CrowdStrike

Exam Questions CCFR-201

CrowdStrike Certified Falcon Responder

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
What information does the MITRE ATT&CK®Framework provide?

A. It provides best practices for different cybersecurity domains, such as Identify andAccess Management
B. It provides a step-by-step cyber incident response strategy
C. It provides the phases of an adversary's lifecycle, the platforms they are known to attack, and the specific methods they use
D. It is a system that attributes an attack techniques to a specific threat actor

Answer: C

Explanation:
According to the [MITRE ATT&CK website], MITRE ATT&CK is a knowledge base of adversary behaviors and techniques based on real-world observations. The knowledge base is organized into tactics and techniques, where tactics are the high-level goals of an adversary, such as initial access, persistence, lateral movement, etc., and techniques are the specific ways an adversary can achieve those goals, such as phishing, credential dumping, remote file copy, etc. The knowledge base also covers different platforms that adversaries target, such as Windows, Linux, Mac, Android, iOS, etc., and different phases of an adversary??s lifecycle, such as reconnaissance, resource development, execution, command and control, etc.

NEW QUESTION 2
You are notified by a third-party that a program may have redirected traffic to a malicious domain. Which Falcon page will assist you in searching for any domain request information related to this notice?

A. Falcon X
B. Investigate
C. Discover
D. Spotlight

Answer: B

Explanation:
According to the [CrowdStrike website], the Investigate page is where you can search for and analyze various types of data collected by the Falcon platform, such as events, hosts, processes, hashes, domains, IPs, etc1. You can use various tools, such as Event Search, Host Search, Process Timeline, Hash Search, Bulk Domain Search, etc., to perform different types of searches and view the results in different ways1. If you want to search for any domain request information related to a notice from a third-party, you can use the Investigate page to do so1. For example, you can use the Bulk Domain Search tool to search for the malicious domain and see which hosts and processes communicated with it1. You can also use the Event Search tool to search for DNSRequest events that contain the malicious domain and see more details about the query and response1.

NEW QUESTION 3
How does a DNSRequest event link to its responsible process?

A. Via both its ContextProcessId decimal and ParentProcessId_decimal fields
B. Via its ParentProcessId_decimal field
C. Via its ContextProcessId_decimal field
D. Via its TargetProcessId_decimal field

Answer: C

Explanation:
According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, a DNSRequest event contains information about a DNS query made by a process2. The event has several fields, such as DomainName, QueryType, QueryResponseCode, etc2. The field that links a DNSRequest event to its responsible process is ContextProcessId_decimal, which contains the decimal value of the process ID of the process that generated the event2. You can use this field to trace the process lineage and identify malicious or suspicious activities2.

NEW QUESTION 4
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 by creating an account
B. An adversary is trying to keep access through persistence using browser extensions
C. An adversary is trying to keep access through persistence using external remote services
D. adversary is trying to keep access through persistence using application skimming

Answer: A

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.

NEW QUESTION 5
Aside from a Process Timeline or Event Search, how do you export process event data from a detection in .CSV format?

A. You can't export detailed event data from a detection, you have to use the Process Timeline or an Event Search
B. In Full Detection Details, you expand the nodes of the process tree you wish to expand and then click the "Export Process Events" button
C. In Full Detection Details, you choose the "View Process Activity" option and then export from that view
D. From the Detections Dashboard, you right-click the event type you wish to export and choose CS

E. JSON or XML

Answer: C

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.

NEW QUESTION 6
The function of Machine Learning Exclusions is to .

A. stop all detections for a specific pattern ID
B. stop all sensor data collection for the matching path(s)
C. Stop all Machine Learning Preventions but a detection will still be generated and files will still be uploaded to the CrowdStrike Cloud
D. stop all ML-based detections and preventions for the matching path(s) and/or stop files from being uploaded to the CrowdStrike Cloud

Answer: D

Explanation:
According to the CrowdStrike Falcon® Data Replicator (FDR) Add-on for Splunk Guide, Machine Learning Exclusions allow you to exclude files or directories from being scanned by CrowdStrike??s machine learning engine, which can reduce false positives and improveperformance2. You can also choose whether to upload the excluded files to the CrowdStrike Cloud or not2.

NEW QUESTION 7
You notice that taskeng.exe is one of the processes involved in a detection. What activity should you investigate next?

