Free Questions for CCFR-201 by actualtestdumps

Shared by English on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What does pivoting to an Event Search from a detection do?

Options:

A- It gives you the ability to search for similar events on other endpoints quickly

B- It takes you to the raw Insight event data and provides you with a number of Event Actions

C- It takes you to a Process Timeline for that detection so you can see all related events

D- It allows you to input an event type, such as DNS Request or ASEP write, and search for those events within the detection

Answer:

B

Explanation:

According to theCrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, pivoting to an Event Search from a detection takes you to the raw Insight event data and provides you with a number of Event Actions1.Insight events are low-level events that are generated by the sensor for various activities, such as process executions, file writes, registry modifications,

network connections, etc1.You can view these events in a table format and use various filters and fields to narrow down the results1.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.These actions can help you investigate and analyze events more efficiently and effectively1.

Question 2

Question Type: MultipleChoice

What are Event Actions?

Options:

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 theCrowdStrike 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.

Question 3

Question Type: MultipleChoice

Which Executive Summary dashboard item indicates sensors running with unsupported versions?

Options:

A- Detections by Severity

B- Inactive Sensors

C- Sensors in RFM

D- Active Sensors

Answer:

C

Explanation:

According to theCrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Executive Summary dashboard provides an overview of your sensor health and activity1.It includes various items, such as Active Sensors, Inactive Sensors, Detections by Severity, etc1.The item that indicates sensors running with unsupported versions is Sensors in RFM (Reduced Functionality Mode)1.RFM is a state where a sensor has limited functionality due to various reasons, such as license expiration, network issues, tampering attempts, or unsupported versions1.You can see the number and percentage of sensors in RFM and the reasons why they are in RFM1.

Question 4

Question Type: MultipleChoice

What happens when a hash is set to Always Block through IOC Management?

Options:

A- Execution is prevented on all hosts by default

B- Execution is prevented on selected host groups

C- Execution is prevented and detection alerts are suppressed

D- The hash is submitted for approval to be blocked from execution once confirmed by Falcon specialists

Answer:

A

Explanation:

According to theCrowdStrike Falcon Data Replicator (FDR) Add-on for Splunk Guide, IOC Management allows you to manage indicators of compromise (IOCs), which are artifacts such as hashes, IP addresses, or domains that are associated with malicious activities2.You can set different actions for IOCs, such as Allow, No Action, or Always Block2.When you set a hash to Always Block through IOC Management, you are preventing that file from executing on any host in your organization by default2.This action also generates a detection alert when the file is blocked2.

Question 5

Question Type: MultipleChoice

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?

Options:

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 theCrowdStrike 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.

Question 6

Question Type: MultipleChoice

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

Options:

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 theCrowdStrike 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 the associated 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.

Question 7

Question Type: MultipleChoice

What information does the MITRE ATT&CK Framework provide?

Options:

A- It provides best practices for different cybersecurity domains, such as Identify and Access 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.

Question 8

Question Type: MultipleChoice

How does a DNSRequest event link to its responsible process?

Options:

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 theCrowdStrike 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.

Question 9

Question Type: MultipleChoice

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

Options:

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 theCrowdStrike 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.

Question 10

Question Type: MultipleChoice

What happens when a quarantined file is released?

Options:

A- It is moved into the C:\CrowdStrike\Quarantine\Released folder 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 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 organization1.This action also removes the file from the quarantine list and deletes it from the CrowdStrike Cloud1.