Download CrowdStrike CCFR-201b Exam Dumps Free

Shared by Graves on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which option best 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 2

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 3

Question Type: MultipleChoice

You are reviewing the raw data in an event search from a detection tree. You find a FileOpenInfo event and want to find out if any other files were opened by the responsible process. Which two field values do you need from this event to perform a Process Timeline search?

Options:

A- ParentProcessId_decimal and aid
B- ResponsibleProcessId_decimal and aid
C- ContextProcessId_decimal and aid
D- TargetProcessId_decimal and aid

Answer:

D

Explanation:

According to theCrowdStrike 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, etc2.The tool requires two parameters:aid(agent ID)

andTargetProcessId_decimal(the decimal value of the process ID)2.These fields can be obtained from any event that involves the process, such as a FileOpenInfo event, which contains information about a file being opened by a process2.

Question 4

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 5

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 6

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 7

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.

Question 8

Question Type: MultipleChoice

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?

Options:

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.

Question 9

Question Type: MultipleChoice

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

Options:

A- The data 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 theCrowdStrike 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.

Question 10

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 11

Question Type: MultipleChoice

Sensor Visibility Exclusion patterns are written in which syntax?

Options:

A- Glob Syntax
B- Kleene Star Syntax
C- RegEx
D- SPL(Splunk)

Answer:

A

Explanation:

According to the [CrowdStrike Falcon Data Replicator (FDR) Add-on for Splunk Guide], Sensor Visibility Exclusions allow you to exclude files or directories from being monitored by the sensor. This can reduce the amount of data sent to the CrowdStrike Cloud and improve performance. Sensor Visibility Exclusion patterns are written in Glob Syntax, which is a simple pattern matching syntax that supports wildcards, such as *, ?, and . For example, you can use *.exe to exclude all files with .exe extension.