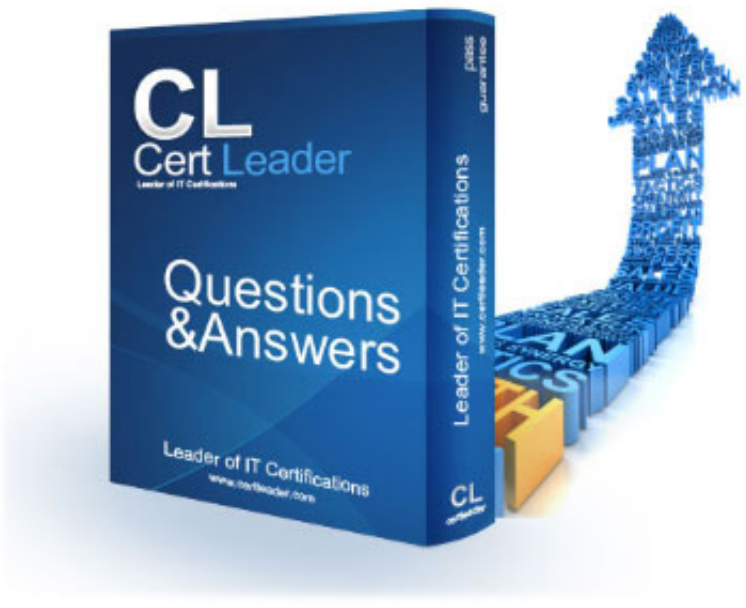
CCFR-201 Dumps

CrowdStrike Certified Falcon Responder

https://www.certleader.com/CCFR-201-dumps.html



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 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 3
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 4
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 5
How does a DNSRequest event link to its responsible process?

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 the CrowdStrike 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.

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 bythat process in a rows-and-columns style view1. You can then click on ??Export CSV?? button at the top right corner1.

NEW QUESTION 7
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 improveperformance2. You can also choose whether to upload the excluded files to the CrowdStrike Cloud or not2.

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
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

Answer: C

Explanation:
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.

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 10
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 14
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 17
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 connectionsD.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 20
How long are quarantined files stored in the CrowdStrike Cloud?

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

Answer: B

Explanation:
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.

NEW QUESTION 23
Where are quarantined files stored on Windows hosts?

A. Windows\Quarantine
B. Windows\System32\Drivers\CrowdStrike\Quarantine

C. Windows\System32\
D. Windows\temp\Drivers\CrowdStrike\Quarantine

Answer: B

Explanation:
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 executed2. The file is also encrypted and renamed with a random string of characters2. On Windows hosts, quarantined files are stored in C:\Windows\System32\Drivers\CrowdStrike\Quarantine folder2.