A. User logons after the detection
B. Executions of schtasks.exe after the detection
C. Scheduled tasks registered prior to the detection
D. Pivot to a Hash search for taskeng.exe

Answer: C

Explanation:
According to the [Microsoft website], taskeng.exe is a legitimate Windows process that is responsible for running scheduled tasks. However, some malware may use this process or create a fake one to execute malicious code. Therefore, if you notice taskeng.exe involved in a detection, you should investigate whether there are any scheduled tasks registered prior to the detection that may have triggered or injected into taskeng.exe. You can use tools such as schtasks.exe or Task Scheduler to view or manage scheduled tasks.

NEW QUESTION 8
Which of the following is NOT a valid event type?

A. StartofProcess
B. EndofProcess
C. ProcessRollup2
D. DnsRequest

Answer: B

Explanation:
According to the [CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+], event types are categories of events that are generated by the sensor for various activities, such as process executions, file writes, registry modifications, network connections, etc. There are many valid event types, such as StartOfProcess, ProcessRollup2, DnsRequest, etc. However, EndOfProcess is not a valid event type, as there is no such event that records the end of a process.

NEW QUESTION 9
What happens when a quarantined file is released?

A. It is moved into theC:\CrowdStrike\Quarantine\Releasedfolder on the host
B. It is allowed to execute on the host
C. It is deleted
D. It is allowed to execute on all hosts

Answer: D

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 organization1. This action also removes the file from the quarantine list and deletes it from the CrowdStrike Cloud1.

NEW QUESTION 10
When looking at the details of a detection, there are two fields called Global Prevalence and Local Prevalence. Which answer best defines Local Prevalence?

A. Local prevalence is the frequency with which the hash of the triggering file is seen across the entire Internet
B. Local Prevalence tells you how common the hash of the triggering file is within your environment (CID)
C. Local Prevalence is the Virus Total score for the hash of the triggering file
D. Local prevalence is the frequency with which the hash of the triggering file is seen across all CrowdStrike customer environments

Answer: B

Explanation:
According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, Global Prevalence and Local Prevalence are two fields that provide information about how common or rare a file is based on its hash value2. Global Prevalence tells you how frequently the hash of the triggering file is seen across all CrowdStrike customer environments2. Local Prevalence tells you how frequently the hash of the triggering file is seen within your environment (CID)2. These fields can help you assess the risk and impact of a detection2.

NEW QUESTION 10
The Falcon platform will show a maximum of how many detections per day for a single Agent Identifier (AID)?

A. 500
B. 750
C. 1000
D. 1200

Answer: C

Explanation:
According to the CrowdStrike Falcon® Data Replicator (FDR) Add-on for Splunk Guide, the Falcon platform will show a maximum of 1000 detections per day for a single AID1. This is a limitimposed by the Falcon API, which is used to retrieve the detections from the CrowdStrike Cloud1. If there are more than 1000 detections per day for a single AID, only the first 1000 will be shown1.

NEW QUESTION 14
Which statement is TRUE regarding the "Bulk Domains" search?

A. It will show a list of computers and process that performed a lookup of any of the domains in your search
B. The "Bulk Domains" search will allow you to blocklist your queried domains
C. The "Bulk Domains" search will show IP address and port information for any associated connectionsD.You should only pivot to the "Bulk Domains" search tool after completing an investigation

Answer: A

Explanation:
According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Bulk Domain Search tool allows you to search for one or more domains and view a summary of information from Falcon events that contain those domains2. The summary includes the hostname, sensor ID, OS, country, city, ISP, ASN, geolocation, process name, command line, and organizational unit of the host that performed a lookup of any of the domains in your search2. This can help you identify potential threats or vulnerabilities in your network2.

NEW QUESTION 19
What information is contained within a Process Timeline?

A. All cloudable process-related events within a given timeframe
B. All cloudable events for a specific host
C. Only detection process-related events within a given timeframe
D. A view of activities on Mac or Linux hosts

Answer: A

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.

NEW QUESTION 20
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 only creates a summary of Dynamic Link Libraries (DLLs) loaded by a process
D. The Process Activity View creates a count of event types only, which can be useful when scoping the event

Answer: A

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.

