



Vendor: CrowdStrike

Exam Code: CCFR-201b

Exam Name: CrowdStrike Certified Falcon Responder

Version: DEMO

QUESTION 1

What are Event Actions?

- A. Automated searches that can be used to pivot between related events and searches
- B. Pivable 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:

Event workflows are automated searches that can be used to pivot between related events and searches. To use a workflow, click the Event Actions button at the bottom of the JSON for any raw event

QUESTION 2

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

Answer: B

QUESTION 3

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

Answer: A

QUESTION 4

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

Answer: D

QUESTION 5

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'

Answer: D

QUESTION 6

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

Answer: A

Explanation:

Domain search under Investigate only gives your Domain Lookup Summary and Processes that looked up specified Domains.

QUESTION 7

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

Answer: A

QUESTION 8

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

Answer: C

QUESTION 9

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

Answer: B

QUESTION 10

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

Answer: D

Explanation:

ContextProcessId of DnsRequest event is equal to the TargetProcessId of the event that spawned the DnsRequest event.

QUESTION 11

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

Answer: D

Thank You for Trying Our Product

Passleader Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.passleader.com/all-products.html>



Microsoft



ORACLE



JUNIPER
NETWORKS



EMC²
where information lives

10% Discount Coupon Code: ASTR14