Free Questions for CCFH-202 by ebraindumps

Shared by Landry on 02-05-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which field in a DNS Request event points to the responsible process?

Options:

A- ContextProcessId_readable

B- TargetProcessId_decimal

C- ContextProcessId_decimal

D- ParentProcessId_decimal

Answer:

A

Explanation:

The ContextProcessId_readable field in a DNS Request event points to the responsible process. The ContextProcessId_readable field is the readable representation of the process identifier for the process that initiated the DNS request. It can be used to identify which process was communicating with a specific domain or IP address. The TargetProcessId_decimal, ContextProcessId_decimal, and

ParentProcessId_decimal fields do not point to the responsible process.

Question 2

Question Type: MultipleChoice

You are reviewing a list of domains recently banned by your organization's acceptable use policy. In particular, you are looking for the number of hosts that have visited each domain. Which tool should you use in Falcon?

Options:

A- Create a custom alert for each domain

B- Allowed Domain Summary Report

C- Bulk Domain Search

D- IP Addresses Search

Answer:

C

Explanation:

Bulk Domain Search is the tool that you should use in Falcon to review a list of domains recently banned by your organization's acceptable use policy and look for the number of hosts that have visited each domain. Bulk Domain Search is an Investigate tool that allows you to search for multiple domains at once and view their network connection events across all hosts in your environment. It shows information such as domain name, number of hosts visited, number of detections generated, etc. for each domain. Create a custom alert for each domain, Allowed Domain Summary Report, and IP Addresses Search are not tools that you should use for this purpose.

Question 3

Question Type: MultipleChoice

What information is shown in Host Search?

Options:

A- Quarantined Files

B- Prevention Policies

C- Intel Reports

D- Processes and Services

Answer:

D

Explanation:

Processes and Services is one of the information that is shown in Host Search. Host Search is an Investigate tool that allows you to view events by category, such as process executions, network connections, file writes, etc. Processes and Services is one of the categories that shows information such as process name, command line, parent process name, parent command line, etc. for each process execution event on a host. Quarantined Files, Prevention Policies, and Intel Reports are not shown in Host Search.

Question 4

Question Type: MultipleChoice

When performing a raw event search via the Events search page, what are Event Actions?

Options:

A- Event Actions contains an audit information log of actions an analyst took in regards to a specific detection

B- Event Actions contains the summary of actions taken by the Falcon sensor such as quarantining a file, prevent a process from executing or taking no actions and creating a detection only

C- Event Actions are pivotable workflows including connecting to a host, pre-made event searches and pivots to other investigatory pages such as host search

D- Event Actions is the field name that contains the event name defined in the Events Data Dictionary such as ProcessRollup, SyntheticProcessRollup, DNS request, etc

Answer:

C

Explanation:

When performing a raw event search via the Events search page, Event Actions are pivotable workflows that allow you to perform various tasks related to the event or the host. For example, you can connect to a host using Real Time Response, run pre-made event searches based on the event type or name, or pivot to other investigatory pages such as host search, hash search, etc. Event Actions do not contain audit information log, summary of actions taken by the Falcon sensor, or the event name defined in the Events Data Dictionary.

Question 5

Question Type: MultipleChoice

To view Files Written to Removable Media within a specified timeframe on a host within the Host Search page, expand and refer to the _____dashboard panel.

Options:

A- Command Line and Admin Tools

B- Processes and Services

C- Registry, Tasks, and Firewall

D- Suspicious File Activity

Answer:

D

Explanation:

To view Files Written to Removable Media within a specified timeframe on a host within the Host Search page, you need to expand and refer to the Suspicious File Activity dashboard panel. The Suspicious File Activity dashboard panel shows information such as files

written to removable media, files written to system directories by non-system processes, files written to startup folders, etc. The other dashboard panels do not show files written to removable media.

Question 6

Question Type: MultipleChoice

What kind of activity does a User Search help you investigate?

Options:

A- A history of Falcon Ul logon activity

B- A list of process activity executed by the specified user account

C- A count of failed user logon activity

D- A list of DNS queries by the specified user account

Answer:

B

Explanation:

User Search is an Investigate tool that helps you investigate a list of process activity executed by the specified user account. It shows information such as process name, command line, parent process name, parent command line, etc. for each process that was executed by the user account on any host in your environment. It does not show a history of Falcon UI logon activity, a count of failed user logon activity, or a list of DNS queries by the specified user account.

Question 7

Question Type: MultipleChoice

What information is provided when using IP Search to look up an IP address?

Options:

A- Both internal and external IPs

B- Suspicious IP addresses

C- External IPs only

D- Internal IPs only

Answer:

C

Explanation:

IP Search is an Investigate tool that allows you to look up information about external IPs only. It shows information such as geolocation, network connection events, detection history, etc. for each external IP address that has communicated with your hosts. It does not show information about internal IPs, suspicious IPs, or both internal and external IPs.

Question 8

Question Type: MultipleChoice

Which field in a DNS Request event points to the responsible process?

Options:

A- ContextProcessId_readable

B- TargetProcessId_decimal

C- ContextProcessId_decimal

D- ParentProcessId_decimal

Answer:

A

Explanation:

The ContextProcessId_readable field in a DNS Request event points to the responsible process. The ContextProcessId_readable field is the readable representation of the process identifier for the process that initiated the DNS request. It can be used to identify which process was communicating with a specific domain or IP address. The TargetProcessId_decimal, ContextProcessId_decimal, and ParentProcessId_decimal fields do not point to the responsible process.

Question 9

Question Type: MultipleChoice

To view Files Written to Removable Media within a specified timeframe on a host within the Host Search page, expand and refer to the _____dashboard panel.

Options:

A- Command Line and Admin Tools

B- Processes and Services

C- Registry, Tasks, and Firewall

D- Suspicious File Activity

Answer:

D

Explanation:

To view Files Written to Removable Media within a specified timeframe on a host within the Host Search page, you need to expand and refer to the Suspicious File Activity dashboard panel. The Suspicious File Activity dashboard panel shows information such as files written to removable media, files written to system directories by non-system processes, files written to startup folders, etc. The other dashboard panels do not show files written to removable media.

Question 10

Question Type: MultipleChoice

What information is shown in Host Search?

Options:

A- Quarantined Files

B- Prevention Policies

C- Intel Reports

D- Processes and Services

Answer:

D

Explanation:

Processes and Services is one of the information that is shown in Host Search. Host Search is an Investigate tool that allows you to view events by category, such as process executions, network connections, file writes, etc. Processes and Services is one of the categories that shows information such as process name, command line, parent process name, parent command line, etc. for each process execution event on a host. Quarantined Files, Prevention Policies, and Intel Reports are not shown in Host Search.

Question 11

Question Type: MultipleChoice

What information is provided when using IP Search to look up an IP address?

Options:

A- Both internal and external IPs

B- Suspicious IP addresses

C- External IPs only

D- Internal IPs only

Answer:

C

Explanation:

IP Search is an Investigate tool that allows you to look up information about external IPs only. It shows information such as geolocation, network connection events, detection history, etc. for each external IP address that has communicated with your hosts. It does not show information about internal IPs, suspicious IPs, or both internal and external IPs.