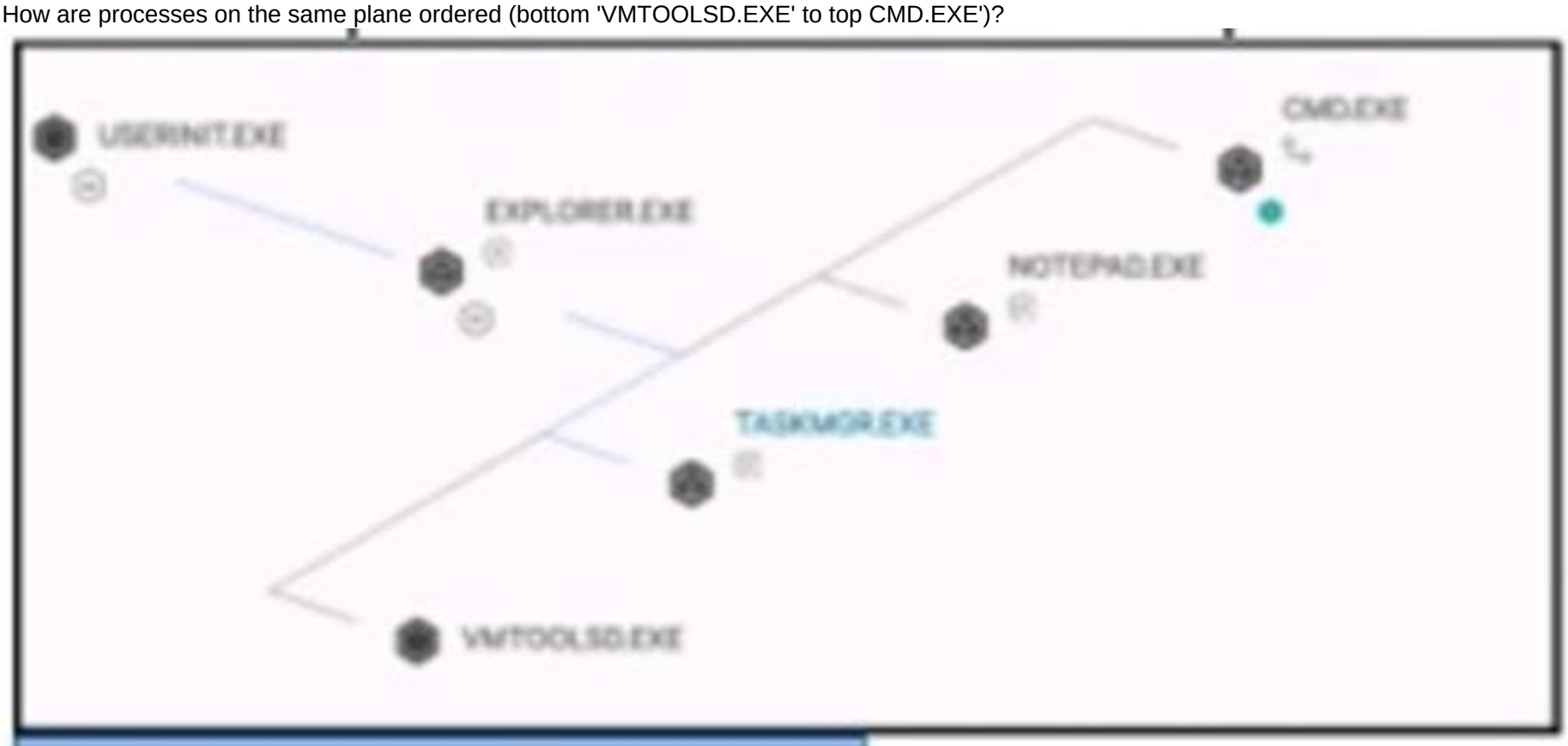
NEW QUESTION 23
From the Detections page, how can you view 'in-progress' detections assigned to Falcon Analyst Alex?

A. Filter on'Analyst: Alex'
B. Alex does not have the correct role permissions as a Falcon Analyst to be assigned detections
C. Filter on 'Hostname: Alex' and 'Status: In-Progress'
D. Filter on 'Status: In-Progress' and 'Assigned-to: Alex*

