



CCFA-200^{Q&As}

CrowdStrike Certified Falcon Administrator





Pass CrowdStrike CCFA-200 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.passapply.com/ccfa-200.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CrowdStrike
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

Which of the following prevention policy settings monitors contents of scripts and shells for execution of malicious content on compatible operating systems?

- A. Script-based Execution Monitoring
- B. FileSystem Visibility
- C. Engine (Full Visibility)
- D. Suspicious Scripts and Commands

Correct Answer: A

The prevention policy setting that monitors contents of scripts and shells for execution of malicious content on compatible operating systems is Script-based Execution Monitoring. Script-based Execution Monitoring is a feature that enables the Falcon sensor to monitor and prevent malicious script execution on Windows systems. The feature uses machine learning and behavioral analysis to detect suspicious scripts or commands executed by various script interpreters, such as PowerShell, WScript, CScript, or Bash. You can enable or disable Script-based Execution Monitoring in the Prevention Policy for Windows hosts¹. References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 2

What is the maximum number of patterns that can be added when creating a new exclusion?

- A. 10
- B. 0
- C. 1
- D. 5

Correct Answer: C

The maximum number of patterns that can be added when creating a new exclusion is one. Each exclusion can only have one pattern, which can be a file path, a hash, a command line or a user name. The other options are either incorrect or not related to creating exclusions. Reference: CrowdStrike Falcon User Guide, page 37.

QUESTION 3

How does the Unique Hosts Connecting to Countries Map help an administrator?

- A. It highlights countries with known malware
- B. It helps visualize global network communication
- C. It identifies connections containing threats



D. It displays intrusions from foreign countries

Correct Answer: B

The Unique Hosts Connecting to Countries Map helps an administrator to visualize global network communication. The map shows the number of unique hosts in your environment that have established network connections to different countries in the past 24 hours. You can use this map to identify unusual or suspicious network activity, such as connections to high-risk countries or regions, or connections from hosts that are not expected to communicate with external entities². References: 2: Cybersecurity Resources | CrowdStrike

QUESTION 4

Which Real Time Response role will allow you to see all analyst session details?

- A. Real Time Response - Read-Only Analyst
- B. None of the Real Time Response roles allows this
- C. Real Time Response -Active Responder
- D. Real Time Response -Administrator

Correct Answer: D

The Real Time Response role that will allow you to see all analyst session details is Real Time Response -Administrator. A Real Time Response -Administrator is a role that has full access and control over the Real Time Response feature in Falcon, which allows you to remotely access and investigate hosts in real time. A Real Time Response - Administrator can view all analyst session details, such as session ID, host name, start and end time, commands executed, and output received. A Real Time Response -Administrator can also create, modify, delete, and assign scripts and commands to other analysts². References: 2: Cybersecurity Resources | CrowdStrike

QUESTION 5

A Falcon Administrator is trying to use Real-Time Response to start a session with a host that has a sensor installed but they are unable to connect. What is the most likely cause?

- A. The host has a user logged into it
- B. The domain controller is preventing the connection
- C. They do not have an RTR role assigned to them
- D. There is another analyst connected into it

Correct Answer: C

The most likely cause for not being able to use Real-Time Response to start a session with a host that has a sensor installed is that they do not have an RTR role assigned to them. An RTR (Real Time Response) role is a role that grants

access and permissions to use the Real Time Response feature in Falcon, which allows you to remotely access and investigate hosts in real time. There are three types of RTR roles:



Real Time Response -Read-Only Analyst, Real Time Response -Active Responder, and Real Time Response -Administrator. You need to have at least one of these roles assigned to you in order to use Real Time Response2.

References: 2: Cybersecurity Resources | CrowdStrike

[CCFA-200 PDF Dumps](#)

[CCFA-200 VCE Dumps](#)

[CCFA-200 Braindumps](#)