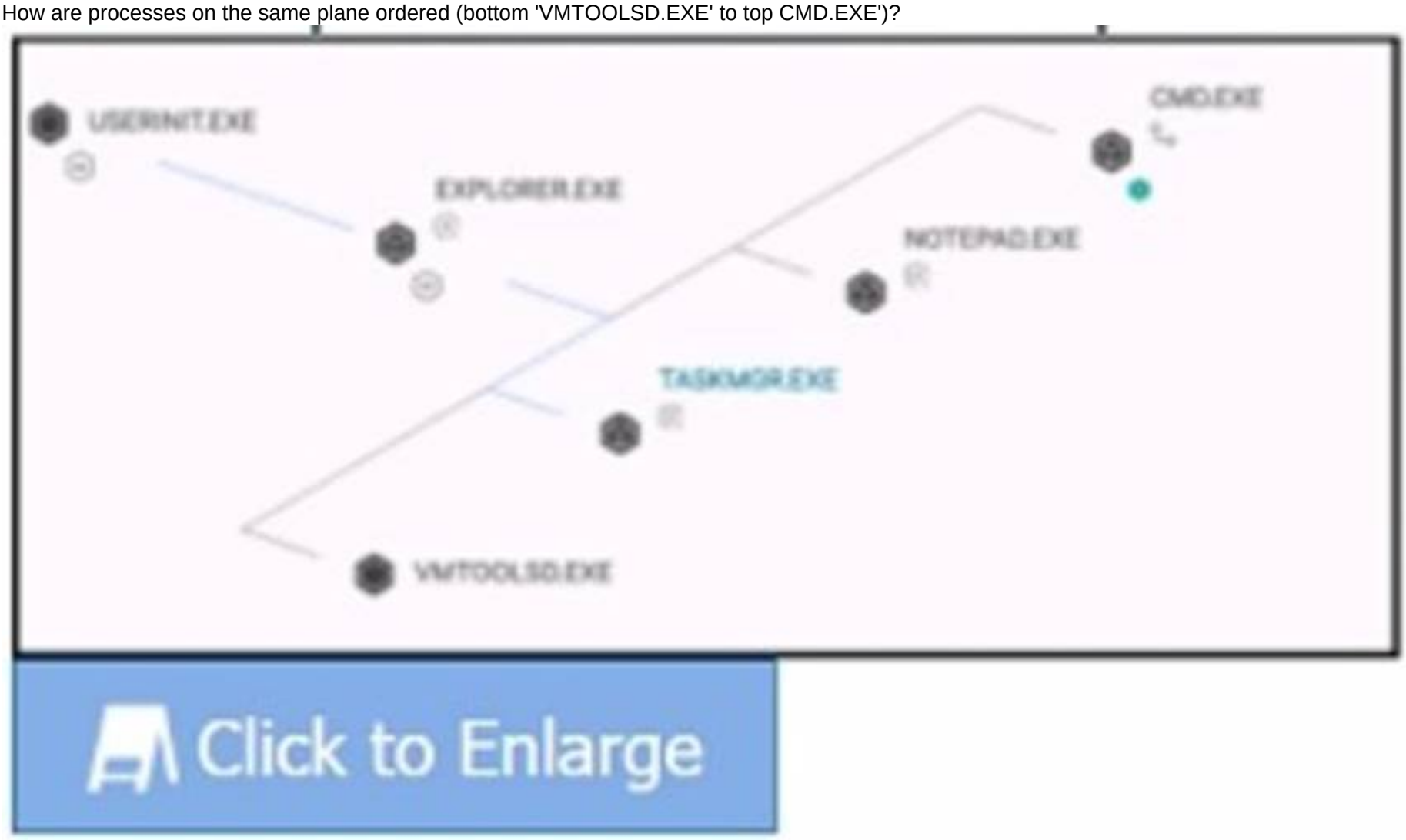
NEW QUESTION 26
From the Detections page, how can you view 'in-progress' detections assigned to Falcon Analyst Alex?

