Easily To Pass New CCFR-201 Verified & Correct Answers [May 13, 2024 [Q37-Q56

Easily To Pass New CCFR-201 Verified & Correct Answers [May 13, 2024
Free CCFR-201 Exam Files Downloaded Instantly

NO.37 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.

NO.38 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 TargetProcessId_decimal value of the child process
* It contains the SensorId_decimal value for related events
* It contains the TargetProcessId_decimal of the parent process

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.

NO.39 Where are quarantined files stored on Windows hosts?

* WindowsQuarantine
* WindowsSystem32DriversCrowdStrikeQuarantine
* WindowsSystem32
* WindowstempDriversCrowdStrikeQuarantine

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:WindowsSystem32DriversCrowdStrikeQuarantine folder2.

NO.40 The Bulk Domain Search tool contains Domain information along with which of the following?

* Process Information
* Port Information
* IP Lookup Information
* Threat Actor Information

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.

NO.41 In the “Full Detection Details”, which view will provide an exportable text listing of events like DNS requests.

Registry Operations, and Network Operations?

* Thedata is unable to be exported
* View as Process Tree
* View as Process Timeline
* View as Process Activity

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.

NO.42 You can jump to a Process Timeline from many views, like a Hash Search, by clicking which of the following?
* ProcessTimeline Link
* PID
* UTCtime
* Process ID or Parent Process ID

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. The tool requires two parameters: aid (agent ID) and TargetProcessId_decimal (the decimal value of the process ID)1. You can jump to a Process Timeline from many views, such as Hash Search, Host Timeline, Event Search, etc., by clicking on either the Process ID or Parent Process ID fields in those views1. This will automatically populate the aid and TargetProcessId_decimal parameters for the Process Timeline tool1.

NO.43 When you configure and apply an IOA exclusion, what impact does it have on the host and what you see in the console?
* The process specified is not sent to the Falcon Sandbox for analysis
* The associated detection will be suppressed and the associated process would have been allowed to run
* The sensor will stop sending events from the process specified in the regex pattern
* The associated IOA will still generate a detection but the associated process would have been allowed to run

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 activities1. This can reduce false positives and improve performance1. When you configure and apply an IOA exclusion, the impact is that the associated detection will be suppressed and theassociated process would have been allowed to run1. This means that you will not see any alerts or events related to that IOA in the console1.

NO.44 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?
* Identifies a detailed list of all process executions for the specified hashes
* Identifies hosts that loaded or executed the specified hashes
* Identifies users associated with the specified hashes
* Identifies detections related to the specified hashes

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.

NO.45 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?
* Draw Process Explorer
* Show a +/- 10-minute window of events
* Show a Process Timeline for the responsible process
* Show Associated Event Data (from TargetProcessId_decimal or ContextProcessId_decimal)

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.

NO.46 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.

NO.47 Which of the following is an example of a MITRE ATT&CK tactic?
* Eternal Blue
* Defense Evasion
* Emotet
* Phishing
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.

NO.48 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.49 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.50 Which of the following is returned from the IP Search tool?
* IP Summary information from Falcon events containing the given IP
* Threat Graph Data for the given IP from Falcon sensors
* Unmanaged host data from system ARP tables for the given IPD.IP Detection Summary information for detection events containing the given IP

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.

NO.51 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.52 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?
* Do nothing, as this file is common and well known
* From detection, click the VT Hash button to pivot to VirusTotal to investigate further
* From detection, use API manager to create a custom blocklist
* From detection, submit to FalconX for deep dive analysis

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.

NO.53 What is an advantage of using a Process Timeline?
* Process related events can be filtered to display specific event types
* Suspicious processes are color-coded based on their frequency and legitimacy over time
* Processes responsible for spikes in CPU performance are displayed overtime
* A visual representation of Parent-Child and Sibling process relationships is provided

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. You can also filter the events by various criteria, such as event type, timestamp range, file name, registry key, network destination, etc2. This is an advantage of using the Process Timeline tool because it allows you to focus on specific events that are relevant to your investigation2.

NO.54 Which of the following tactic and technique combinations is sourced from MITRE ATT&CK information?
* Falcon Intel via Intelligence Indicator – Domain
* Machine Learning via Cloud-Based ML
* Malware via PUP
* Credential Access via OS Credential Dumping

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.

NO.55 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’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’s lifecycle, such as reconnaissance, resource development, execution, command and control, etc.

NO.56 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.