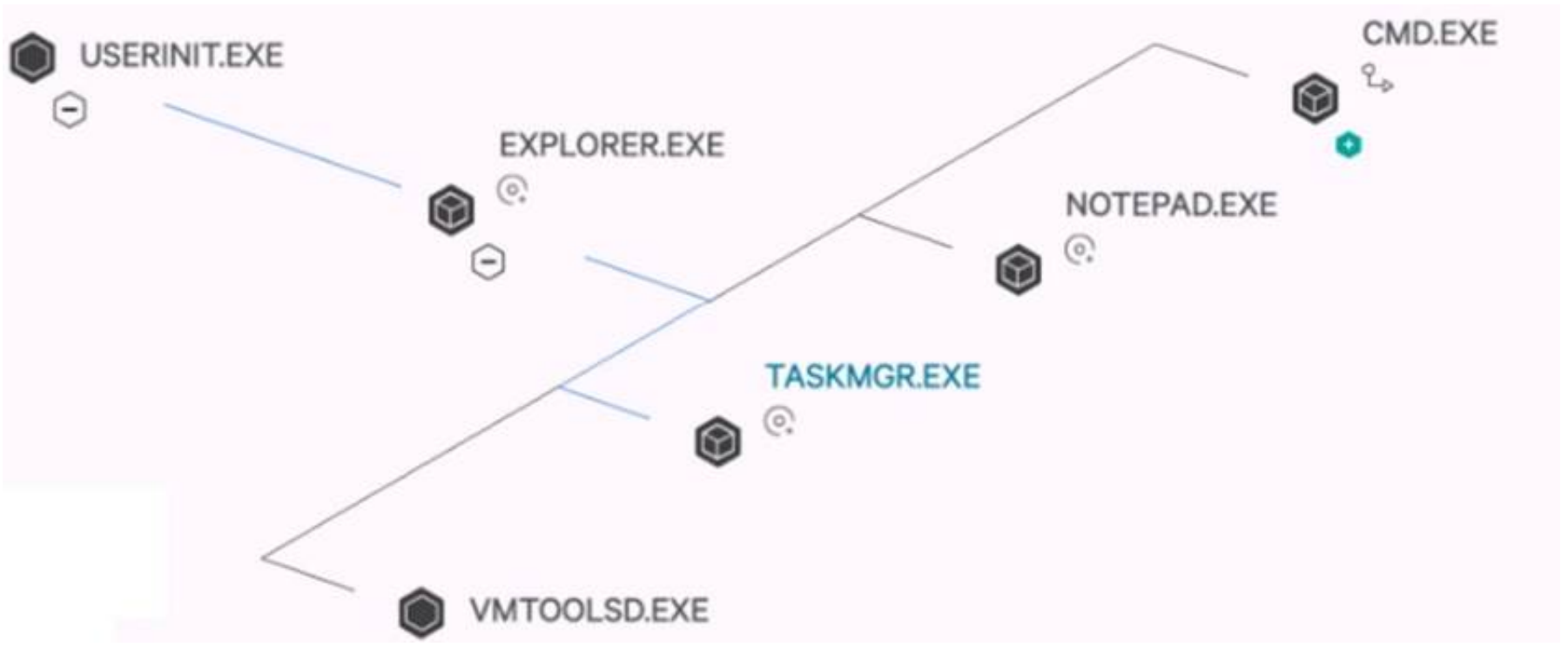
Answer: D

Explanation:
According to the CrowdStrike Falcon® Data Replicator (FDR) Add-on for Splunk Guide, the Detections page allows you to view and manage detections generated by the CrowdStrike Falcon platform2. You can use various filters to narrow down the detections based on criteria such asstatus, severity, tactic, technique, etc2. To view ??in-progress?? detections assigned to Falcon Analyst Alex, you can filter on ??Status: In-Progress?? and 'Assigned-to: Alex*'2. The asterisk (*) is a wildcard that matches any characters after Alex2.

NEW QUESTION 27
How are processes on the same plane ordered (bottom 'VMTOOLSD.EXE' to top CMD.EXE')?



Click to Enlarge



A. Process ID (Descending, highest on bottom)
B. Time started (Descending, most recent on bottom)
C. Time started (Ascending, most recent on top)
D. Process ID (Ascending, highest on top)

Answer: B

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.

NEW QUESTION 29
What are Event Actions?

A. Automated searches that can be used to pivot between related events and searches
B. Pivotable hyperlinks available in a Host Search
C. Custom event data queries bookmarked by the currently signed in Falcon user
D. Raw Falcon event data

Answer: A

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.

NEW QUESTION 31
From a detection, what is the fastest way to see children and sibling process information?

