CrowdStrike.CCFR-201b.v2026-09-14.q89

Exam Code:	CCFR-201b
Exam Name:	CrowdStrike Certified Falcon Responder
Certification Provider:	CrowdStrike
Free Question Number:	89
Version:	v2026-09-14
# of views:	104
# of Questions views:	900
https://www.freecram.net/torrent/CrowdStrike.CCFR-201b.v2026-09-14.q89.html	

NEW QUESTION: 1
What information does the MITREATT AND CKFramework provide?
A. It provides a step-by-step cyber incident response strategy
B. It is a system that attributes an attack techniques to a specific threat actor
C. It provides best practices for different cybersecurity domains, such as Identify and Access Management
D. It provides the phases of an adversary's lifecycle, the platforms they are known to attack, and the specific methods they use
Answer: (SHOW ANSWER)

NEW QUESTION: 2
Detections in Falcon are classified by their origin. Which of the following is NOT a recognized type of detection?
A. Behavioral
B. Custom IOA
C. Intelligence
D. Machine Learning
Answer: (SHOW ANSWER)

NEW QUESTION: 3
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 using browser extensions
B. adversary is trying to keep access through persistence using application skimming
C. An adversary is trying to keep access through persistence using external remote services
D. An adversary is trying to keep access through persistence by creating an account
Answer: (SHOW ANSWER)

NEW QUESTION: 4
A responder decides to set a specific Custom IOA to the ' Monitor ' action. Which of the following sentences best describes the technical result of this choice?
A. The sensor will log the activity in the audit logs but will not generate a detection.
B. The sensor will create detections with ' Informational ' severity but will not block the activity.
C. The sensor will automatically isolate the host from the network.
D. The sensor will block the activity and alert the user with a pop-up.
Answer: (SHOW ANSWER)

NEW QUESTION: 5
Executive dashboards provide a high-level view of security. Which of the following CANNOT be seen from the Executive Summary Dashboard?
A. The organization's current CrowdScore trend.
B. The top 10 hosts with the most detections.
C. A breakdown of Agent Versions across the fleet.
D. Detections broken down by Tactic.
Answer: (SHOW ANSWER)

NEW QUESTION: 6
An adversary is attempting to disable security features by modifying the system registry. Which of the following native Windows processes is specifically designed to create, modify, and delete Registry keys via the command line?
A. reg.exe
B. svchost.exe
C. lsass.exe
D. taskmgr.exe
Answer: (SHOW ANSWER)

NEW QUESTION: 7
To understand how a threat moved on a system, a responder must know the role of common processes. Which of the following statements best describes the standard functionality of explorer.exe?
A. It is a system process responsible for the Local Security Authority subsystem.
B. It is the primary process responsible for the File Explorer UI and the user's desktop environment.
C. It is the service control manager that handles the starting of background tasks.
D. It is the Windows Command Processor used for executing batch files.
Answer: (SHOW ANSWER)

NEW QUESTION: 8

A security analyst is triaging a high-severity alert on a critical production server. To understand the adversary
' s intent and technical execution within the framework of industry standards, the analyst refers to the console ' s categorization. Which specific methodology does CrowdStrike utilize within the Falcon platform to classify detections based on technical behavior?
A. NIST Incident Response Lifecycle
B. Falcon Adversary Attribution Matrix
C. MITRE-Based Falcon Detections Framework
D. Cyber Kill Chain Classification
Answer: (SHOW ANSWER)

NEW QUESTION: 9
The Falcon sensor can take several automated actions to protect an endpoint. Which of the following is NOT an action that Falcon takes upon detection?
A. Process Termination
B. File Quarantine
C. Network Isolation
D. Process Restart
Answer: (SHOW ANSWER)

NEW QUESTION: 10
An executive asks for a definition of 'CrowdScore'. Which of the following sentences best describes what CrowdScore is?
Freecram.net
A. It is the total number of detections that have been resolved within the last 24 hours.
B. It is a metric designed to show an organization's threat level on a continual basis by aggregating related detections.
C. It is a measure of the total processing power being used by the Falcon sensors globally.
D. It is a ranking system that compares your organization's security to other companies.
Answer: (SHOW ANSWER)

NEW QUESTION: 11
A responder needs to categorize an incident based on the high-level goals of the attacker. Which of the following lists correctly identifies the "Objectives" as they are natively defined and used within the Falcon platform?
A. Triage, Containment, Remediation, Eradication, Reporting, Recovery
B. Explore, Keep Access, Gain Access, Falcon Detection Method, Contact Controlled systems, Follow Through
C. Identify, Protect, Detect, Respond, Recover, Lessons Learned
D. Reconnaissance, Delivery, Weaponization, Exploitation, Installation, Command and Control
Answer: B (LEAVE A REPLY)

