Providing You the Best Accurate IDP PDF Cram Exam with 100% Passing Guarantee

Customers first are our mission, and we will try our best to help all of you to get your IDP certification. We offer you the best valid and latest CrowdStrike IDP study practice, thus you will save your time and study with clear direction. Besides, we provide you with best safety shopping experience. The Paypal system will guard your personal information and keep it secret. In addition, the high pass rate will ensure you pass your IDP Certification with high score.

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	• 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 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	• Configuration and Connectors: Addresses domain controller monitoring, subnet management, risk settings, MFA and IDaaS connectors, authentication traffic inspection, and country-based lists.
Topic 5	• Risk Assessment: Covers entity risk categorization, risk and event analysis dashboards, filtering, user risk reduction, custom insights versus reports, and export scheduling.
Topic 6	• GraphQL API: Covers Identity API documentation, creating API keys, permission levels, pivoting from Threat Hunter to GraphQL, and building queries.
Topic 7	• User Assessment: Examines user attributes, differences between users • endpoints • entities, risk baselining, risky account types, elevated privileges, watchlists, and honeytoken accounts.
Topic 8	• 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 9	• Multifactor Authentication (MFA) and Identity-as-a-service (IDaaS) Configuration Basics: Focuses on accessing and configuring MFA and IDaaS connectors, configuration fields, and enabling third-party MFA integration.

>> IDP PDF Cram Exam <<

100% Pass Quiz 2026 The Best IDP: CrowdStrike Certified Identity Specialist(CCIS) Exam PDF Cram Exam

To pass the certification exam, you need to select right IDP study guide and grasp the overall knowledge points of the real exam. The test questions from our IDP dumps collection cover almost content of the exam requirement and the real exam. Trying to download the free demo in our website and check the accuracy of IDP Test Answers and questions. Getting certification will be easy for you with our materials.

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. Enforcing NTLMv2 responses
- C. Upgrading endpoints running end-of-life Acrobat Reader
- D. Upgrading endpoints running end-of-life operating systems

Answer: C

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
How should an organization address the domain risk score found in the Domain Security Overview page?

- A. Prioritizing the detections by severity, addressing the High (Red) detections first
- B. Prioritizing the risks by severity, addressing the Low (Green) risks first
- C. Prioritizing the risks by severity, addressing the Medium (Yellow) risks first
- D. Address the risks on the list from top to bottom as risks are presented in a descending order

Answer: D

Explanation:
TheDomain Security Overviewpage in Falcon Identity Protection presents domain risks in aprioritized, descending order, based on a combination ofseverity, likelihood, and consequence. The CCIS curriculum emphasizes that organizations should address risksfrom top to bottom, as the list is already optimized to reflect the most impactful identity risks first.
This ordering allows security teams to focus remediation efforts where they will produce the greatest reduction in overall domain risk score. Addressing risks sequentially ensures alignment with Falcon's risk modeling and avoids misprioritization that could occur if teams focus only on color-based severity or individual detections.

The incorrect options reflect common misconceptions:
* Medium risks should not be prioritized over higher-impact risks.
* Detections are different from risks and should not be addressed independently of risk context.
* Low risks are intentionally deprioritized by the platform.
By following the descending order provided in the Domain Security Overview, organizations align remediation with Falcon'sZero Trust-driven identity risk scoring methodology, makingOption Athe correct answer.

NEW QUESTION # 60
The events are excluded by default while Low, Medium, and High detections are visible.

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

Answer: C

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 # 61
When creating an API client, which scope withWritepermissions must be enabled prior to using Identity Protection API?

- A. Identity Protection Assessment
- B. Identity Protection GraphQL
- C. There is no need for Write permissions in order to use IDP API
- D. Identity Protection Health

Answer: B

Explanation:
To interact with Falcon Identity Protection using GraphQL, the API client must be created with the appropriate permission scopes. According to the CCIS curriculum, theIdentity Protection GraphQLscope withWrite permissionsmust be enabled prior to using the Identity Protection API.
This scope allows the API client to execute GraphQL queries and mutations related to identity detections, incidents, users, and risk data. Even when performing read-only operations, CrowdStrike requires the GraphQL Write scope to authorize GraphQL query execution within the Falcon platform.
The other options are incorrect because:
* Identity Protection Assessment and Health are read-only data scopes.
* The statement that Write permissions are not required is explicitly false per CCIS documentation.
Because GraphQL access requires theIdentity Protection GraphQL (Write)scope,Option Dis the correct and verified answer.

NEW QUESTION # 62
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. Save as Custom Report

- C. Save as Custom Query
- D. Export to API Builder

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 # 63
.....