Free Questions for CCFR-201 by dumpshq

Shared by Stuart on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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?

Options:

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 theCrowdStrike 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.

Question 2

Question Type: MultipleChoice

The Process Activity View provides a rows-and-columns style view of the events generated in a detection. Why might this be helpful?

Options:

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 theCrowdStrike 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.

Question 3

Question Type: MultipleChoice

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

Options:

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 theCrowdStrike 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 status, 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.

Question 4

Question Type: MultipleChoice

Where can you find hosts that are in Reduced Functionality Mode?

Options:

A- Event Search

B- Executive Summary dashboard

C- Host Search

D- Installation Tokens

Answer:

C

Explanation:

According to theCrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, Reduced Functionality Mode (RFM) is a state where a host'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.

Question 5

Question Type: MultipleChoice

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

Options:

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.

Question 6

Question Type: MultipleChoice

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

Options:

A- Eternal Blue

B- Defense Evasion

C- Emotet

D- Phishing

Answer:

B

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.

Question 7

Question Type: MultipleChoice

Which is TRUE regarding a file released from quarantine?

Options:

A- No executions are allowed for 14 days after release

B- It is allowed to execute on all hosts

C- It is deleted

D- It will not generate future machine learning detections on the associated host

Answer:

B

Explanation:

According to theCrowdStrike 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.

Question 8

Question Type: MultipleChoice

Which of the following is returned from the IP Search tool?

Options:

A- IP Summary information from Falcon events containing the given IP

B- Threat Graph Data for the given IP from Falcon sensors

C- Unmanaged host data from system ARP tables for the given IP D. IP Detection Summary information for detection events containing the given IP

Answer:

A

Explanation:

According to theCrowdStrike 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.

Question 9

Question Type: MultipleChoice

What happens when a hash is allowlisted?

Options:

A- Execution is prevented, but detection alerts are suppressed

B- Execution is allowed on all hosts, including all other Falcon customers

C- The hash is submitted for approval to be allowed to execute once confirmed by Falcon specialists

D- Execution is allowed on all hosts that fall under the organization's CID

Answer:

D

Explanation:

According to theCrowdStrike Falcon Data Replicator (FDR) Add-on for Splunk Guide, the allowlist feature allows you to exclude files or directories from being scanned or blocked by CrowdStrike's machine learning engine or indicators of attack (IOAs)2.This can reduce false positives and improve performance2.When you allowlist a hash, you are allowing that file to execute on any host that belongs to your organization's CID (customer ID)2.This does not affect other Falcon customers or hosts outside your CID2.

Question 10

Question Type: MultipleChoice

A list of managed and unmanaged neighbors for an endpoint can be found:

Options:

A- by using Hosts page in the Investigate tool

B- by reviewing 'Groups' in Host Management under the Hosts page

C- under 'Audit' by running Sensor Visibility Exclusions Audit

D- only by searching event data using Event Search

Answer:

A

Explanation:

According to theCrowdStrike 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.This can help you identify potential threats or vulnerabilities in your network2.

Question 11

Question Type: MultipleChoice

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

Options:

A- Always Block

B- Never Block

C- Always Allow

D- No Action

Answer:

A

Explanation:

According to theCrowdStrike 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.