NEW QUESTION: 12
Bulk Search tools have several features in common. Which of the following is incorrect as a feature common to all Bulk Search types?
A. They allow for searching multiple items (up to 500) at once.
B. Search results can be exported for further analysis.
C. They search across historical telemetry in the cloud.
D. Regular Expressions (Regex) are allowed within the search fields.
Answer: (SHOW ANSWER)

NEW QUESTION: 13
Refer to the image.

freecram.net

What does the arrowed line indicate?
A. PowerShell spawned Notepad.exe, which injected a thread back to Excel.exe
B. The thread injection was considered a Medium severity injection
C. PowerShell spawned Notepad.exe, which injected a thread back to PowerShell
D. Notepad.exe injected itself into Excel.exe
Answer: (SHOW ANSWER)
The arrowed relationship indicates process injection activity, not a normal parent-child process relationship. In the displayed graph, PowerShell launches Notepad.exe, and the highlighted relationship shows Notepad.exe injecting a thread back into PowerShell. This type of behavior is suspicious because adversaries often use benign-looking processes as injection targets or injectors to hide execution, evade detection, or manipulate process behavior. Option B is incorrect because the arrow does not primarily describe severity; severity is a separate detection attribute. Option D is incorrect because the visual relationship does not show Notepad injecting into itself.

Option A is also incorrect because the highlighted relationship points back to PowerShell, not Excel. Correctly reading these graph relationships is essential during Falcon detection analysis.

NEW QUESTION: 14
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 of the parent process
C. It contains the TargetProcessId_decimal value of the child process
D. It contains the SensorId_decimal value for related events
Answer: (SHOW ANSWER)

NEW QUESTION: 15
When training a new team member on how to interpret Falcon telemetry, a senior responder explains the definition of a 'Tactic'. Which of the following sentences best captures the technical definition of a Tactic in this context?
A. It is the unique cryptographic hash associated with a malicious file discovered on disk.
B. It is the specific command-line string used to execute a PowerShell script.
C. It is the adversary's tactical goal: the fundamental reason for performing a specific action.
D. It represents the specific software version or exploit code used to crash a service.
Answer: (SHOW ANSWER)

NEW QUESTION: 16
When navigating the ' Custom IOA ' creation wizard, a user must select a rule type. Which of the following is NOT a valid IOA rule type available for selection?
A. Domain Name
B. Scheduled Task
C. Process Creation
D. File Creation
Answer: B (LEAVE A REPLY)

Valid CCFR-201b Dumps shared by EduDump.com for Helping Passing CCFR-201b Exam! EduDump.com now offer the **newest CCFR-201b exam dumps**, the EduDump.com CCFR-201b exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CCFR-201b dumps with Test Engine here: https://www.edudump.com/exams/CrowdStrike/CCFR-201b/premium/ (**212** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 17

Which of the following is NOT a valid event type?

A. DnsRequest

B. ProcessRollup2

C. StartofProcess

D. EndofProcess

Answer: (SHOW ANSWER)

NEW QUESTION: 18

Which is TRUE regarding a file released from quarantine?

A. It is deleted

B. No executions are allowed for 14 days after release

C. It will not generate future machine learning detections on the associated host

D. It is allowed to execute on all hosts

Answer: (SHOW ANSWER)

NEW QUESTION: 19

A responder is analyzing a file's prevalence. If the data shows 'Local: High' and 'Global: Unique', which of the following is the most likely conclusion?

A. The file is internally developed software unique to the organization.

B. The file is common off-the-shelf malware seen globally.

C. The file is a known commodity tool used by many different actors.

D. The file is a standard Windows system component.

Answer: (SHOW ANSWER)

NEW QUESTION: 20

Filtering is essential for managing a high volume of alerts. Which of the following filters is available by default within the 'Endpoint Detections' dashboard to help narrow down specific threats?

Pdfcram.net

A. Triggering File

B. Hardware BIOS Version

C. Local Subnet Mask

D. Sensor Update Policy Name

Answer: (SHOW ANSWER)

NEW QUESTION: 21

What action is needed to ensure Falcon does not block or generate a detection for a process by using the file hash?

