Actual exam question from CrowdStrike's CCFR-201

Question #: 1

Topic #: 1

[All CCFR-201 Questions]

Where can you find hosts that are in Reduced Functionality Mode?

A. Event Search

B. Executive Summary dashboard

C. Host Search

D. Installation Tokens

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 2

Topic #: 1

[All CCFR-201 Questions]

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

A. Severity

B. Event Types

C. User Name

D. Detection ID

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 3

Topic #: 1

[All CCFR-201 Questions]

How does a DNSRequest event link to its responsible process?

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

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 4

Topic #: 1

[All CCFR-201 Questions]

What information does the MITRE ATT&CK Framework provide?

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 attack techniques to a specific threat actor

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 5

Topic #: 1

[All CCFR-201 Questions]

Within the MITRE-Based Falcon Detections Framework, what is the correct way to interpret Keep Access > Persistence > Create Account?

A. An adversary is trying to keep access through persistence by creating an account

B. An adversary is trying to keep access through persistence using browser extensions

C. An adversary is trying to keep access through persistence using external remote services

D. An adversary is trying to keep access through persistence using application skimming

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 6

Topic #: 1

[All CCFR-201 Questions]

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

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

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 7

Topic #: 1

[All CCFR-201 Questions]

What are Event Actions?

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

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 8

Topic #: 1

[All CCFR-201 Questions]

Where are quarantined files stored on Windows hosts?

A. Windows\Quarantine

B. Windows\System32\Drivers\CrowdStrike\Quarantine

C. Windows\System32\

D. Windows\temp\Drivers\CrowdStrike\Quarantine

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 9

Topic #: 1

[All CCFR-201 Questions]

How long does detection data remain in the CrowdStrike Cloud before purging begins?

A. 90 Days

B. 45 Days

C. 30 Days

D. 14 Days

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 10

Topic #: 1

[All CCFR-201 Questions]

What is an advantage of using a Process Timeline?

A. Process related events can be filtered to display specific event types

B. Suspicious processes are color-coded based on their frequency and legitimacy over time

C. Processes responsible for spikes in CPU performance are displayed over time

D. A visual representation of Parent-Child and Sibling process relationships is provided

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 11

Topic #: 1

[All CCFR-201 Questions]

What action is used when you want to save a prevention hash for later use?

A. Always Block

B. Never Block

C. Always Allow

D. No Action

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 12

Topic #: 1

[All CCFR-201 Questions]

You receive an email from a third-party vendor that one of their services is compromised, the vendor names a specific IP address that the compromised service was using. Where would you input this indicator to find any activity related to this IP address?

A. IP Addresses

B. Remote or Network Logon Activity

C. Remote Access Graph

D. Hash Executions

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 13

Topic #: 1

[All CCFR-201 Questions]

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?

A. ParentProcessId_decimal and aid

B. ResponsibleProcessId_decimal and aid

C. ContextProcessId_decimal and aid

D. TargetProcessId_decimal and aid

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 14

Topic #: 1

[All CCFR-201 Questions]

How long are quarantined files stored in the CrowdStrike Cloud?

A. 45 Days

B. 90 Days

C. 30 Days

D. Quarantined files are not deleted

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 15

Topic #: 1

[All CCFR-201 Questions]

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?

A. Falcon X

B. Investigate

C. Discover

D. Spotlight

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 16

Topic #: 1

[All CCFR-201 Questions]

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

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 17

Topic #: 1

[All CCFR-201 Questions]

Sensor Visibility Exclusion patterns are written in which syntax?

A. Glob Syntax

B. Kleene Star Syntax

C. RegEx

D. SPL (Splunk)

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 18

Topic #: 1

[All CCFR-201 Questions]

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

A. The data is unable to be exported

B. View as Process Tree

C. View as Process Timeline

D. View as Process Activity

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 19

Topic #: 1

[All CCFR-201 Questions]

What happens when a quarantined file is released?

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

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 20

Topic #: 1

[All CCFR-201 Questions]

Which is TRUE regarding a file released from quarantine?

A. No executions are allowed for 14 days after release

B. It is allowed to execute on all hosts

C. It is deleted

D. It will not generate future machine learning detections on the associated host

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 21

Topic #: 1

[All CCFR-201 Questions]

From the Detections page, how can you view 'in-progress' detections assigned to Falcon Analyst Alex?

