Real CCFR-201 are Uploaded by BraindumpsIT provide 2023 Latest CCFR-201 Practice Tests Dumps [Q14-Q30

Real CCFR-201 are Uploaded by **BraindumpsIT** provide **2023** Latest CCFR-201 Practice Tests Dumps.
All CCFR-201 Dumps and CrowdStrike Certified Falcon Responder Training Courses Help candidates to study and pass the CrowdStrike Certified Falcon Responder Exams hassle-free! NO.14 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.

NO.15 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.

NO.16 What does the Full Detection Details option provide?

* It provides a visualization of program ancestry via the Process Tree View
* It provides a visualization of program ancestry via the Process Activity View
* It provides detailed list of detection events via the Process Table View
* It provides a detailed list of detection events via the Process Tree View

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.

NO.17 What action is used when you want to save a prevention hash for later use?

* Always Allow
* Never Block
* No Action
* Always Block

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.

NO.18 Where can you find hosts that are in Reduced Functionality Mode?

* Event Search
* Executive Summary dashboard
* Host Search
* Installation Tokens

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&#8217;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.

NO.19 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.

NO.20 Within the MITRE-Based Falcon Detections Framework, what is the correct way to interpret Keep Access > Persistence > Create Account?
* An adversary is trying to keep access through persistence by creating an account
* An adversary is trying to keep access through persistence using browser extensions
* An adversary is trying to keep access through persistence using external remote services
* adversary is trying to keep access through persistence using application skimming
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.

NO.21 Which of the following is NOT a valid event type?
* StartofProcess
* EndofProcess
* ProcessRollup2
* DnsRequest
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.

NO.22 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&#8217;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&#8217;s related activity, such as which hosts and processes were involved, where they were located, and whether they triggered any alerts1.

NO.23 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.

NO.24 When examining raw event data, what is the purpose of the field called ParentProcessld_decimal?

* It contains an internal value not useful for an investigation
* It contains the TargetProcessld_decimal value of the child process
* It contains the Sensorld_decimal value for related events
* It contains the TargetProcessld_decimal of the parent process

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.

NO.25 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.

NO.26 What is the difference between Managed and Unmanaged Neighbors in the Falcon console?

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

Explanation

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

NO.27 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.

NO.28 Which of the following is NOT a filter available on the Detections page?

* Severity
* CrowdScore
* Time
* Triggering File

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.

NO.29 What happens when a hash is set to Always Block through IOC Management?

* Execution is prevented on all hosts by default
* Execution is prevented on selected host groups
* Execution is prevented and detection alerts are suppressed
* The hash is submitted for approval to be blocked from execution once confirmed by Falcon specialists

Explanation

According to the CrowdStrike Falcon Data Replicator (FDR) Add-on for Splunk Guide, IOC Management allows you to manage indicators of compromise (IOCs), which are artifacts such as hashes, IP addresses, or domains that are associated with malicious activities2. You can set different actions for IOCs, such as Allow, No Action, or Always Block2. When you set a hash to Always Block through IOC Management, you are preventing that file from executing on any host in your organization by default2. This action also generates a detection alert when the file is blocked2.

NO.30 What information does the MITRE ATT&CKFramework provide?

* It provides best practices for different cybersecurity domains, such as Identify and Access Management
* It provides a step-by-step cyber incident response strategy
* It provides the phases of an adversary&#8217;s lifecycle, the platforms they are known to attack, and the specific methods they use
* It is a system that attributes an attack techniques to a specific threat actor

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&#8217;s lifecycle, such as reconnaissance, resource development, execution, command and control, etc.

Valid Way To Pass CrowdStrike's CCFR-201 Exam with : https://www.braindumpsit.com/CCFR-201_real-exam.html