A. Create a Custom IOA with an action of allow for the hash

B. Create an IOA Exclusion with an action of allow for the hash

C. Create a Machine Learning Exclusion with an action of allow for the hash

D. Create a Custom IOC with an action of allow for the hash

Answer: (SHOW ANSWER)

NEW QUESTION: 22
From the Detections page, how can you view ' in-progress ' detections assigned to Falcon Analyst Alex?
A. Filter on ' Analyst: Alex '
B. Filter on ' Hostname: Alex ' and ' Status: In-Progress '
C. Alex does not have the correct role permissions as a Falcon Analyst to be assigned detections
D. Filter on ' Status: In-Progress ' and ' Assigned-to: Alex*
Answer: (SHOW ANSWER)

NEW QUESTION: 23
Which of the following sentences best describes the primary objective of ' Real-time Analysis ' within the Falcon platform?
A. Manually updating the Falcon sensor on every machine in the fleet.
B. Investigating incoming telemetry in real time or on a near real-time basis to catch active threats.
C. Analyzing historical logs from the past 90 days to find missed threats.
D. Scanning every file on a hard drive once per week for dormant viruses.
Answer: (SHOW ANSWER)

NEW QUESTION: 24
CrowdStrike implements a specific framework within the Falcon console to help responders categorize detections based on the adversary's ultimate goals and the technical means used to achieve them. This classification system, which maps activity to known industry standards, is known as the:
A. CrowdStrike Intelligence Lifecycle Mapping
B. Falcon Adversary Attribution and Motivation Matrix
C. MITRE-Based Falcon Detections Framework
D. Unified Behavioral Threat Hunting Schema
Answer: (SHOW ANSWER)

NEW QUESTION: 25
You notice that taskeng.exe is one of the processes involved in a detection. What activity should you investigate next?
A. Executions of schtasks.exe after the detection
B. Pivot to a Hash search for taskeng.exe
C. User logons after the detection
D. Scheduled tasks registered prior to the detection
Answer: (SHOW ANSWER)

NEW QUESTION: 26

When using 'User Search' to investigate a potentially compromised account, which of the following is NOT a filter available in the User Search?

A. Username

B. Time Range

C. Hostname

D. Process ID

Answer: (SHOW ANSWER)

NEW QUESTION: 27

The primary purpose for running a Hash Search is to:

A. determine the origin of the detection

B. review the processes involved with a detection

C. determine any network connections

D. review information surrounding a hash's related activity

Answer: (SHOW ANSWER)

NEW QUESTION: 28

An analyst is triaging a detection that has been categorized under the 'Follow Through' Objective Layer.

Based on the Falcon technical documentation, which of the following adversary tactics is most likely to be observed within this specific layer?

A. Discovery of local network shares and services

B. Initial Access via a drive-by download

C. Collection of sensitive data for exfiltration

D. Credential Access through memory scraping

Answer: (SHOW ANSWER)

NEW QUESTION: 29

Which of the following tactic and technique combinations is sourced from MITREATT AND CKinformation?

A. Falcon Intel via Intelligence Indicator - Domain

B. Machine Learning via Cloud-Based ML

C. Credential Access via OS Credential Dumping

D. Malware via PUP

Answer: (SHOW ANSWER)

NEW QUESTION: 30

In the 'Graph View' of a detection, processes are connected by arrows. Which of the following does a yellow arrow connecting two processes indicate?

Freecram.net

A. A file was written by the first process and read by the second.

B. A Thread Injector-Injectee relationship (Process Injection).

C. A Network connection was established between the two processes.
D. A standard Parent-Child relationship.
Answer: (SHOW ANSWER)

NEW QUESTION: 31
Depending on the subscription level, "Cloudable Events" (standard telemetry) have a specific retention period. What is the minimum period of time that these events are retained?
A. 30 days
B. 14 days
C. 1 day
D. 7 days
Answer: (SHOW ANSWER)

Valid CCFR-201b Dumps shared by EduDump.com for Helping Passing CCFR-201b Exam! EduDump.com now offer the **newest CCFR-201b exam dumps**, the EduDump.com CCFR-201b exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CCFR-201b dumps with Test Engine here: https://www.edudump.com/exams/CrowdStrike/CCFR-201b/premium/ (**212** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 32
Which of the following is NOT a filter available on the Detections page?
A. Severity
B. Time
C. Triggering File
D. CrowdScore
Answer: (SHOW ANSWER)

NEW QUESTION: 33
When reviewing a Host Timeline, which of the following filters is available?
A. User Name
B. Detection ID
C. Event Types
D. Severity
Answer: (SHOW ANSWER)

NEW QUESTION: 34
When managing files within the 'Quarantined Files' dashboard, which of the following is NOT a valid action available to the responder?

