[Full-Version 2023 New CCFR-201 Actual Exam Dumps, CrowdStrike Practice Test [Q12-Q32

[Full-Version] 2023 New CCFR-201 Actual Exam Dumps, CrowdStrike Practice Test
Study HIGH Quality CCFR-201 Free Study Guides and Exams Tutorials

Q12. What are Event Actions?
* Automated searches that can be used to pivot between related events and searches
* Pivotable hyperlinks available in a Host Search
* Custom event data queries bookmarked by the currently signed in Falcon user
* Raw Falcon event data

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.

Q13. What do IOA exclusions help you achieve?

* Reduce false positives based on Next-Gen Antivirus settings in the Prevention Policy
* Reduce false positives of behavioral detections from IOA based detections only
* Reduce false positives of behavioral detections from IOA based detections based on a file hash
* Reduce false positives of behavioral detections from Custom IOA and OverWatch detections only

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.

Q14. 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?

* Falcon X
* Investigate
* Discover
* Spotlight

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.

Q15. 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?

* SHA256 and TargetProcessId_decimal
* SHA256 and ParentProcessId_decimal
* aid and ParentProcessId_decimal
* aid and TargetProcessId_decimal

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.

Q16. From a detection, what is the fastest way to see children and sibling process information?

* Select the Event Search option. Then from the Event Actions, select Show Associated Event Data (From TargetProcessId_decimal)
* Select Full Detection Details from the detection
* Right-click the process and select “Follow Process Chain”
* Select the Process Timeline feature, enter the AID. Target Process ID, and Parent Process ID

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.

Q17. What information is contained within a Process Timeline?
* All cloudable process-related events within a given timeframe
* All cloudable events for a specific host
* Only detection process-related events within a given timeframe
* A view of activities on Mac or Linux hosts

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. You can specify a timeframe to limit the events to a certain period1. The tool works for any host platform, not just Mac or Linux1.

Q18. The function of Machine Learning Exclusions is to_____.
* stop all detections for a specific pattern ID
* stop all sensor data collection for the matching path(s)
* Stop all Machine Learning Preventions but a detection will still be generated and files will still be uploaded to the CrowdStrike Cloud
* stop all ML-based detections and preventions for the matching path(s) and/or stop files from being uploaded to the CrowdStrike Cloud

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.

Q19. Which Executive Summary dashboard item indicates sensors running with unsupported versions?
* Detections by Severity
* Inactive Sensors
* Sensors in RFM
* Active Sensors

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.

Q20. The Process Activity View provides a rows-and-columns style view of the events generated in a detection.

Why might this be helpful?
* The Process Activity View creates a consolidated view of all detection events for that process that can be exported for further analysis
* The Process Activity View will show the Detection time of the earliest recorded activity which might indicate first affected machine
* The Process Activity View only creates a summary of Dynamic Link Libraries (DLLs) loaded by a process

* The Process Activity View creates a count of event types only, which can be useful when scoping the event
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.

Q21. What types of events are returned by a Process Timeline?
* Only detection events
* All cloudable events
* Only process events
* Only network events
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.

Q22. What does pivoting to an Event Search from a detection do?
* It gives you the ability to search for similar events on other endpoints quickly
* It takes you to the raw Insight event data and provides you with a number of Event Actions
* It takes you to a Process Timeline for that detection so you can see all related events
* It allows you to input an event type, such as DNS Request or ASEP write, and search for those events within the detection
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.

Q23. How long does detection data remain in the CrowdStrike Cloud before purging begins?
* 90 Days
* 45 Days
* 30 Days
* 14 Days
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.

Q24. How long are quarantined files stored in the CrowdStrike Cloud?
* 45 Days
* 90 Days

* Days
* Quarantined files are not deleted

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.

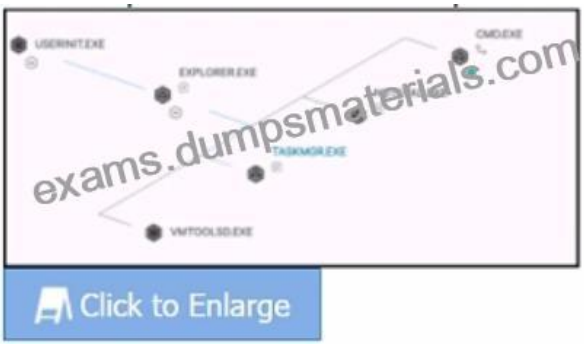
Q25. When reviewing a Host Timeline, which of the following filters is available?

