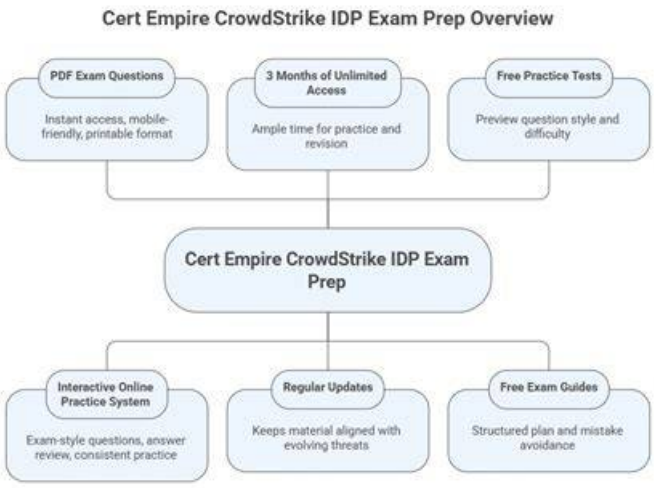
Features Of Web-based CrowdStrike IDP Practice Exam



P.S. Free 2026 CrowdStrike IDP dumps are available on Google Drive shared by Getcertkey: https://drive.google.com/open?id=1GOcI6eJByiKoJ2kTIzCAVCY9z1QBVtoA

Getcertkey provides proprietary preparation guides for the certification exam offered by the IDP exam dumps. In addition to containing numerous questions similar to the IDP Exam, the CrowdStrike Certified Identity Specialist(CCIS) Exam (IDP) exam questions are a great way to prepare for the CrowdStrike IDP exam dumps.

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 Assessment: Covers entity risk categorization, risk and event analysis dashboards, filtering, user risk reduction, custom insights versus reports, and export scheduling.
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	• 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 5	• GraphQL API: Covers Identity API documentation, creating API keys, permission levels, pivoting from Threat Hunter to GraphQL, and building queries.
Topic 6	• 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 7	• 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.

Topic 8	• User Assessment: Examines user attributes, differences between users • endpoints • entities, risk baselining, risky account types, elevated privileges, watchlists, and honeytoken accounts.
Topic 9	• Configuration and Connectors: Addresses domain controller monitoring, subnet management, risk settings, MFA and IDaaS connectors, authentication traffic inspection, and country-based lists.
Topic 10	• Risk Management with Policy Rules: Covers creating and managing policy rules and groups, triggers, conditions, enabling • disabling rules, applying changes, and required Falcon roles.

CrowdStrike Certified Identity Specialist(CCIS) Exam Sample Questions (Q48-Q53):

NEW QUESTION # 48
Which of the following isNOTa default insight but can be created with a custom insight?

- A. Using Unmanaged Endpoints
- B. Poorly Protected Accounts with SPN
- C. Compromised Password
- D. GPO Exposed Password

Answer: B

Explanation:
In Falcon Identity Protection,default insightsare prebuilt analytical views provided by CrowdStrike to immediately highlight common and high-impact identity risks across the environment. These default insights are automatically available in theRisk AnalysisandInsightsareas and are designed to surface well-known identity exposure patterns without requiring customization. Examples ofdefault insightsincludeUsing Unmanaged Endpoints,GPO Exposed Password, and Compromised Password. These insights are natively provided because they represent frequent and high-risk identity attack vectors such as credential exposure, unmanaged authentication sources, and password compromise, all of which directly contribute to elevated identity risk scores.
Poorly Protected Accounts with SPN (Service Principal Name), however, isnot provided as a default insight. While Falcon Identity Protection does collect and analyze SPN-related risk signals-such as Kerberoasting exposure and weak service account protections-this specific grouping must be created by administrators usingcustom insight filters. Custom insights allow teams to define precise conditions, combine attributes (privilege level, SPN presence, password age, MFA status), and tailor risk visibility to their organization's threat model.
This distinction is emphasized in the CCIS curriculum, which explains thatcustom insights extend beyond default coverage, enabling deeper, organization-specific identity risk analysis. Therefore,Option Dis the correct answer.

NEW QUESTION # 49
An account without a phone number, operating system, or role of CEO would typically be defined as:

- A. Human
- B. Programmatic

- C. Enterprise
- D. Corporate

Answer: B

Explanation:
Falcon Identity Protection classifies accounts based onobserved authentication behavior and associated identity attributes, not solely on naming conventions. According to the CCIS curriculum,programmatic accounts(such as service accounts or application accounts) typically lack human-centric attributes like a phone number, assigned operating system, job title, or executive role (for example, CEO).
Human accounts generally have enriched identity context sourced from directory services and identity providers, including user profile details, interactive login behavior, and endpoint associations. In contrast, programmatic accounts authenticate non-interactively, often on predictable schedules, and do not require personal attributes to function.
Falcon analyzes authentication traffic to automatically identify these characteristics and classify the account accordingly. An account missing human identity signals-such as a phone number or endpoint ownership- strongly aligns with programmatic behavior.
Because the absence of personal attributes and interactive context is a defining indicator of aprogrammatic account,Option Ais the correct and verified answer.