A. Investigate
B. Download
C. Release
D. Delete
Answer: (SHOW ANSWER)

NEW QUESTION: 35
An analyst notices a detection that has been automatically flagged with the 'New Activity' status. Which of the following statements best describes what this status indicates?
A. The Falcon Overwatch team has manually verified that the detection is an active threat.
B. A brand new detection has been triggered on a host that was recently added to the network.
C. A detection that was previously moved to a resolved status has generated new telemetry and activity.
D. A user has logged into a machine for the first time since the sensor was installed.
Answer: (SHOW ANSWER)

NEW QUESTION: 36
Where are quarantined files stored on Windows hosts?
A. Windows\temp\Drivers\CrowdStrike\Quarantine
B. Windows\System32\
C. Windows\System32\Drivers\CrowdStrike\Quarantine
D. Windows\Quarantine
Answer: (SHOW ANSWER)

NEW QUESTION: 37
Analyze the following process lineage observed during a detection triage on a Windows 10 workstation:
root > smss.exe > winlogon.exe > userinit.exe > explorer.exe > windows_media_player_y35s21-4ak.exe.
Based on the fact that the suspicious process originated from the user's desktop shell environment (explorer.
exe), what is the most likely entry vector for this attack?
A. Remote exploitation of a system service
B. User execution via a Phishing email or drive-by download
C. Malicious persistence via a WMI event subscription
D. Credential theft through a compromised Domain Controller
Answer: (SHOW ANSWER)

NEW QUESTION: 38
An analyst needs to quickly view the activity surrounding a suspicious process. Which of the following sequences of steps will pivot to an auto-filled process timeline in the Falcon UI?

A. Activity Dashboard > Click Detection > Export to PDF
B. Investigate > Bulk Search > Enter SHA256 > View Results
C. Configuration > Host Groups > Select Host > Network History
D. Host Search > Processes and Services > Filename > Start Time > Process ID
Answer: (SHOW ANSWER)

NEW QUESTION: 39
Your lead analyst instructs you to dump the kernel memory of a Windows system using Real Time Response (RTR).
Which native RTR command best helps you to quickly achieve the task?
A. CSWINDIAG
B. dumpmem
C. xmemdump
D. memdump
Answer: (SHOW ANSWER)
The correct RTR command is xmemdump. In Falcon Real Time Response, memory acquisition commands must be selected carefully because different commands collect different types of diagnostic or memory data. CSWINDIAG is associated with collecting diagnostic information and troubleshooting data, not directly dumping kernel memory. memdump is generally associated with process memory collection rather than the Windows kernel-memory task described in the question. dumpmem is not the best native RTR command for this scenario. Since the lead analyst specifically asks for kernel memory from a Windows system, xmemdump is the appropriate command. This matters operationally because using the wrong RTR command can waste response time and fail to collect the artifact required for deeper forensic analysis.

NEW QUESTION: 40
While the host timeline is comprehensive, some data is not included in that specific view. Which of the following CANNOT be seen directly from the host timeline?
Freecram.net
A. Event Name
B. CPU Temperature
C. Timestamp
D. PID (Process ID)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 41
During the incident response process, a responder must update the status of a detection. Which of the following options is NOT a valid detection status recognized by the Falcon console?
A. Complete
B. In Progress
C. True Positive
D. New

Answer: (SHOW ANSWER)

NEW QUESTION: 42
A responder is analyzing a MITRE-related alert and sees the technique 'Explore > Discovery > Cloud Service Dashboard'. Which of the following scenarios best describes the technical activity associated with this technique?
A. An adversary uses an automated script to bruteforce S3 bucket permissions.
B. An adversary executes an API call to terminate all running EC2 instances in a region.
C. An adversary uses a cloud service dashboard GUI with stolen credentials to gain useful information from an operational cloud environment.
D. An adversary deploys a crypto-miner inside a compromised Docker container.
Answer: (SHOW ANSWER)

NEW QUESTION: 43
What is an advantage of using a Process Timeline?
A. Process related events can be filtered to display specific event types
B. Processes responsible for spikes in CPU performance are displayed overtime
C. Suspicious processes are color-coded based on their frequency and legitimacy over time
D. A visual representation of Parent-Child and Sibling process relationships is provided
Answer: (SHOW ANSWER)

NEW QUESTION: 44
While examining the 'Process Details' sidebar of a detection, a responder sees the following icons: "25 Network Operations" and "277 Disk Operations". What does this contextual data represent?
A. The number of other hosts that have seen similar network and disk activity.
B. The percentage of the CPU being consumed by the network and disk.
C. The specific number of telemetry events recorded for network and disk activity by that process.
D. The total size in megabytes of the data sent over the network and written to disk.
Answer: (SHOW ANSWER)

NEW QUESTION: 45
Refer to the image.