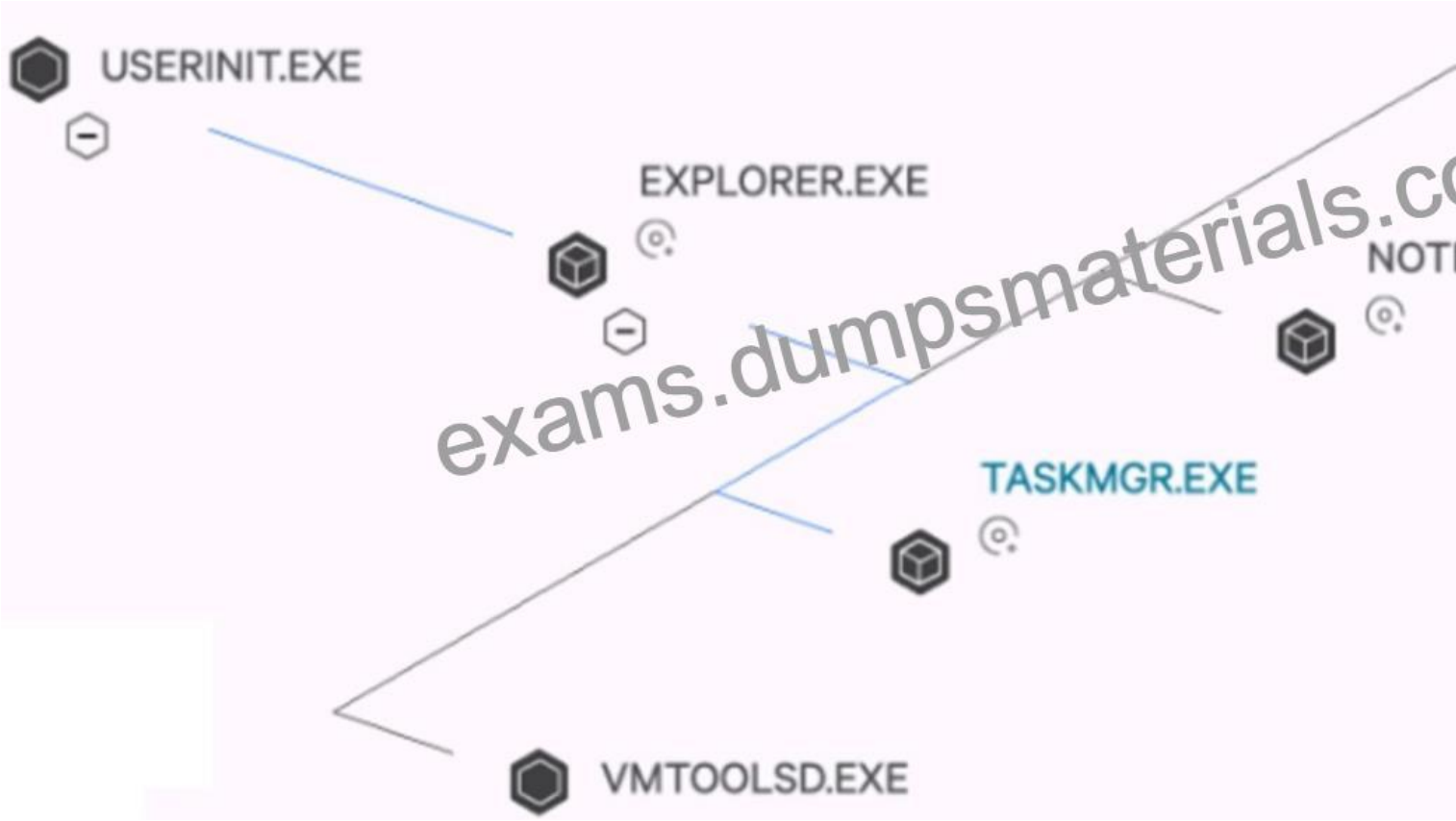
* Severity
* Event Types
* User Name
* Detection ID

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.

Q26. How are processes on the same plane ordered (bottom ‘VMTOOLSD.EXE’ to top CMD.EXE’)?





* Process ID (Descending, highest on bottom)
* Time started (Descending, most recent on bottom)
* Time started (Ascending, most recent on top)
* Process ID (Ascending, highest on top)

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.

Q27. When examining a raw DNS request event, you see a field called ContextProcessld_decimal. What is the purpose of that field?

* It contains the TargetProcessld_decimal value for other related events
* It contains an internal value not useful for an investigation
* It contains the ContextProcessld_decimal value for the parent process that made the DNS request
* It contains the TargetProcessld_decimal value for the process that made the DNS request

Explanation

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the ContextProcessld_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.

Q28. Which is TRUE regarding a file released from quarantine?

* No executions are allowed for 14 days after release
* It is allowed to execute on all hosts
* It is deleted
* It will not generate future machine learning detections on the associated host

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.

Q29. In the Hash Search tool, which of the following is listed under Process Executions?
* Operating System
* File Signature
* Command Line
* Sensor Version

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.

Q30. The primary purpose for running a Hash Search is to:
* determine any network connections
* review the processes involved with a detection
* determine the origin of the detection
* review information surrounding a hash’s related activity

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.

Q31. Aside from a Process Timeline or Event Search, how do you export process event data from a detection in

.CSV format?
* You can’t export detailed event data from a detection, you have to use the Process Timeline or an Event Search
* In Full Detection Details, you expand the nodes of the process tree you wish to expand and then click the “Export Process Events” button
* In Full Detection Details, you choose the “View Process Activity” option and then export from that view
* From the Detections Dashboard, you right-click the event type you wish to export and choose CSV.JSON or XML

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.

Q32. What action is used when you want to save a prevention hash for later use?
* Always Block
* Never Block
* Always Allow
* No Action

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.