A. Select the Event Search optio
B. Then from the Event Actions, select Show Associated Event Data (From TargetProcessId_decimal)
C. Select Full Detection Details from the detection
D. Right-click the process and select "Follow Process Chain"
E. Select the Process Timeline feature, enter the AI
F. Target Process ID, and Parent Process ID

Answer: B

Explanation:
According to the CrowdStrike Falcon® Data Replicator (FDR) Add-on for Splunk Guide, the Full Detection Details tool allows you to view detailed information about a detection, such as detection ID, severity, tactic, technique, description, etc1. You can also view the events generated by the processes involved in the detection in different ways, such as process tree, process timeline, or process activity1. The process tree view provides a graphical representation of the process hierarchy and activity1. You can see children and sibling processes information by expanding or collapsing nodes in the tree1.

NEW QUESTION 33
In the "Full Detection Details", which view will provide an exportable text listing of events like DNS requests. Registry Operations, and Network Operations?

A. Thedata is unable to be exported
B. View as Process Tree
C. View as Process Timeline
D. View as Process Activity

Answer: D

Explanation:
According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Full Detection Details tool allows you to view detailed information about a detection, such as detection ID, severity, tactic, technique, description, etc1. You can also view the events generated by the processes involved in the detection in different ways, such as process tree, process timeline, or process activity1. The process activity view provides a rows-and-columns style view of the events, such as DNS requests, registry operations, network operations, etc1. You can also export this view to a CSV file for further analysis1.

NEW QUESTION 35
When analyzing an executable with a global prevalence of common; but you do not know what the executable is. what is the best course of action?

A. Do nothing, as this file is common and well known
B. From detection, click the VT Hash button to pivot to VirusTotal to investigate further
C. From detection, use API manager to create a custom blocklist
D. From detection, submit to FalconX for deep dive analysis

Answer: B

Explanation:
According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, global prevalence is a field that indicates how frequently the hash of a file is seen across all CrowdStrike customer environments1. A global prevalence of common means that the file is widely distributed and likely benign1. However, if you do not know what the executable is, you may want to investigate it further to confirm its legitimacy and functionality1. One way to do that is to click the VT Hash button from the detection, which will pivot you to VirusTotal, a service that analyzes files and URLs for viruses, malware, and other threats1. You can then see more information about the file, such as its name, size, type, signatures, detections, comments, etc1.

NEW QUESTION 36
When you configure and apply an IOA exclusion, what impact does it have on the host and what you see in the console?

A. The process specified is not sent to the Falcon Sandbox for analysis
B. The associated detection will be suppressed and the associated process would have been allowed to run
C. The sensor will stop sending events from the process specified in the regex pattern
D. The associated IOA will still generate a detection but the associated process would have been allowed to run

Answer: B

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.

NEW QUESTION 39
What does the Full Detection Details option provide?

A. It provides a visualization of program ancestry via the Process Tree View
B. It provides a visualization of program ancestry via the Process Activity View
C. It provides detailed list of detection events via the Process Table View
D. It provides a detailed list of detection events via the Process Tree View

Answer: A

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.

NEW QUESTION 40
After running an Event Search, you can select many Event Actions depending on your results. Which of the following is NOT an option for any Event Action?

A. Draw Process Explorer
B. Show a +/- 10-minute window of events
C. Show a Process Timeline for the responsible process
D. Show Associated Event Data (from TargetProcessId_decimal or ContextProcessId_decimal)

Answer: A

Explanation:
According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Event Search tool allows you to search for events based on various criteria, such as event type, timestamp, hostname, IP address, etc1. You can also select one or more events and perform various actions, such as show a process timeline, show a host timeline, show associated event data, show a +/- 10-minute window of events, etc1. However, there is no option to draw a process explorer, which is a graphical representation of the process hierarchy and activity1.

NEW QUESTION 45
Which of the following tactic and technique combinations is sourced from MITRE ATT&CK information?

A. Falcon Intel via Intelligence Indicator - Domain
B. Machine Learning via Cloud-Based ML
C. Malware via PUP
D. Credential Access via OS Credential Dumping

Answer: D

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.

NEW QUESTION 46
What action is used when you want to save a prevention hash for later use?

A. Always Block
B. Never Block
C. Always Allow
D. No Action

Answer: A

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.

NEW QUESTION 50
.....

Relate Links

100% Pass Your CCFR-201 Exam with Exambible Prep Materials

https://www.exambible.com/CCFR-201-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/