You are using Advanced Event Search to find the event record for a suspicious network connection.

Using the Event List Interactions button for the event, indicated by the arrow in the image above, which option will show all contextual event data around the process execution being investigated?

A. Show Responsible Process Data

B. Inspect

C. Show +/- 10-minute windows of events

D. Investigate Host

Answer: (SHOW ANSWER)

The correct option is Show Responsible Process Data. When investigating a suspicious network connection, the network event itself is only one part of the activity. The responder needs to identify the process responsible for initiating the connection and then pivot into the contextual process data around that execution. "Inspect" is useful for looking at the selected raw event details, but it does not provide the broader responsible-process context. "Show +/- 10-minute windows of events" expands the time window, but it is not specifically focused on the process responsible for the network activity.

"Investigate Host" pivots to host-level context, which is broader than the process-specific requirement.

Responsible process data is the most direct investigative pivot here.

NEW QUESTION: 46

An administrator needs to download a file for analysis that was blocked by the sensor. Where are quarantine files located within the Falcon UI?

A. Endpoint Security > Monitor > Quarantined Files

B. Dashboards > Security > Quarantine

C. Investigate > Quarantine

D. Configuration > Response > Quarantine
Answer: (SHOW ANSWER)

Valid CCFR-201b Dumps shared by EduDump.com for Helping Passing CCFR-201b Exam! EduDump.com now offer the **newest CCFR-201b exam dumps**, the EduDump.com CCFR-201b exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CCFR-201b dumps with Test Engine here: https://www.edudump.com/exams/CrowdStrike/CCFR-201b/premium/ (**212** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 47
A responder needs to find a specific sequence of network connections that did not trigger a detection. Which search tool allows them to search for anything within the raw telemetry?
A. User Search
B. Host Search
C. Hash Search
D. Event Search
Answer: (SHOW ANSWER)

NEW QUESTION: 48
A list of managed and unmanaged neighbors for an endpoint can be found:
A. by using Hosts page in the Investigate tool
B. under " Audit " by running Sensor Visibility Exclusions Audit
C. only by searching event data using Event Search
D. by reviewing " Groups " in Host Management under the Hosts page
Answer: (SHOW ANSWER)

NEW QUESTION: 49
How long are quarantined files stored in the CrowdStrike Cloud?
A. Quarantined files are not deleted
B. 90 Days
C. 45 Days
D. Days
Answer: (SHOW ANSWER)

NEW QUESTION: 50
Where can you find hosts that are in Reduced Functionality Mode?
A. Host Search
B. Event Search

C. Executive Summary dashboard
D. Installation Tokens
Answer: (SHOW ANSWER)

NEW QUESTION: 51
What happens when a quarantined file is released?
A. It is allowed to execute on the host
B. It is moved into theC:\CrowdStrike\Quarantine\Releasedfolder on the host
C. It is allowed to execute on all hosts
D. It is deleted
Answer: C (LEAVE A REPLY)

NEW QUESTION: 52
The Activity Dashboard is a core feature for security teams. What is the primary purpose of this dashboard?
A. To view the raw telemetry of every event happening on the network.
B. To provide a summary of the current threat state and active detections in the environment.
C. To manage the installation and update of Falcon sensors.
D. To audit the changes made by other Falcon administrators.
Answer: (SHOW ANSWER)

NEW QUESTION: 53
A responder is explaining the quarantine process to a system administrator. What happens technically when a file is quarantined by the Falcon sensor?
A. It is deleted from the disk and a log is sent to the cloud.
B. It is renamed to a .tmp extension and moved to the Windows Recycle Bin.
C. It is moved to the CrowdStrike Cloud and removed from the local host immediately.
D. It is compressed, password protected, and moved to the Quarantine folder on the endpoint.
Answer: (SHOW ANSWER)

NEW QUESTION: 54
When reviewing CrowdScore Incidents, which of the following statements is INCORRECT?
A. Incidents are defined as inactive after 10 hours pass without any new related activity.
B. Incidents aggregate related detections to reduce alert fatigue.
C. A high CrowdScore indicates a higher likelihood of a sophisticated or widespread attack.
D. CrowdScore is only visible to users with the 'Falcon Administrator' role.
Answer: (SHOW ANSWER)

NEW QUESTION: 55
What must be true about a custom script before it can be executed from within a Fusion SOAR Workflow?

