**Vendor:**CrowdStrike

**Exam Code:**CCFR-201

**Exam Name:**CrowdStrike Certified Falcon Responder

**Version:**Demo

**QUESTION 1**

What do IOA exclusions help you achieve?

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

Correct Answer: B

According to the CrowdStrike 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 2**

Which of the following tactic and technique combinations is sourced from MITRE ATTandCK information?

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

Correct Answer: D

According to the [MITRE ATTandCK website], MITRE ATTandCK 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 ATTandCK information, which describes how adversaries can obtain credentials from operating system memory or disk storage by using tools such as Mimikatz or ProcDump.

---

**QUESTION 3**

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

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

Correct Answer: B

According to the CrowdStrike 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 4**

What happens when you create a Sensor Visibility Exclusion for a trusted file path?

A. It excludes host information from Detections and Incidents generated within that file path location

B. It prevents file uploads to the CrowdStrike cloud from that file path

C. It excludes sensor monitoring and event collection for the trusted file path

D. It disables detection generation from that path, however the sensor can still perform prevention actions

Correct Answer: C

According to the CrowdStrike Falcon?Data Replicator (FDR) Add-on for Splunk Guide, Sensor Visibility Exclusions allow you to exclude certain files or directories from being monitored by the CrowdStrike sensor, which can reduce noise and improve performance2. This means that no events will be collected or sent to the CrowdStrike Cloud for those files or directories2.

---

**QUESTION 5**

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

A. Detections by Severity

B. Inactive Sensors

C. Sensors in RFM

D. Active Sensors

Correct Answer: C

According to the CrowdStrike 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 6

What is an advantage of using the IP Search tool?

A. IP searches provide manufacture and timezone data that can not be accessed anywhere else

B. IP searches allow for multiple comma separated IPv6 addresses as input

C. IP searches offer shortcuts to launch response actions and network containment on target hosts

D. IP searches provide host, process, and organizational unit data without the need to write a query

Correct Answer: D

According to the CrowdStrike 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, geolocation, process name, command line, and organizational unit of the host that communicated with that IP address1. This is an advantage of using the IP Search tool because it provides host, process, and organizational unit data without the need to write a query1.

## QUESTION 7

What information is contained within a Process Timeline?

A. All cloudable process-related events within a given timeframe

B. All cloudable events for a specific host

C. Only detection process-related events within a given timeframe

D. A view of activities on Mac or Linux hosts

Correct Answer: A

According to the CrowdStrike 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, etc1. You can specify a timeframe to limit the events to a certain period1. The tool works for any host platform, not just Mac or Linux1.

## QUESTION 8

What is the difference between Managed and Unmanaged Neighbors in the Falcon console?

A. A managed neighbor is currently network contained and an unmanaged neighbor is uncontained

B. A managed neighbor has an installed and provisioned sensor

C. An unmanaged neighbor is in a segmented area of the network

D. A managed sensor has an active prevention policy

Correct Answer: B

According to the CrowdStrike Falcon?Data Replicator (FDR) Add-on for Splunk Guide, you can use the Hosts page in the Investigate tool to view information about your endpoints, such as hostname, IP address, OS, sensor version, etc2. You can also see a list of managed and unmanaged neighbors for each endpoint, which are other devices that have communicated with that endpoint over the network2. A managed neighbor is a device that has an installed and provisioned sensor that reports to the CrowdStrike Cloud2. An unmanaged neighbor is a device that does not have an installed or provisioned sensor2.

---

**QUESTION 9**

In the Hash Search tool, which of the following is listed under Process Executions?

A. Operating System

B. File Signature

C. Command Line

D. Sensor Version

Correct Answer: C

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Hash Search tool allows you to search for one or more SHA256 hashes and view a summary of information from Falcon events that contain those hashes1. The summary includes the hostname, sensor ID, OS, country, city, ISP, ASN, geolocation, process name, command line, and organizational unit of the host that loaded or executed those hashes1. You can also see a count of detections and incidents related to those hashes1. Under Process Executions, you can see the process name and command line for each hash execution1.

---

**QUESTION 10**

You found a list of SHA256 hashes in an intelligence report and search for them using the Hash Execution Search. What can be determined from the results?

A. Identifies a detailed list of all process executions for the specified hashes

B. Identifies hosts that loaded or executed the specified hashes

C. Identifies users associated with the specified hashes

D. Identifies detections related to the specified hashes

Correct Answer: B

According to the CrowdStrike Falcon Devices Add-on for Splunk Installation and Configuration Guide v3.1.5+, the Hash Execution Search tool allows you to search for one or more SHA256 hashes and view a summary of information from Falcon events that contain those hashes1. The summary includes the hostname, sensor ID, OS, country, city, ISP, ASN, and geolocation of the host that loaded or executed those hashes1. You can also see a count of detections and incidents related to those hashes1.

---

**QUESTION 11**

What happens when you open the full detection details?

A. Theprocess explorer opens and the detection is removed from the console

B. The process explorer opens and you\\'re able to view the processes and process relationships

C. The process explorer opens and the detection copies to the clipboard

D. The process explorer opens and the Event Search query is run for the detection

Correct Answer: B

According to the [CrowdStrike Falcon?Data Replicator (FDR) Add-on for Splunk Guide], when you open the full detection details from a detection alert or dashboard item, you are taken to a page where you can view detailed information about the detection, such as detection ID, severity, tactic, technique, description, etc. 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 activity. The process tree view is also known as the process explorer, which provides a graphical representation of the process hierarchy and activity. You can view the processes and process relationships by expanding or collapsing nodes in the tree. You can also see the event types and timestamps for each process.

---

**QUESTION 12**

You can jump to a Process Timeline from many views, like a Hash Search, by clicking which of the following?

A. ProcessTimeline Link

B. PID

C. UTCtime

D. Process ID or Parent Process ID

Correct Answer: D

According to the CrowdStrike 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, etc1. The tool requires two parameters: aid (agent ID) and TargetProcessId_decimal (the decimal value of the process ID)1. You can jump to a Process Timeline from many views, such as Hash Search, Host Timeline, Event Search, etc., by clicking on either the Process ID or Parent Process ID fields in those views1. This will automatically populate the aid and TargetProcessId_decimal parameters for the Process Timeline tool1.