Free Questions for CCFH-202 by vceexamstest

Shared by Keller on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

With Custom Alerts you are able to configure email alerts using predefined templates so you're notified about specific activity in your environment. Which of the following outlines the steps required to properly create a custom alert rule?

Options:

A- Choose the template you would like to configure, setup how often you would like the alert to run, and then schedule the alert

B- Choose the template you would like to configure, preview the search results, and then schedule the alert

C- Create the query for the alert, setup the email template for the alert, and then set the schedule for the alert

D- Create a new custom template, configure the email template, and then create the custom query for the alert

Answer:

B

Explanation:

These are the steps required to properly create a custom alert rule. Custom Alerts are a feature that allows you to configure email alerts using predefined templates so you're notified about specific activity in your environment. You can choose from various templates that cover different use cases, such as suspicious PowerShell activity, network connections to risky countries, etc. You can also preview the search results of the template before scheduling the alert. You do not need to create the query for the alert, setup the email template for the alert, or create a new custom template, as these are already provided by the predefined templates.

Question 2

Question Type: MultipleChoice

Which of the following is TRUE about a Hash Search?

Options:

A- Wildcard searches are not permitted with the Hash Search

B- The Hash Search provides Process Execution History

C- The Hash Search is available on Linux

D- Module Load History is not presented in a Hash Search

Answer:

B

Explanation:

The Hash Search is an Investigate tool that allows you to search for a file hash and view its process execution history across all hosts in your environment. It shows information such as process name, command line, parent process name, parent command line, etc. for each execution of the file hash. Wildcard searches are permitted with the Hash Search, as long as they are at least four characters long. The Hash Search is available on Linux, as well as Windows and Mac OS X. Module Load History is presented in a Hash Search, along with other information such as File Write History and Detection History.

Question 3

Question Type: **MultipleChoice**

While you're reviewing Unresolved Detections in the Host Search page, you notice the User Name column contains "hostnameS " What does this User Name indicate?

Options:

A- The User Name is a System User

B- The User Name is not relevant for the dashboard

C- There is no User Name associated with the event

D- The Falcon sensor could not determine the User Name

Answer:

C

Explanation:

When you see "hostnameS" in the User Name column in the Host Search page, it means that there is no User Name associated with the event. This can happen when the event is related to a system process or service that does not have a user context. It does not mean that the User Name is a System User, that the User Name is not relevant for the dashboard, or that the Falcon sensor could not determine the User Name.

Question 4

Question Type: MultipleChoice

The Process Timeline Events Details table will populate the Parent Process ID and the Parent File columns when the cloudable Event data contains which event field?

Options:

A- ContextProcessld_decimal

B- RawProcessld_decimal

C- ParentProcessld_decimal

D- RpcProcessld_decimal

Answer:

C

Explanation:

The ParentProcessld_decimal event field is what the Process Timeline Events Details table will populate the Parent Process ID and the Parent File columns with when the cloudable Event data contains it. The ParentProcessld_decimal event field is the decimal representation of the process identifier for the parent process of the target process. It can be used to trace the process ancestry and identify potential malicious activity. The ContextProcessld_decimal, RawProcessld_decimal, and RpcProcessld_decimal event fields are not used to populate the Parent Process ID and the Parent File columns.

Question 5

Question Type: **MultipleChoice**

What is the difference between a Host Search and a Host Timeline?

Options:

A- Host Search is used for detection investigation and Host Timeline is used for proactive hunting

B- A Host Search organizes the data in useful event categories like process executions and network connections, a Host Timeline provides an uncategorized view of recorded events in chronological order

C- You access a Host Search from a detection to show you every recorded process event related to the detection and you can only populate the Host Timeline fields manually

D- There is no difference. You just get to them different ways

Answer:

B

Explanation:

This is the difference between a Host Search and a Host Timeline. A Host Search is an Investigate tool that allows you to view events by category, such as process executions, network connections, file writes, etc. A Host Timeline is an Investigate tool that allows you to view all events in chronological order, without any categorization. Both tools can be used for detection investigation and proactive hunting, depending on the use case and preference. You can access a Host Search from a detection or manually enter the host details. You can also populate the Host Timeline fields manually or from other pages in Falcon.

Question 6

Question Type: MultipleChoice

What elements are required to properly execute a Process Timeline?

Options:

A- Agent ID (AID) and Target Process ID

B- Agent ID (AID) only

C- Hostname and Local Process ID

D- Target Process ID only

Answer:

A

Explanation:

The Agent ID (AID) and the Target Process ID are the elements that are required to properly execute a Process Timeline. The Agent ID (AID) is a unique identifier for each host that has a Falcon sensor installed. The Target Process ID is the decimal representation of the process identifier for the process that you want to investigate. These two elements are used to query the cloud for the events related to the process on the host. The Agent ID (AID) only, the Hostname and Local Process ID, and the Target Process ID only are not sufficient to execute a Process Timeline.