Exam Questions CCFR-201

CrowdStrike Certified Falcon Responder

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

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

A. It provides best practices for different cybersecurity domains, such as Identify andAccess 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 5
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 6
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 7
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 8
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 ofadversary 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 9
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 10
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 10
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 12
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 14
In the Hash Search tool, which of the following is listed under Process Executions?

A. Operating System
B. File Signature
C. Command Line
D. Sensor Version

Answer: C

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. Under Process Executions, you can see the process name and command line for each hash execution1.

NEW QUESTION 18
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 20
Which of the following is NOT a valid event type?

A. StartofProcess
B. EndofProcess
C. ProcessRollup2
D. DnsRequest

Answer: B

Explanation:
According to the [CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+], event types are categories of events that are generated by the sensor for various activities, such as process executions, file writes, registry modifications, network connections, etc. There are many valid event types, such as StartOfProcess, ProcessRollup2, DnsRequest, etc. However, EndOfProcess is not a valid event type, as there is no such event that records the end of a process.

NEW QUESTION 24
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 25
The Falcon platform will show a maximum of how many detections per day for a single Agent Identifier (AID)?

A. 500
B. 750
C. 1000
D. 1200

Answer: C

Explanation:
According to the CrowdStrike Falcon® Data Replicator (FDR) Add-on for Splunk Guide, the Falcon platform will show a maximum of 1000 detections per day for a single AID1. This is a limitimposed by the Falcon API, which is used to retrieve the detections from the CrowdStrike Cloud1. If there are more than 1000 detections per day for a single AID, only the first 1000 will be shown1.

NEW QUESTION 30
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 32
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 34
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 39
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 41
A list of managed and unmanaged neighbors for an endpoint can be found:

A. by using Hosts page in the Investigate tool
B. by reviewing "Groups" in Host Management under the Hosts page
C. under "Audit" by running Sensor Visibility Exclusions Audit
D. only by searching event data using Event Search

Answer: A

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. This can help you identify potential threats or vulnerabilities in your network2.

NEW QUESTION 44
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 45
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 49
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 52
In the "Full Detection Details", which view will provide an exportable text listing of events like DNS requests. Registry Operations, and Network Operations?

A. Thedata 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 55
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 59
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 63
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 67

.....

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