CCFA-200b최신덤프문제모음집 & CCFA-200b유효한 인증시험덤프

그리고 KoreaDumps CCFA-200b 시험 문제집의 전체 버전을 클라우드 저장소에서 다운로드할 수 있습니다: https://drive.google.com/open?id=1WreRHaYLXtbnJGJidFGuJ7iR4vz_cUg0

CrowdStrike CCFA-200b인증시험이 이토록 인기가 많으니 우리KoreaDumps에서는 모든 힘을 다하여 여러분이 응시에 도움을 드리겠으며 또 일년무료 업뎃서비스를 제공하며, KoreaDumps 선택으로 여러분은 자신의 꿈과 더 가까워질 수 있습니다. 희망찬 내일을 위하여 KoreaDumps선택은 정답입니다. KoreaDumps선택함으로 당신이 바로 진정한 IT인사입니다.

CrowdStrike CCFA-200b 시험요강:

주제	소개
주제 1	• Sensor Deployment: This domain focuses on verifying installation prerequisites, applying default policies and best practices, uninstalling sensors, and troubleshooting sensor issues across supported operating systems.
주제 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.
주제 3	• 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.
주제 4	• Dashboards and Reports: This domain covers understanding different sensor report types and their use cases, and interpreting various audit logs for tracking platform activities.

>> CCFA-200b최신 덤프문제모음집 <<

시험대비 CCFA-200b최신 덤프문제모음집 최신버전 덤프데모 문제

KoreaDumps에는 전문적인 업계인사들이CrowdStrike CCFA-200b시험문제와 답에 대하여 연구하여, 시험준비중인 여러분들한테 유용하고 필요한 시험가이드를 제공합니다. 만약KoreaDumps의 제품을 구매하려면, 우리 KoreaDumps에서는 아주 디테일 한 설명과 최신버전 최고품질의자료를 즉적중율이 높은 문제와 답을제공합니다.CrowdStrike CCFA-200b자료는 충분한 시험대비자료가 될 것입니다. 안심하시고 KoreaDumps가 제공하는 상품을 사용하시고, 100%통과 율을 확신합니다.

최신 CrowdStrike Certified Falcon Administrator CCFA-200b 무료샘플문

제 (Q80-Q85):

질문 # 80
What information can be found in the Real Time Response (RTR) Audit Log?

- A. IP Address, Prevention Policy, recent detections, and host group assignment
- B. Real Time Response (RTR) information is not collected via audit logs
- C. Session end time, command return results, and file activity
- D. Session start time, duration, user, hostname, commands used, and retrieved files

정답：D

질문 # 81
When creating a Host Group for all Workstations in an environment, what is the best method to ensure all workstation hosts are added to the group?

- A. Create a Dynamic Group and Import All Workstations
- B. Create a Static Group and Import all Workstations
- C. Create a Dynamic Group with Type=Workstation Assignment
- D. Create a Static Group with Type=Workstation Assignment

정답：C

설명:
The best method to ensure all workstation hosts are added to the group is to create a Dynamic Group with Type=Workstation Assignment. A Dynamic Group is a group that automatically updates its membership based on certain criteria or filters. A Type=Workstation Assignment filter will match all hosts that have the workstation type assigned in their Active Directory domain. This way, any new or existing workstation hosts will be added to the group without manual intervention.

질문 # 82
Which of the following is an effective Custom IOA rule pattern to kill any process attempting to access www.badguydomain.com?

- A. Custom IOA rules cannot be created for domains
- B. \Device\HarddiskVolume2*.exe -SingleArgument www.badguydomain.com /kill
- C. badguydomain\.com.*
- D. .*badguydomain.com.*

정답：D

설명:
You are usuing RegEx here and need leading ".*" to capture www and then need a ".*" at the end to identify any sites falling under badguydomain.com.

질문 # 83
What information does the API Audit Trail Report provide?

- A. A list of actions taken via Falcon OAuth2-based APIs
- B. A list of newly added hosts
- C. A list of specific changes to prevention policy
- D. A list of analyst login activity

정답：A

설명:
The information that the API Audit Trail Report provides is a list of actions taken via Falcon OAuth2-based APIs. The API Audit Trail Report allows you to view and audit the activity and usage of the Falcon APIs by different API clients and users in your organization. You can use this report to monitor who accessed what data, when, and how via the Falcon APIs.

질문 # 84
What is the purpose of a containment policy?

- A. To define which Falcon analysts can contain endpoints
- B. To define allowed IP addresses over which your hosts will communicate when contained
- C. To define the trigger under which a machine is put in Network Containment (e.g. a critical detection)
- D. To define the duration of Network Containment

정답：B

설명:
In the Containment Policy page have the title "Network traffic allowlist" and it only allows to add IPs or CIDR networks to exclude in the moment of the isolation of any host, because it is a global policy, not allowing make distinctions between machines.

질문 # 85
.....

참고: KoreaDumps에서 Google Drive로 공유하는 무료 2026 CrowdStrike CCFA-200b 시험 문제집이 있습니다: https://drive.google.com/open?id=1WreRHaYLXtbnJGJidFGuJ7iR4vz_cUg0