Latest Test CrowdStrike IDP Discount - Reliable IDP Exam Questions

What's more, part of that Actual4dump IDP dumps now are free: https://drive.google.com/open?id=1M_tNxuBG7tM9NEUYNRIAVuz2cF_BCqwR

If you want to start your learning as quickly as possible, just choose us, we can do this for you. Our IDP study materials is famous for instant download, and you can get the downloading link and password within ten minutes after purchasing, if you don't receive, you can ask our service stuff for help. Besides, IDP Exam Dumps of us contain both questions and answers, and you can check the answer when you finish practicing. IDP study materials are also have certain questions and it will help you to pass the exam successfully.

CrowdStrike IDP Exam Syllabus Topics:

Topic	Details
Topic 1	• Falcon Fusion SOAR for Identity Protection: Explores SOAR workflow automation including triggers, conditions, actions, creating custom • templated • scheduled workflows, branching logic, and loops.
Topic 2	• Risk Management with Policy Rules: Covers creating and managing policy rules and groups, triggers, conditions, enabling • disabling rules, applying changes, and required Falcon roles.
Topic 3	• Configuration and Connectors: Addresses domain controller monitoring, subnet management, risk settings, MFA and IDaaS connectors, authentication traffic inspection, and country-based lists.
Topic 4	• Domain Security Assessment: Focuses on domain risk scores, trends, matrices, severity • likelihood • consequence factors, risk prioritization, score reduction, and configuring security goals and scopes.

Topic 5	• GraphQL API: Covers Identity API documentation, creating API keys, permission levels, pivoting from Threat Hunter to GraphQL, and building queries.
Topic 6	• Threat Hunting and Investigation: Focuses on identity-based detections and incidents, investigation pivots, incident trees, detection evolution, filtering, managing exclusions and exceptions, and risk types.

Reliable IDP Exam Questions - IDP Reliable Test Sample

Students are worried about whether the IDP practice materials they have purchased can help them pass the exam and obtain a certificate. They often encounter situations in which the materials do not match the contents of the exam that make them waste a lot of time and effort. But with IDP exam dump, you do not need to worry about similar problems. Because our study material is prepared strictly according to the exam outline by industry experts, whose purpose is to help students pass the exam smoothly. As the authoritative provider of IDP Test Guide, we always pursue high passing rates compared with our peers to gain more attention from potential customers.

CrowdStrike Certified Identity Specialist(CCIS) Exam Sample Questions (Q58-Q63):

NEW QUESTION # 58
Which of the following actions willNOThelp to decrease a domain risk score?

- A. Enabling SMB Signing within Active Directory
- B. Upgrading endpoints running end-of-life operating systems
- C. Enforcing NTLMv2 responses
- D. Upgrading endpoints running end-of-life Acrobat Reader

Answer: D

Explanation:
Falcon Identity Protection evaluatesdomain riskby analyzing identity-related weaknesses such as insecure authentication protocols, legacy directory configurations, and exposure to credential-based attacks. Actions that harden Active Directory and authentication mechanisms will directly reduce domain risk scores.
Measures such asenabling SMB signing,enforcing NTLMv2, andupgrading unsupported operating systemsremove common identity attack paths and are explicitly recommended in the CCIS curriculum as effective domain risk remediation steps.
In contrast,upgrading end-of-life Acrobat Readeraddresses anendpoint application vulnerability, not an identity or directory-related risk. While important for endpoint hygiene, it does not influence identity telemetry, authentication behavior, or domain controller security assessed by Falcon Identity Protection.
Because domain risk scoring is strictly tied to identity infrastructure and authentication posture,Option Bdoes not contribute to lowering the domain risk score and is therefore the correct answer.

NEW QUESTION # 59
When an endpoint that has not been used in the last90 daysbecomes active, a detection forUse of Stale Endpointis reported.

- A. 30 days
- B. 60 days
- C. 90 days
- D. 180 days

Answer: C

Explanation:
Falcon Identity Protection identifiesstale endpointsas systems that have not authenticated or shown activity for an extended period and then suddenly become active. According to the CCIS curriculum, an endpoint that has been inactive for90 daysand then resumes activity will trigger aUse of Stale Endpointdetection.

This detection is important because attackers frequently exploit dormant or forgotten systems to re-enter environments, evade monitoring, or move laterally. A long period of inactivity followed by sudden authentication activity is considered a strong identity risk signal.
The 90-day threshold is used to establish a reliable inactivity baseline while minimizing false positives.
Shorter timeframes could incorrectly flag normal usage patterns, while longer timeframes could delay detection of genuine threats.
Because Falcon explicitly defines stale endpoint activity using a90-day inactivity window,Option Bis the correct answer.

