CrowdStrike CCFA-200b Fragen und Antworten, CrowdStrike Falcon Administrator Prüfungsfragen

Außerdem sind jetzt einige Teile dieser Pass4Test CCFA-200b Prüfungsfragen kostenlos erhältlich: https://drive.google.com/open?id=1qqmNy3Obu6lx6xYzuS933XrXA2OxMT-_

Einige Websites bieten auch die neuesten Lernmaterialien zur CrowdStrike CCFA-200b Prüfung im Internet. Aber sie haben keine zuverlässigen Garatie. Ich würde hier sagen, dass Pass4Test einen Grundwert hat. Alle CrowdStrike-Prüfungen sind sehr wichtig. Im Zeitalter der rasanten entwickelten Informationstechnologie ist Pass4Test nur eine von den vielen. Warum wählen die meisten Menschen Pass4Test? Dies liegt darin, die von Pass4Test gebotenen Prüfungsfragen und Antworten wird Sie sicherlich in die Lage bringen, das Exam zu bestehen. wieso? Weil es die neuerlich aktualisierten Materialien bietet. Diese haben die Mehrheit der Kandidaten schon bewiesen.

Die Schulungsunterlagen zur CrowdStrike CCFA-200b Prüfung von Pass4Test sind eine Sammlung der Erfahrungen von denjenigen, die im IT-Bereich schon zertifiziert sind und ein Ergebnis der Innovation. Unsere Berufsgruppe von IT-Eliten bietet den breiten Kandidaten ständig die neuesten Schulungsunterlagen zur CrowdStrike CCFA-200b Zertifizierungsprüfung, deren Korrektheit zweifellos ist. Unser Ziel liegt darin, dass die Kandidaten in kürzester Zeit die CrowdStrike CCFA-200b Ziertifizierungsprüfung beim ersten Versuch bestehen können.

>> CCFA-200b Deutsch <<

CCFA-200b Fragenpool & CCFA-200b Exam Fragen

Durch CrowdStrike CCFA-200b Zertifizierungsprüfung wird sich viel Wandel bei Ihnen vollziehen. Beispielsweise werden Ihr Beruf und Leben sicher viel verbessert, weil die CrowdStrike CCFA-200b Zertifizierungsprüfung sowieso eine ziemlich wichtige Prüfung ist. Aber so einfach ist es nicht, diese Prüfung zu bestehen.

CrowdStrike CCFA-200b Prüfungsplan:

Thema	Einzelheiten
Thema 1	• Rules Configuration: This domain involves creating custom IOA rules, configuring exclusions to resolve false positives, managing IOC settings for threat detection, and configuring CID-wide General Settings.
Thema 2	• Policy Application: This domain encompasses configuring prevention policies for security posture, sensor update policies, RTR audit policies, containment policies with IP exclusions, and managing quarantined files.
Thema 3	• Group Creation: This domain covers assigning endpoints to appropriate groups for policy application and following best practices for managing host group structures.

Thema 4	• Host Management and Setup: This domain addresses filtering and organizing hosts, disabling detections and understanding their effects, managing Reduced Functionality Mode situations, locating inactive sensors and their retention, and utilizing relevant management reports.
Thema 5	• Dashboards and Reports: This domain covers understanding different sensor report types and their use cases, and interpreting various audit logs for tracking platform activities.

CrowdStrike Falcon Administrator CCFA-200b Prüfungsfragen mit Lösungen (Q223-Q228):

223. Frage
To enhance your security, you want to detect and block based on a list of domains and IP addresses. How can you use IOC management to help this objective?

- A. Using IOC management, import the list of hashes and IP addresses and set the action to Detect Only
- B. Using IOC management, import the list of hashes and IP addresses and set the action to Prevent/Block
- C. Blocking of Domains and IP addresses is not a function of IOC management. A Custom IOA Rule should be used instead
- D. Using IOC management, import the list of hashes and IP addresses and set the action to No Action

Antwort: C

Begründung:
IOC management only allows "Detect only" and "No Action" among the possible actions.
Therefore, it cannot be used to block based on IPs or domains. Custom IOA Rule groups allow to create rule types based on Network Connection (configuring a remote IP address) and domains, and gives the options to "Monitor", "Detect" and "Kill Process", being the late one the closest to
"block".

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

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

Antwort: B

Begründung:
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 analysts.

225. Frage
Which of the following would give you information about inactive sensors within the Falcon console?

- A. Sensor Update Policies
- B. Sensor Coverage Lookup
- C. Sensor Downloads
- D. Sensor Health

Antwort: D

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

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

Antwort: C

Begründung:
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 hosts.

227. Frage
An administrator creating an exclusion is limited to applying a rule to how many groups of hosts?

- A. There is a limit of three groups of hosts applied to any exclusion
- B. Each exclusion can be aligned to only one group of hosts
- C. File exclusions are not aligned to groups or hosts
- D. There is no limit and exclusions can be applied to any or all groups

Antwort: D

Begründung:
An exclusion is a rule that tells the Falcon platform to ignore certain files, folders, processes, or registry keys when performing prevention or detection actions. An administrator can create an exclusion and apply it to one or more groups of hosts, or to all hosts in the organization. For example, an administrator can create an exclusion for a legitimate application that is causing false positives and apply it to the group of hosts that are running that application.

228. Frage
.....

⇛ www.zertpruefung.ch ⇚ nach 《 CCFA-200b 》 und laden Sie es kostenlos herunter □CCFA-200b PDF Demo

- CCFA-200b PDF □ CCFA-200b Zertifizierungsfragen ▶ CCFA-200b PDF □ Suchen Sie auf （ www.itzert.com ） nach ⇛ CCFA-200b ⇚ und erhalten Sie den kostenlosen Download mühelos □CCFA-200b Unterlage
- CCFA-200b Dumps und Test Überprüfungen sind die beste Wahl für Ihre CrowdStrike CCFA-200b Testvorbereitung □ Öffnen Sie die Webseite 《 www.zertpruefung.de 》 und suchen Sie nach kostenloser Download von ➽ CCFA-200b □ □CCFA-200b Kostenlos Downloden
- Kostenlos CCFA-200b dumps torrent - CrowdStrike CCFA-200b Prüfung prep - CCFA-200b examcollection braindumps □ Suchen Sie einfach auf 《 www.itzert.com 》 nach kostenloser Download von ☀ CCFA-200b □☀□ □CCFA-200b Prüfung
- CCFA-200b Unterlage □ CCFA-200b Kostenlos Downloden □ CCFA-200b Exam □ Öffnen Sie die Webseite ➡ www.pruefungfrage.de □□□ und suchen Sie nach kostenloser Download von ☀ CCFA-200b □☀□ □CCFA-200b Kostenlos Downloden
- www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, learn.eggdemy.com, daotao.wisebusiness.edu.vn, myportal.utt.edu.tt, Disposable vapes

P.S. Kostenlose und neue CCFA-200b Prüfungsfragen sind auf Google Drive freigegeben von Pass4Test verfügbar: https://drive.google.com/open?id=1qqmNy3Obu6lx6xYzuS933XrXA2OxMT-_