Dumps IDP Torrent - IDP Actual Questions

In order to meet a wide range of tastes, our company has developed the three versions of the IDP preparation questions, which includes PDF version, online test engine and windows software. According to your own budget and choice, you can choose the most suitable one for you. And if you don't know which one to buy, you can free download the demos of the IDP Study Materials to check it out. The demos of the IDP exam questions are a small part of the real exam questions.

Our IDP exam questions have a very high hit rate, of course, will have a very high pass rate. Before you select a product, you must have made a comparison of your own pass rates. Our IDP study materials must appear at the top of your list. And our IDP learning quiz has a 99% pass rate. This is the result of our efforts and the best gift to the user. Our IDP Study Materials can have such a high pass rate, and it is the result of step by step that all members uphold the concept of customer first. If you use a trial version of IDP training prep, you will want to buy it!

>> Dumps IDP Torrent <<

IDP Actual Questions | Exam IDP Material

When candidates decide to pass the IDP exam, the first thing that comes to mind is to look for a study material to prepare for their exam. The most people will consider that choose IDP question torrent, because it has now provided thousands of online test papers for the majority of test takers to perform simulation exercises, helped tens of thousands of candidates pass the IDP Exam, and got their own dream industry certificates. That is to say, there is absolutely no mistake in choosing our IDP test guide to prepare your exam, you will pass your exam in first try and achieve your dream soon.

CrowdStrike IDP Exam Syllabus Topics:

Topic	Details
Topic 1	• GraphQL API: Covers Identity API documentation, creating API keys, permission levels, pivoting from Threat Hunter to GraphQL, and building queries.
Topic 2	• Risk Assessment: Covers entity risk categorization, risk and event analysis dashboards, filtering, user risk reduction, custom insights versus reports, and export scheduling.

Topic 3	• Falcon Identity Protection Fundamentals: Introduces the four menu categories (monitor, enforce, explore, configure), subscription differences between ITD and ITP, user roles, permissions, and threat mitigation capabilities.
Topic 4	• User Assessment: Examines user attributes, differences between users • endpoints • entities, risk baselining, risky account types, elevated privileges, watchlists, and honeytoken accounts.
Topic 5	• Identity Protection Tenets: Examines Falcon Identity Protection's architecture, domain traffic inspection, EDR complementation, human vulnerability protection, log-free detections, and identity-based attack mitigation.
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.

CrowdStrike Certified Identity Specialist(CCIS) Exam Sample Questions (Q20-Q25):

NEW QUESTION # 20
Which of the following best describes how Policy Group and Policy Rule precedence works?

- A. Policy Groups are evaluated in the order in which the groups appear on the page. The Policy Rules within those groups are evaluated in the order in which they appear in the group
- B. Policy Groups only group Policy Rules together. Precedence is dictated by the Rules
- C. There is no precedence with Policy Groups or Policy Rules; they enact policy if the conditions match
- D. Policy Groups are evaluated in the order in which the groups appear on the page; however, Policy Rules within those groups have no precedence

Answer: A

Explanation:
Falcon Identity Protection enforces deterministic policy execution using a clear and predictable precedence model. As outlined in the CCIS curriculum, Policy Groups are evaluated top to bottom, based on their order in the console. Within each Policy Group, Policy Rules are evaluated sequentially, also from top to bottom.
This ordered evaluation ensures consistent enforcement behavior and allows administrators to design layered identity controls. When a rule's conditions are met and an action is executed, subsequent rules may or may not be evaluated depending on rule logic and configuration. This model gives administrators precise control over enforcement priority.
The incorrect options misunderstand how precedence works. Policy enforcement is not unordered, nor are Policy Groups merely visual containers. Both grouping and rule order matter.
This precedence model is critical for avoiding conflicting enforcement actions and aligns with Zero Trust principles by ensuring predictable, auditable identity enforcement. Therefore, Option A is the correct answer.

NEW QUESTION # 21
How should a user be classified if one requires observation for potential risk to the business?

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

Answer: B

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 # 22
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 works with your IT policy enforcement through the use of identity and behavioral analytics
- B. Falcon Fusion will only work with certain users
- C. Falcon Fusion will only send emails to the user
- D. Falcon Fusion is not identity based

Answer: A

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 # 23
Falcon Identity Protection can continuously assess identity events and associate them with potential threats WITHOUTwhich of the following?

- A. Ingesting logs
- B. The need for string-based queries
- C. Machine-learning-powered detection rules
- D. API-based connectors

Answer: B

Explanation:
Falcon Identity Protection is architected as alog-free identity security platform, a core tenet emphasized throughout the CCIS curriculum. Unlike traditional SIEM- or log-based solutions, Falcon Identity Protection doesnot require string-based queriesto continuously assess identity events or associate them with threats.
Instead, the platform relies onmachine-learning-powered detection rules,real-time authentication traffic inspection, andAPI-based connectorsto collect and analyze identity telemetry directly from domain controllers and identity providers. This approach eliminates the operational complexity of building, tuning, and maintaining query logic.
String-based queries are commonly associated with legacy log aggregation tools and SIEM platforms, where analysts must manually search logs to identify suspicious behavior. Falcon Identity Protection replaces this model withbehavioral baselining and automated correlation, enabling continuous identity risk assessment without human-driven query execution.
Because Falcon does not require string-based queries to operate,Option Dis the correct and verified answer.

NEW QUESTION # 24
The events are excluded by default while Low, Medium, and High detections are visible.

- A. Informational
- B. Internal
- C. Inferior
- D. Indiscrete

Answer: A

Explanation:
In Falcon Identity Protection,Informationaldetections represent low-impact events that provide context but do not indicate elevated identity risk. According to the CCIS curriculum,Informational events are excluded by defaultfrom standard detection views to reduce noise and allow analysts to focus on higher-risk activity.
By default,Low, Medium, and High severity detections remain visible, as these contribute directly to identity risk scoring, incident formation, and investigative workflows. Informational detections can still be viewed if filters are adjusted, but they are intentionally hidden in default views.
This design supports efficient threat triage by prioritizing detections that are more likely to represent real security concerns. The other options listed are not valid detection severity classifications within Falcon Identity Protection.
Because Informational events are excluded by default while higher-severity detections remain visible,Option Ais the correct and verified answer.

NEW QUESTION # 25
.....

There may be a lot of people feel that the preparation process for exams is hard and boring, and hard work does not necessarily mean good results, which is an important reason why many people are afraid of examinations. Today, our IDP study materials will radically change this. High question hit rate makes you no longer aimless when preparing for the exam, so you just should review according to the content of our IDP Study Materials prepared for you. Instant answer feedback allows you to identify your vulnerabilities in a timely manner, so as to make up for your weaknesses.