Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

CCFA-200 Dumps
CCFA-200 Braindumps
CCFA-200 Real Questions
CCFA-200 Practice Test
CCFA-200 Actual Questions

PASS

CrowdStrike

CCFA-200

CrowdStrike Certified Falcon Administrator (CCFA)

Question: 40

Even though you are a Falcon Administrator, you discover you are unable to use the "Connect to Host" feature to gather additional information which is only available on the host.

Which role do you need added to your user account to have this capability?

A. Real Time Responder
B. Endpoint Manager
C. Falcon Investigator
D. Remediation Manager

Answer: A

Question: 41

Which port and protocol does the sensor use to communicate with the CrowdStrike Cloud?

A. TCP port 22 (SSH)
B. TCP port 443 (HTTPS)
C. TCP port 80 (HTTP)
D. TCP UDP port 53 (DNS)

Answer: B

Question: 42

What type of information is found in the Linux Sensors Dashboard?

A. Hosts by Kernel Version, Shells spawned by Root, Wget/Curl Usage
B. Hidden File execution, Execution of file from the trash, Versions Running with ComputerNames
C. Versions running, Directory Made Invisible to Spotlight, Logging/Auditing Referenced, Viewed, or Modified
D. Private Information Accessed, Archiving Tools C Exfil, Files Made Executable

Answer: A

Question: 43

How long are detection events kept in Falcon?

A. Detection events are kept for 90 days
B. Detections events are kept for your subscribed data retention period
C. Detection events are kept for 7 days
D. Detection events are kept for 30 days

Answer: B

Question: 44

What can the Quarantine Manager role do?

A. Manage and change prevention settings
B. Manage quarantined files to release and download
C. Manage detection settings
D. Manage roles and users

Answer: B

Question: 45

How do you find a list of inactive sensors?

A. The Falcon platform does not provide reporting for inactive sensors
B. A sensor is always considered active until removed by an Administrator
C. Run the Inactive Sensor Report in the Host setup and management option
D. Run the Sensor Aging Report within the Investigate option

Answer: C

Question: 46

The Falcon sensor uses certificate pinning to defend against man-in-the-middle attacks.

Which statement is TRUE concerning Falcon sensor certificate validation?

A. SSL inspection should be configured to occur on all Falcon traffic
B. Some network configurations, such as deep packet inspection, interfere with certificate validation
C. HTTPS interception should be enabled to proceed with certificate validation
D. Common sources of interference with certificate pinning include protocol race conditions and resource contention

Answer: B

Question: 47

You have an existing workflow that is triggered on a critical detection that sends an email to the escalation team. Your CISO has asked to also be notified via email with a customized message.

What is the best way to update the workflow?

A. Clone the workflow and replace the existing email with your CISO's email
B. Add a sequential action to send a custom email to your CISO
C. Add a parallel action to send a custom email to your CISO
D. Add the CISO's email to the existing action

Answer: C

Question: 48

You have been provided with a list of 100 hashes that are not malicious but your company has deemed to be inappropriate for work computers. They have asked you to ensure that they are not allowed to run in your environment. You have chosen to use Falcon to do this.

Which is the best way to accomplish this?

A. Using the Support Portal, create a support ticket and include the list of binary hashes, asking support to create an "Execution Prevention" rule to prevent these processes from running
B. Using Custom Alerts in the Investigate App, create a new alert using the template"Process Execution" and within that rule, select the option to "Block Execution"
C. Using IOC Management, gather the list of SHA256 or MD5 hashes for each binary and then upload them. Set all hashes to "Block" and ensure that the prevention policy these computers are using includes the option for "Custom Blocking" under Execution Blocking.
D. Using the API, gather the list of SHA256 or MD5 hashes for each binary and then upload them, setting them all to "Never Allow"

Answer: C

Question: 49

Which is a filter within the Host setup and management > Host management page?

A. User name
B. OU
C. BIOS Version
D. Locality

Answer: B

Question: 50

How do you assign a Prevention policy to one or more hosts?

A. Create a new policy and assign it directly to those hosts on the Host Management page
B. Modify the users roles on the User Management page
C. Ensure the hosts are in a group and assign that group to a custom Prevention policy
D. Create a new policy and assign it directly to those hosts on the Prevention policy page

Answer: C

Question: 51

Where do you obtain the Windows sensor installer for CrowdStrike Falcon?

A. Sensors are downloaded from the Hosts > Sensor Downloads
B. Sensor installers are unique to each customer and must be obtained from support
C. Sensor installers are downloaded from the Support section of the CrowdStrike website
D. Sensor installers are not used because sensors are deployed from within Falcon

Answer: A

Question: 52

Which of the following applies to Custom Blocking Prevention Policy settings?

A. Hashes must be entered on the Prevention Hashes page before they can be blocked via this policy
B. Blocklisting applies to hashes, IP addresses, and domains

C. Executions blocked via hash blocklist may have partially executed prior to hash calculation process remediation may be necessary
D. You can only blocklist hashes via the API

Answer: C

Question: 53

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

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

Answer: C

Question: 54

Why is it critical to have separate sensor update policies for Windows/Mac/*nix?

A. There may be special considerations for each OS
B. To assist with testing and tracking sensor rollouts
C. The network protocols are different for each host OS
D. It is an auditing requirement

Answer: A

Question: 55

What information is provided in Logan Activities under Visibility Reports?

A. A list of all logons for all users
B. A list of last endpoints that a user logged in to
C. A list of users who are remotely logged on to devices based on local IP and local port
D. A list of unique users who are remotely logged on to devices based on the country

Answer: B

SAMPLE QUESTIONS

These questions are for demo purpose only. ***Full version*** *is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

Actual Exam Questions*: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

Exam Dumps*: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

Practice Tests*: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

Guaranteed Success*: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

Updated Content: *Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

Technical Support*: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*