Quiz 2026 CrowdStrike High Hit-Rate New IDP Learning Materials

BTW, DOWNLOAD part of ActualTestsQuiz IDP dumps from Cloud Storage: https://drive.google.com/open?id=1ZO3yiwEgo0tqTtedHMKrVPJdsP5ss2Dz

When looking for a job, of course, a lot of companies what the personnel managers will ask applicants that have you get the IDP certification to prove their abilities, therefore, we need to use other ways to testify our knowledge we get when we study at college , such as get the IDP Test Prep to obtained the qualification certificate to show their own all aspects of the comprehensive abilities, and the IDP exam guide can help you in a very short period of time to prove yourself perfectly and efficiently.

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	• 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 4	• Zero Trust Architecture: Covers NIST SP 800-207 framework, Zero Trust principles, Falcon's implementation, differences from traditional security models, use cases, and Zero Trust Assessment score calculation.
Topic 5	• 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 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.
Topic 7	• User Assessment: Examines user attributes, differences between users • endpoints • entities, risk baselining, risky account types, elevated privileges, watchlists, and honeytoken accounts.

>> New IDP Learning Materials <<

CrowdStrike IDP Latest Exam Tips, IDP Valid Exam Vce Free

If you don't have enough time to study for your certification exam, ActualTestsQuiz provides CrowdStrike IDP Pdf questions. You may quickly download CrowdStrike IDP exam questions in PDF format on your smartphone, tablet, or desktop. You can Print CrowdStrike IDP PDF Questions and answers on paper and make them portable so you can study on your own time and carry them wherever you go.

CrowdStrike Certified Identity Specialist(CCIS) Exam Sample Questions (Q29-Q34):

NEW QUESTION # 29
Which option can be selected from the Threat Hunter menu to open the current Threat Hunter query in a new window as Graph API format?

- A. Open Query in API Builder
- B. Export to API Builder
- C. Save as Custom Query
- D. Save as Custom Report

Answer: A

Explanation:
Falcon Threat Hunter provides a direct integration with theAPI Builderto support advanced investigation workflows and automation. According to the CCIS curriculum, analysts can take an existing Threat Hunter query and convert it into aGraphQL-compatible formatby selectingOpen Query in API Builderfrom the Threat Hunter menu.
This option opens the current query in a new window within API Builder, automatically translating the query structure into GraphQL syntax where applicable. This enables security teams to reuse validated hunting logic for automation, reporting, or external integrations without rewriting queries from scratch.
The other menu options serve different purposes:
* Export to API Builderis not a valid menu action.
* Save as Custom Querystores the query for reuse inside Threat Hunter.
* Save as Custom Reportgenerates a reporting artifact, not an API query.
BecauseOpen Query in API Builderis the only option that opens the query in GraphQL format in a new window,Option Dis the correct and verified answer.

NEW QUESTION # 30
Within Domain Security Overview, whatGoalincorporates all risks into one security assessment report?

- A. Pen Testing
- B. Privileged User Management
- C. AD Hygiene
- D. Reduce Attack Surface

Answer: D

Explanation:
Within the Domain Security Overview,Goalsare used to tailor how identity risks are grouped, evaluated, and reported. TheReduce Attack Surfacegoal is the only option thatincorporates all identity risks into a single, comprehensive security assessment.
The CCIS curriculum explains that Reduce Attack Surface provides a holistic view of identity exposure by aggregating risks related to authentication paths, account hygiene, privileges, misconfigurations, and legacy identity weaknesses. This goal is designed for organizations seeking an overall understanding of their identity security posture rather than focusing on a specific domain such as privileged users or directory hygiene.
Other goals are more specialized:
* AD Hygienefocuses on directory configuration issues.
* Privileged User Managementconcentrates on high-privilege identities.
* Pen Testingaligns more with adversarial simulation than continuous risk assessment.

Reduce Attack Surface aligns directly withZero Trust principles, helping organizations identify and eliminate unnecessary identity access paths. Therefore,Option Cis the correct and verified answer.

NEW QUESTION # 31
Which entity tab will show an administrator how to lower the account's risk score?

- A. Risk
- B. Timeline
- C. Asset
- D. Activity

Answer: A

Explanation:
In CrowdStrike Falcon Identity Protection, theRisktab within a user or account entity provides administrators with direct visibility intowhy an account has a specific risk score and what actions can be taken to reduce that score. This functionality is a core component of theUser AssessmentandRisk Assessmentsections of the CCIS (CrowdStrike Identity Specialist) curriculum.
The Risk tab aggregates bothanalysis-based risksanddetection-based risks, clearly identifying contributing factors such as compromised passwords, excessive privileges, risky authentication behavior, stale or never- used accounts, and policy violations. It also highlights theseverity, likelihood, and consequenceof each risk factor, allowingadministrators to prioritize remediation efforts effectively. Most importantly, this tab provides actionable guidance, enabling teams to understand which specific remediation steps-such as enforcing MFA, resetting credentials, reducing privileges, or disabling unused accounts-will directly lower the account's overall risk score.
Other entity tabs do not provide this capability. TheTimelinetab focuses on chronological events and detections, theActivitytab displays authentication and behavioral activity, and theAssettab shows associated endpoints and resources. Only theRisktab is designed to explain risk drivers and guide remediation, making Option Dthe correct and verified answer.

NEW QUESTION # 32
How many days will an identity-based incident be suppressed if new events related to the same incident occur?

- A. 14 days
- B. 30 days
- C. 7 days
- D. 5 days

Answer: D

Explanation:
Falcon Identity Protection usesincident suppression windowsto prevent alert fatigue while still maintaining accurate incident tracking. According to the CCIS documentation, whennew events related to an existing identity-based incident occur, the incident issuppressed for 5 days.
This suppression means that Falcon does not generate a new incident for the same activity during this window. Instead, additional detections areadded to the existing incident, allowing analysts to view the full progression of the threat in a single investigative context.
The 5-day suppression window ensures that ongoing identity attacks-such as repeated authentication abuse or lateral movement-are consolidated rather than fragmented across multiple incidents. This improves investigation efficiency and aligns with Falcon's incident lifecycle management approach.
Because the suppression period is fixed at5 days,Option Dis the correct and verified answer.

NEW QUESTION # 33
Which of the following actions under the Investigate menu will pivot to Falcon Identity Protection from an identity-based detection?

- A. Search for involved entities in Threat Hunter
- B. Investigate involved users
- C. Search for events in Threat Hunter
- D. Investigate involved endpoints

Answer: A

Explanation:
Falcon Identity Protection integrates directly withThreat Hunterto enable deeper investigation of identity- based activity. According to the CCIS curriculum, selectingSearch for involved entities in Threat Hunter allows analysts to pivot from an identity-based detection into Threat Hunter while preserving identity context.
This pivot enables analysts to examine related users, service accounts, endpoints, and authentication behavior using advanced queries and timelines. Importantly, this action maintains the identity-centric investigation flow, bridging detections with broader hunting capabilities.
The other options do not perform this specific pivot:
* Investigating users or endpoints remains within entity views.
* Searching for events in Threat Hunter does not preserve entity context.
BecauseSearch for involved entities in Threat Hunteris the correct pivot action,Option Bis the verified answer.

NEW QUESTION # 34
.....

If you want to get satisfying result in CrowdStrike IDP practice test, our online training materials will be the best way to success, which apply to any level of candidates. We guarantee the best deal considering the quality and price of IDP Braindumps Pdf that you won't find any better available. Our learning materials also contain detailed explanations expert for correct IDP test answers.