Free Questions for CCFR-201 by ebraindumps

Shared by Terrell on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

When examining a raw DNS request event, you see a field called ContextProcessId_decimal. What is the purpose of that field?

Options:

A- It contains the TargetProcessId_decimal value for other related events

B- It contains an internal value not useful for an investigation

C- It contains the ContextProcessId_decimal value for the parent process that made the DNS request

D- It contains the TargetProcessId_decimal value for the process that made the DNS request

Answer:

D

Explanation:

According to theCrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the ContextProcessId_decimal field contains the decimal value of the process ID of the process that generated the event1.This field can be used to trace the process lineage and identify malicious or suspicious activities1.For a DNS request event, this field indicates which

process made the DNS request1.

Question 2

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 3

Question Type: MultipleChoice

When reviewing a Host Timeline, which of the following filters is available?

Options:

A- Severity

B- Event Types

C- User Name

D- Detection ID

Answer:

B

Explanation:

According to theCrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Host Timeline tool allows you to view all events recorded by the sensor for a given host in a chronological order1.The events include process executions, file writes, registry modifications, network connections, user logins, etc1.You can use various filters to narrow down the events based on criteria such as event type, timestamp range, file name, registry key, network destination, etc1.However, there is no filter for severity, user name, or detection ID, as these are not attributes of the events1.

Question 4

Question Type: MultipleChoice

What do IOA exclusions help you achieve?

Options:

A- Reduce false positives based on Next-Gen Antivirus settings in the Prevention Policy

B- Reduce false positives of behavioral detections from IOA based detections only

C- Reduce false positives of behavioral detections from IOA based detections based on a file hash

D- Reduce false positives of behavioral detections from Custom IOA and OverWatch detections only

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 activities2.This can reduce false positives and improve performance2.IOA exclusions only apply to IOA based detections, not other types of detections such as machine learning, custom IOA, or OverWatch2.

Question 5

Question Type: MultipleChoice

Which of the following tactic and technique combinations is sourced from MITRE ATT&CK information?

Options:

A- Falcon Intel via Intelligence Indicator - Domain

B- Machine Learning via Cloud-Based ML

C- Malware via PUP

D- Credential Access via OS Credential Dumping

Answer:

D

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. Credential Access via OS Credential Dumping is an example of a tactic and technique combination sourced from MITRE ATT&CK information, which describes how adversaries can obtain credentials from operating system memory or disk storage by using tools such as Mimikatz or ProcDump.

Question 6

Question Type: MultipleChoice

Which option indicates a hash is allowlisted?

Options:

A- No Action

B- Allow

C- Ignore

D- Always Block

Answer:

B

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.The option to indicate that a hash is allowlisted is 'Allow'2.