A. The Response Policy must allow for the execution of Workflows
B. The script must exist on the host locally
C. The script must contain input and output JSON fields
D. The Share with workflows option must be enabled for the custom script
Answer: (SHOW ANSWER)
For a custom script to be executed from a Fusion SOAR Workflow, it must be made available to workflows by enabling the "Share with workflows" option. This is a permissions and availability requirement: the workflow engine cannot call a custom script unless the script has explicitly been shared for workflow use. The script does not need to already exist locally on the endpoint, because Falcon can invoke scripts through RTR mechanisms depending on configuration. Input and output JSON fields may be useful for structured automation, but they are not the core prerequisite stated in the question. A Response Policy controls RTR permissions and access, but the specific workflow execution requirement is that the custom script must be shared with workflows.

NEW QUESTION: 56
When an analyst is trying to pinpoint the exact moment an endpoint came online after being shut down for the weekend, which timeline view is the best to use?
A. Host Timeline
B. Network Timeline
C. Process Timeline
D. User Timeline
Answer: (SHOW ANSWER)

NEW QUESTION: 57
An analyst needs to perform local sandbox analysis on a malicious file. When they download a quarantined file from the Falcon UI, what is the file format and the default password?
A. .7-zip, password: infected
B. .exe, no password
C. .zip, password: crowdstrike
D. .rar, password: malware
Answer: (SHOW ANSWER)

NEW QUESTION: 58
Data retention is a key factor in retrospective hunting. How long will " Detection Related Events " be retained in the Falcon environment?
A. 1 year
B. 30 days
C. 90 days
D. 60 days
Answer: (SHOW ANSWER)

NEW QUESTION: 59
When an analyst downloads a quarantined file from the Falcon UI for offline analysis, what is the specific file format and the required password for extraction?
A. The file is downloaded as a 7-zip archive and requires the password 'infected' for extraction.
B. The file is downloaded in its raw binary format without any encryption or compression.
C. The file is downloaded as a standard ZIP archive but does not require a password to open.
D. The file is downloaded as an encrypted .exe that can only be opened by a CrowdStrike sensor.
Answer: (SHOW ANSWER)
I have expanded and refined these questions to reflect the high-complexity, scenario-based format used in theCrowdStrike Certified Falcon Responder (CCFR)exam. These revised questions now include detailed operational context and focus on administrative nuances.

NEW QUESTION: 60
A responder is using ' Host Search ' to gather baseline data on a machine. Which of the following pieces of information is NOT provided by the Host Search results?
freecram.net
A. Macro Execution History for Microsoft Office products.
B. Recent network connections and IP addresses.
C. List of running services and drivers.
D. List of local user accounts and administrators.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 61
In the context of raw event searching, the term 'ProcessRollup2' refers to a value within which field?
A. event_type
B. process_status
C. action_id
D. event_simpleName
Answer: (SHOW ANSWER)

Valid CCFR-201b Dumps shared by EduDump.com for Helping Passing CCFR-201b Exam! EduDump.com now offer the **newest CCFR-201b exam dumps**, the EduDump.com CCFR-201b exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CCFR-201b dumps with Test Engine here: https://www.edudump.com/exams/CrowdStrike/CCFR-201b/premium/ (**212** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 62

A responder is focused on a specific malicious script and wants to see everything that the script ' s process did. Which timeline is the best tool for this task?

A. Administrative Timeline

B. User Timeline

C. Process Timeline

D. Host Timeline

Answer: (SHOW ANSWER)

NEW QUESTION: 63

In the 'User Search - File Written' section, a responder can see various files dropped by a user. Which of the following file types CANNOT be seen from this view?

A. Archive files (.zip, .7z)

B. Executions (Process starts)

C. Scripts (.ps1, .sh)

D. Executables (.exe)

Answer: (SHOW ANSWER)

NEW QUESTION: 64

Sensor Visibility Exclusion patterns are written in which syntax?

A. Kleene Star Syntax

B. SPL(Splunk)

C. RegEx

D. Glob Syntax

Answer: (SHOW ANSWER)

NEW QUESTION: 65

Responders use 'IP Search' to track connections to malicious infrastructure. Which of the following statements about the IP Search is FALSE?