NEW QUESTION # 60
How should a user be classified if one requires observation for potential risk to the business?

- A. Honeytoken Account
- B. High Risk
- C. Marked User
- D. Watched User

Answer: D

Explanation:
Within Falcon Identity Protection, aWatched Useris a user explicitly designated forheightened monitoring due to potential business risk. According to the CCIS curriculum, watchlists are designed to provide additional visibility into users whose behavior, access level, or role may warrant closer observation, even if they have not yet exhibited confirmed malicious activity.
Watched Users may include executives, administrators, users with access to sensitive systems, or accounts suspected of being targeted. Placing a user on a watchlist does not imply compromise; instead, it ensures their activity is prioritized in investigations, detections, and dashboards.
The other options are incorrect:
* Honeytoken Accountsare decoy accounts designed to detect malicious usage.
* High Riskis a calculated risk state, not a monitoring classification.
* Marked Useris not a valid Falcon Identity Protection classification.
Because the CCIS material explicitly identifiesWatched Usersas accounts requiring observation for potential risk,Option Cis the correct and verified answer.

NEW QUESTION # 61
Falcon Identity Protection monitors network traffic to build user behavioral profiles to help identify unusual user behavior. How can this be beneficial to create a Falcon Fusion workflow?

- A. Falcon Fusion will only send emails to the user
- B. Falcon Fusion will only work with certain users
- C. Falcon Fusion works with your IT policy enforcement through the use of identity and behavioral analytics
- D. Falcon Fusion is not identity based

Answer: C

Explanation:
Falcon Identity Protection continuously inspects authentication traffic and network behavior to establish behavioral baselines for users and accounts. These baselines enable the platform to detect deviations that indicate potential compromise, misuse, or insider threat activity. This behavioral intelligence directly enhances the effectiveness ofFalcon Fusion workflows.
Falcon Fusion leveragesidentity and behavioral analyticsas decision points within workflows, allowing automated actions to be triggered when abnormal behavior is detected. For example, a workflow can automatically enforce MFA, notify administrators, isolate risky sessions, or initiate remediation when a user deviates from their established baseline.
The CCIS curriculum highlights that Falcon Fusion is designed tointegrate identity risk signals with IT policy enforcement, enabling Zero Trust-aligned automation. This capability goes far beyond simple notifications and supports coordinated responses across security and IT teams.
Options A, B, and C are incorrect because Falcon Fusion is fully identity-aware, applies broadly across users and entities, and supports a wide range of actions beyond email notifications. Therefore,Option Daccurately describes how behavioral profiling strengthens Falcon Fusion workflows.

NEW QUESTION # 62

What trigger will cause a Falcon Fusion Workflow to activate from Falcon Identity Protection?

- A. Spotlight user action > Host
- B. New endpoint detection
- C. Alert > Identity detection
- D. New incident

Answer: C

Explanation:
Falcon Fusion workflows integrate directly with Falcon Identity Protection throughidentity-based triggers, allowing automated responses to identity threats. The correct trigger that activates a Falcon Fusion workflow from Identity Protection isAlert > Identity detection.
Identity detections are generated when Falcon observes suspicious or malicious identity behavior, such as credential abuse, abnormal authentication patterns, lateral movement attempts, or policy violations related to identity risk. These detections are distinct from endpoint-only detections or incidents and are specifically designed to representidentity-based attack activity.
WhileNew incidentandNew endpoint detectionare valid Falcon Fusion triggers in other Falcon modules, they are not the primary triggers for identity-focused automation. Similarly,Spotlight user action > Host relates to vulnerability management workflows rather than identity analytics.
The CCIS curriculum emphasizes that Falcon Fusion enablesautomated identity response, such as notifying security teams, disabling accounts, enforcing MFA, or triggering SOAR actions, based onidentity detections.
Therefore, workflows tied toAlert > Identity detectionallow organizations to respond quickly and consistently to identity threats, makingOption Cthe correct answer.

NEW QUESTION # 63
.....

hhi.instructure.com, bbs.t-firefly.com, 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, vietnamfranchise.vn, bbs.t-firefly.com, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free 2026 CrowdStrike IDP dumps are available on Google Drive shared by Actual4dump: https://drive.google.com/open?id=1M_tNxuBG7tM9NEUYNRIAVuz2cF_BCqwR