CrowdStrike

Exam Questions CCFR-201

CrowdStrike Certified Falcon Responder

NEW QUESTION 1
Which of the following is NOT a filter available on the Detections page?

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

Answer: D

Explanation:
According to the CrowdStrike Falcon® Data Replicator (FDR) Add-on for Splunk Guide, the Detections page allows you to view and manage detections generated by the CrowdStrike Falcon platform2. You can use various filters to narrow down the detections based on criteria such as severity, CrowdScore, time, tactic, technique, etc2. However, there is no filter for triggering file, which is the file that caused the detection2.

NEW QUESTION 2
When examining raw event data, what is the purpose of the field called ParentProcessld_decimal?

A. It contains an internal value not useful for an investigation
B. It contains the TargetProcessld_decimal value of the child process
C. It contains the Sensorld_decimal value for related events
D. It contains the TargetProcessld_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 ParentProcessld_decimal field contains the decimal value of the process ID of the parent process that spawned or injected into the target process1. This field can be used to trace the process lineage and identify malicious or suspicious activities1.

NEW QUESTION 3
What information does the MITRE ATT&CK®Framework provide?

A. It provides best practices for different cybersecurity domains, such as Identify 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 4
You are reviewing the raw data in an event search from a detection tree. You find a FileOpenlnfo 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. ParentProcessld_decimal and aid
B. ResponsibleProcessld_decimal and aid
C. ContextProcessld_decimal and aid
D. TargetProcessld_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
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
How does a DNSRequest event link to its responsible process?

A. Via both its ContextProcessld decimal and ParentProcessld_decimal fields
B. Via its ParentProcessld_decimal field
C. Via its ContextProcessld_decimal field
D. Via its TargetProcessld_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 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
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 9
How long are quarantined files stored on the host?

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

Answer: C

Explanation:
According to the CrowdStrike Falcon® Data Replicator (FDR) Add-on for Splunk Guide, quarantined files are never deleted from the host unless you manually delete them or release them from quarantine2. When you release a file from quarantine, you are restoring it to its original location and allowing it to execute on any host in your organization2. This action also removes the file from the quarantine list and deletes it from the CrowdStrike Cloud2.

NEW QUESTION 10
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
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 13
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 17
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 21
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 24
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 27
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 29
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 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 TargetProcessld_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 34
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 38
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 42
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 45
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 49
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 TargetProcessld_decimal or ContextProcessld_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 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 IPD.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 54

Which of the following is an example of a MITRE ATT&CK tactic?

A. Eternal Blue
B. Defense Evasion
C. Emotet
D. Phishing

Answer: B

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. Defense Evasion is one of the tactics defined by MITRE ATT&CK, which covers actions that adversaries take to avoid detection or prevent security controls from blocking their activities. Eternal Blue, Emotet, and Phishing are examples of techniques, not tactics.

NEW QUESTION 55

......