A. It provides Intel data if the IP is known to CrowdStrike.

B. It shows the first and last time the IP was seen in the environment.

C. It identifies every host that connected to a specific IP.

D. The search only allows for one IP to be entered at a time.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 66

When a responder is looking at the ' Full Detection Details ' page, they can toggle between several views.

Which of the following is NOT a layout option available for viewing these details?

A. Process Timeline

B. List View

C. Tree View

D. Graph View
Answer: (SHOW ANSWER)

NEW QUESTION: 67
When investigating system-level persistence, it is critical to know what the services.exe process is responsible for. What is its primary function?
A. Monitoring network traffic for potential data exfiltration.
B. Managing user profiles and registry hives during login.
C. Providing a graphical interface for the Windows Task Manager.
D. Launching and managing the lifecycle of system services.
Answer: (SHOW ANSWER)

NEW QUESTION: 68
Which statement is TRUE regarding the "Bulk Domains" search?
A. The "Bulk Domains" search will allow you to blocklist your queried domains
B. It will show a list of computers and process that performed a lookup of any of the domains in your search
C. The "Bulk Domains" search will show IP address and port information for any associated connections
D. You should only pivot to the "Bulk Domains" search tool after completing an investigation
Answer: (SHOW ANSWER)

NEW QUESTION: 69
A responder is analyzing a process tree where a suspicious executable is listed as a direct child of services.
exe. In this scenario, which source is most likely responsible for the execution?
A. A web browser download initiated by the end user.
B. A Windows Service or a process launched by the Service Control Manager.
C. A script executed directly from a removable USB drive.
D. An interactive user login via RDP.
Answer: (SHOW ANSWER)

NEW QUESTION: 70
Administrators can define their own criteria for alerts. Which of the following is an example of a custom detection within the Falcon platform?
Freecram.net
A. Overwatch Managed Detections
B. Sensor-based Malware Detections
C. Behavioral IOA Detections
D. Blacklisted Hashes
Answer: (SHOW ANSWER)

NEW QUESTION: 71
When performing a 'Hash Search', which of the following is NOT a filter available for use?
A. Filename
B. SHA256
C. File Type
D. MD5
Answer: (SHOW ANSWER)

NEW QUESTION: 72
Which Executive Summary dashboard item indicates sensors running with unsupported versions?
A. Detections by Severity
B. Active Sensors
C. Inactive Sensors
D. Sensors in RFM
Answer: (SHOW ANSWER)

NEW QUESTION: 73
You can jump to a Process Timeline from many views, like a Hash Search, by clicking which of the following?
A. PID
B. UTCtime
C. Process ID or Parent Process ID
D. ProcessTimeline Link
Answer: C (LEAVE A REPLY)

NEW QUESTION: 74
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 creates a count of event types only, which can be useful when scoping the event
D. The Process Activity View only creates a summary of Dynamic Link Libraries (DLLs) loaded by a process
Answer: (SHOW ANSWER)

NEW QUESTION: 75

During the configuration of a new IOA rule, the administrator must decide what action the sensor should take.
Which of the following is NOT a valid IOA rule action?
A. Block
B. No Action
C. Monitor
D. Kill Process
Answer: (SHOW ANSWER)

NEW QUESTION: 76
What do IOA exclusions help you achieve?
A. Reduce false positives of behavioral detections from IOA based detections based on a file hash
B. Reduce false positives of behavioral detections from IOA based detections only
C. Reduce false positives of behavioral detections from Custom IOA and OverWatch detections only
D. Reduce false positives based on Next-Gen Antivirus settings in the Prevention Policy
Answer: (SHOW ANSWER)

Valid CCFR-201b Dumps shared by EduDump.com for Helping Passing CCFR-201b Exam! EduDump.com now offer the **newest CCFR-201b exam dumps**, the EduDump.com CCFR-201b exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CCFR-201b dumps with Test Engine here: https://www.edudump.com/exams/CrowdStrike/CCFR-201b/premium/ (**212** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 77
Which of the following subtitles/sub-views cannot be seen in the results of a 'Hash Search'?
A. Execution History
B. Process Timeline
C. Intel Indicators
D. File Metadata
Answer: (SHOW ANSWER)

NEW QUESTION: 78
What is an advantage of using the IP Search tool?
A. IP searches offer shortcuts to launch response actions and network containment on target hosts
B. IP searches provide manufacture and timezone data that can not be accessed anywhere else

C. IP searches allow for multiple comma separated IPv6 addresses as input
D. IP searches provide host, process, and organizational unit data without the need to write a query
Answer: (SHOW ANSWER)