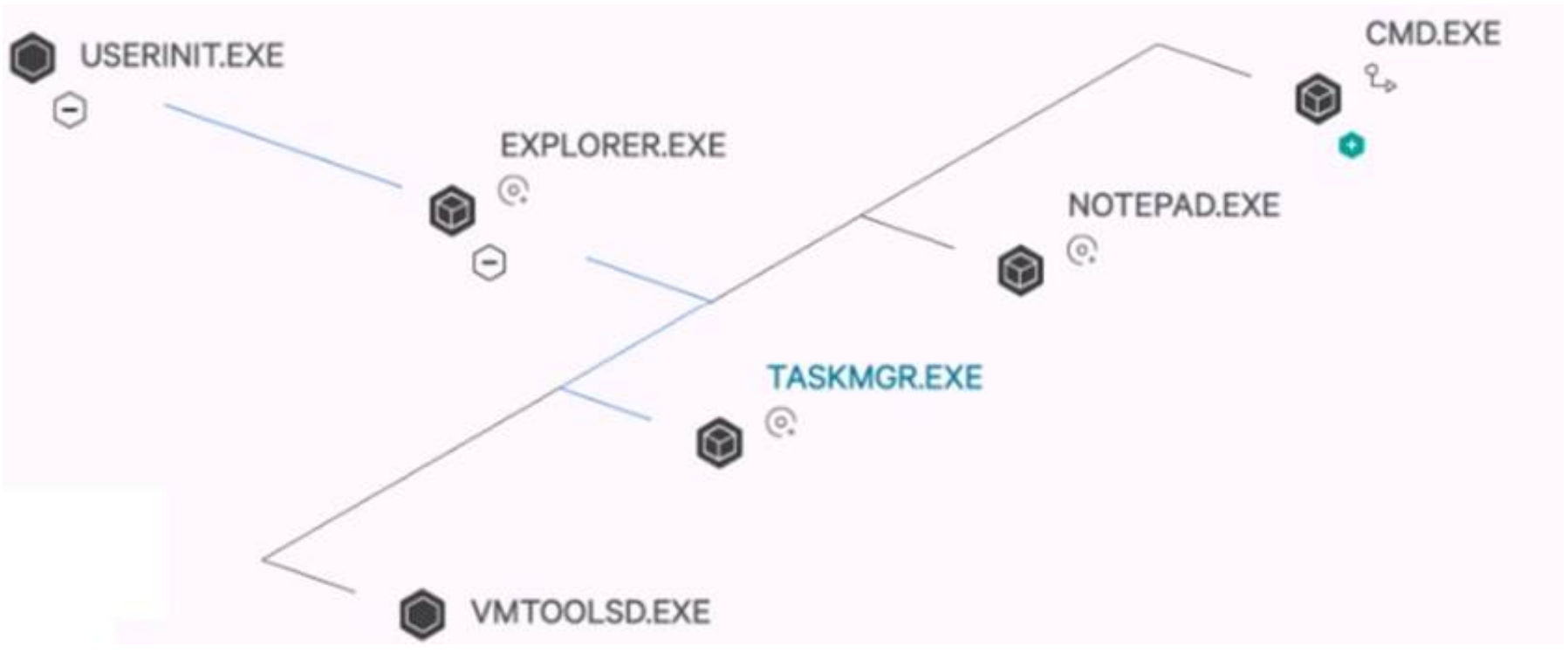
A. Filter on'Analyst: Alex'
B. Alex does not have the correct role permissions as a Falcon Analyst to be assigned detections
C. Filter on 'Hostname: Alex' and 'Status: In-Progress'
D. Filter on 'Status: In-Progress' and 'Assigned-to: Alex*

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 asstatus, severity, tactic, technique, etc2. To view ??in-progress?? detections assigned to Falcon Analyst Alex, you can filter on ??Status: In-Progress?? and 'Assigned-to: Alex*'2. The asterisk (*) is a wildcard that matches any characters after Alex2.

NEW QUESTION 28
How are processes on the same plane ordered (bottom 'VMTOOLSD.EXE' to top CMD.EXE')?





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 31
From a detection, what is the fastest way to see children and sibling process information?

A. Select the Event Search optio
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 35
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 40
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 43
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 45
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 48
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 51
Which of the following tactic and technique combinations is sourced from MITRE ATT&CK information?

A. Falcon Intel via Intelligence Indicator - Domain
B. Machine Learning via Cloud-Based ML
C. Malware via PUP
D. Credential Access via OS Credential Dumping

Answer: D

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. Credential Access via OS Credential Dumping is an example of a tactic and technique combination sourced from MITRE ATT&CK information, which describes how adversaries can obtain credentials from operating system memory or disk storage by using tools such as Mimikatz or ProcDump.

NEW QUESTION 54
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 55
What happens when you open the full detection details?

A. Theprocess 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 58

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CCFR-201 Exam with Our Prep Materials Via below:

https://www.certleader.com/CCFR-201-dumps.html