A. Filter on 'Analyst: Alex'

B. Alex does not have the correct role permissions as a Falcon Analyst to be assigned detections

C. Filter on 'Hostname: Alex' and 'Status: In-Progress'

D. Filter on 'Status: In-Progress' and 'Assigned-to: Alex'

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 22

Topic #: 1

[All CCFR-201 Questions]

The Bulk Domain Search tool contains Domain information along with which of the following?

A. Process Information

B. Port Information

C. IP Lookup Information

D. Threat Actor Information

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 23

Topic #: 1

[All CCFR-201 Questions]

The Process Activity View provides a rows-and-columns style view of the events generated in a detection. Why might this be helpful?

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

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 24

Topic #: 1

[All CCFR-201 Questions]

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

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 25

Topic #: 1

[All CCFR-201 Questions]

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

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 26

Topic #: 1

[All CCFR-201 Questions]

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

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

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 27

Topic #: 1

[All CCFR-201 Questions]

The function of Machine Learning Exclusions is to _____.

A. stop all detections for a specific pattern ID

B. stop all sensor data collection for the matching path(s)

C. stop all Machine Learning Preventions but a detection will still be generated and files will still be uploaded to the CrowdStrike Cloud

D. stop all ML-based detections and preventions for the matching path(s) and/or stop files from being uploaded to the CrowdStrike Cloud

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 28

Topic #: 1

[All CCFR-201 Questions]

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

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 29

Topic #: 1

[All CCFR-201 Questions]

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

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 30

Topic #: 1

[All CCFR-201 Questions]

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

A. Results from a Host Search return information in an organized view by type, while a Host Timeline returns a view of all events recorded by the sensor

B. A Host Timeline only includes process execution events and user account activity

C. Results from a Host Timeline include process executions and related events organized by data type. A Host Search returns a temporal view of all events for the given host

D. There is no difference - Host Search and Host Timeline are different names for the same search page

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 31

Topic #: 1

[All CCFR-201 Questions]

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

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 32

Topic #: 1

[All CCFR-201 Questions]

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

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 33

Topic #: 1

[All CCFR-201 Questions]

What happens when you open the full detection details?

A. The process 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

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 34

Topic #: 1

[All CCFR-201 Questions]

After pivoting to an event search from a detection, you locate the ProcessRollup2 event. Which two field values are you required to obtain to perform a Process Timeline search so you can determine what the process was doing?

A. SHA256 and TargetProcessId_decimal

B. SHA256 and ParentProcessId_decimal

C. aid and ParentProcessId_decimal

D. aid and TargetProcessId_decimal

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 35

Topic #: 1

[All CCFR-201 Questions]

Which of the following is NOT a valid event type?

A. StartofProcess

B. EndofProcess

C. ProcessRollup2

D. DnsRequest

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 36

Topic #: 1

[All CCFR-201 Questions]

When examining raw event data, what is the purpose of the field called ParentProcessId_decimal?

A. It contains an internal value not useful for an investigation

B. It contains the TargetProcessId_decimal value of the child process

C. It contains the SensorId_decimal value for related events

D. It contains the TargetProcessId_decimal of the parent process

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 37

Topic #: 1

[All CCFR-201 Questions]

Which of the following is returned from the IP Search tool?

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

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 38

Topic #: 1

[All CCFR-201 Questions]

What types of events are returned by a Process Timeline?

A. Only detection events

B. All cloudable events

C. Only process events

D. Only network events

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 39

Topic #: 1

[All CCFR-201 Questions]

After running an Event Search, you can select many Event Actions depending on your results. Which of the following is NOT an option for any Event Action?

A. Draw Process Explorer

B. Show a +/- 10-minute window of events

C. Show a Process Timeline for the responsible process

D. Show Associated Event Data (from TargetProcessId_decimal or ContextProcessId decimal)

Show Suggested Answer

Actual exam question from CrowdStrike's CCFR-201

Question #: 40

Topic #: 1

[All CCFR-201 Questions]

From a detection, what is the fastest way to see children and sibling process information?

A. Select the Event Search option. Then from the Event Actions, select Show Associated Event Data (From TargetProcessId_decimal)

B. Select Full Detection Details from the detection

C. Right-click the process and select "Follow Process Chain"

D. Select the Process Timeline feature, enter the AID, Target Process ID, and Parent Process ID

Show Suggested Answer