NEW QUESTION: 79
To speed up investigations, Falcon uses ' event workflows ' . Which of the following sentences best describes what event workflows are?
A. They are PDF reports that summarize an incident for executive review.
B. They are automated searches that can be used to pivot between related events and searches.
C. They are automated scripts that perform remediation actions like killing processes.
D. They are schedules for when the sensor should perform a full disk scan.
Answer: (SHOW ANSWER)

NEW QUESTION: 80
From a detection, what is the fastest way to see children and sibling process information?
A. Select Full Detection Details from the detection
B. Select the Process Timeline feature, enter the AID. Target Process ID, and Parent Process ID
C. Select the Event Search option. Then from the Event Actions, select Show Associated Event Data (From TargetProcessId_decimal)
D. Right-click the process and select " Follow Process Chain "
Answer: (SHOW ANSWER)

NEW QUESTION: 81
How long are quarantined files stored on the host?
A. Quarantined files are never deleted from the host
B. 90 Days
C. 45 Days
D. 30 Days
Answer: (SHOW ANSWER)

NEW QUESTION: 82
A responder releases a file from quarantine on a specific workstation. What is the default scope of the allowlist that is created during this process?
A. All hosts within the same host group as the source host
B. Global (applies to all hosts in the environment)
C. All hosts running the same operating system version
D. Only the specific host where the file was originally quarantined
Answer: (SHOW ANSWER)

NEW QUESTION: 83

What are Event Actions?

A. Pivotable hyperlinks available in a Host Search

B. Custom event data queries bookmarked by the currently signed in Falcon user

C. Raw Falcon event data

D. Automated searches that can be used to pivot between related events and searches

Answer: (SHOW ANSWER)

NEW QUESTION: 84

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

A. Phishing

B. Eternal Blue

C. Emotet

D. Defense Evasion

Answer: (SHOW ANSWER)

NEW QUESTION: 85

CrowdStrike supports various deployment types. What is a 'POD sensor'?

A. A sensor specifically designed for mobile devices (iOS/Android).

B. A legacy sensor used only for disconnected or air-gapped systems.

C. A physical appliance that sits on the network to monitor traffic.

D. A sensor that is installed directly on a Kubernetes or Docker host to monitor containers.

Answer: (SHOW ANSWER)

NEW QUESTION: 86

While reviewing the high-level organizational structure of a complex detection in the Falcon console, a responder identifies several layers of activity. Which of the following is NOT officially recognized as an Objective Layer within the CrowdStrike detection hierarchy?

A. Gain Access

B. Lateral Movement

C. Contact Controlled Systems

D. Follow Through

Answer: (SHOW ANSWER)

NEW QUESTION: 87

How does a DNSRequest event link to its responsible process?

A. Via its ParentProcessId_decimal field

B. Via both its ContextProcessId__decimal and ParentProcessId_decimal fields

C. Via its TargetProcessId_decimal field

D. Via its ContextProcessId_decimal field

Answer: (SHOW ANSWER)

NEW QUESTION: 88
Evaluate the following process tree observed in a detection:
root > smss.exe > winlogon.exe > userinit.exe > explorer.exe > windows_media_player_y35s21-4ak.exe Based on the parent-child relationships, which entry source is most likely?
A. A phishing attack where the user executed a malicious file from the desktop.
B. A supply chain attack targeting the Windows Boot manager.
C. A remote service exploitation targeting a system process.
D. A scheduled task running under the SYSTEM account.
Answer: (SHOW ANSWER)

NEW QUESTION: 89
A SOC Manager is reviewing the monthly efficiency of the incident response team. They are specifically analyzing how many alerts were handled by each individual analyst and the ratio of legitimate threats to noise to optimize staffing levels. While navigating the Detection Resolutions Dashboard, which of the following metrics would they NOT find, as it is primarily located within the Activity or Executive summary dashboards?
A. Detection resolution status breakdown
B. Total count of False Positives
C. Total Detections by Host
D. Detections by user (Analyst performance)
Answer: (SHOW ANSWER)

Valid CCFR-201b Dumps shared by EduDump.com for Helping Passing CCFR-201b Exam! EduDump.com now offer the **newest CCFR-201b exam dumps**, the EduDump.com CCFR-201b exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CCFR-201b dumps with Test Engine here: https://www.edudump.com/exams/CrowdStrike/CCFR-201b/premium/ (**212** Q&As Dumps, **35%OFF Special Discount Code: freecram**)