NEW QUESTION # 50
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 are evaluated in the order in which the groups appear on the page; however, Policy Rules within those groups have no precedence
- C. Policy Groups only group Policy Rules together. Precedence is dictated by the Rules
- D. There is no precedence with Policy Groups or Policy Rules; they enact policy if the conditions match

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 # 51
What is the recommended action for the"Guest Account Enabled"risk?

- A. Disable the endpoint in Active Directory
- B. Disable Guest accounts on all endpoints
- C. Add related endpoints to a watchlist
- D. Apply a policy rule with an "Access" trigger and "Block" action on the Guest account

Answer: B

Explanation:
In Falcon Identity Protection, the"Guest Account Enabled"risk highlights the presence of local or domain guest accounts that remain active across endpoints. Guest accounts are inherently high-risk because they typically lack strong authentication controls, are rarely monitored, and are frequently abused by attackers for lateral movement and persistence.
The CCIS curriculum explicitly recommendsdisabling Guest accounts on all endpointsas the primary remediation action. This is because guest accounts often bypass standard identity governance processes and violate the principles ofleast privilegeandZero Trust, both of which are foundational to Falcon Identity Protection's security model. Disabling these accounts removes an

unnecessary and dangerous authentication path from the environment.
Other options are incorrect because:
* Adding endpoints to a watchlist does not remediate the risk.
* Blocking access via a policy rule is less effective than eliminating the account entirely.
* Disabling endpoints in Active Directory does not directly address the guest account exposure.
Falcon Identity Protection prioritizeselimination of weak identity configurations, and disabling guest accounts is a direct, effective action that immediately lowers identity risk scores and reduces attack surface.
Therefore,Option Cis the correct and verified answer.

NEW QUESTION # 52
Which CrowdStrike documentation category would you search to find GraphQL examples?

- A. XDR
- B. Threat Intelligence
- C. Identity Protection APIs
- D. CrowdStrike APIs

Answer: D

Explanation:
GraphQL is the underlying query technology used by multiple CrowdStrike platforms, including Falcon Identity Protection.
According to the CCIS curriculum,GraphQL examples are documented under the broader "CrowdStrike APIs" documentation category, not limited to a single product.
The CrowdStrike APIs section includes:
* Authentication and API key usage
* GraphQL schema references
* Example GraphQL queries and mutations
* Pagination, filtering, and response handling
While Identity Protection uses GraphQL for identity-specific queries, the examples themselves are centralized underCrowdStrike APIsto provide consistency across Falcon modules. Product-specific use cases are then layered on top of these core examples.
The other options are incorrect:
* Threat Intelligence focuses on adversary data.
* XDR covers detection and correlation concepts.
* Identity Protection APIs describe endpoints and permissions, not general GraphQL usage examples.
Therefore,Option Ais the correct and verified answer.

NEW QUESTION # 53
.....

and obtain a free download □IDP Latest Test Cost

- IDP Desktop and Practice Test Software By www.prepawaypdf.com □ Search on ☀ www.prepawaypdf.com □☀□ for ➥ IDP □ to obtain exam materials for free download □IDP Valid Vce
- IDP Valid Exam Dumps □ IDP Valid Vce □ IDP Latest Test Cost □ Download （ IDP ） for free by simply searching on ➤ www.pdfvce.com □ □IDP Test Voucher
- Latest IDP Test Preparation □ Exam IDP Material □ IDP Real Exam □ Search for （ IDP ） and download it for free immediately on ▷ www.prepawaypdf.com ◁ □Exam IDP Pattern
- Exam IDP Pattern □ Flexible IDP Learning Mode □ IDP Valid Vce □ Open “ www.pdfvce.com ” and search for 【 IDP 】 to download exam materials for free □IDP Latest Dumps Free
- Flexible IDP Learning Mode □ IDP Practice Exam Pdf □ IDP Latest Test Format □ Open 「 www.pdfdumps.com 」 and search for ➠ IDP □ to download exam materials for free □IDP Latest Dumps Free
- notefolio.net, www.slideshare.net, hanson.net, learn.csisafety.com.au, jobs.electronicsweekly.com, 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, myportal.utt.edu.tt, telegra.ph, wibki.com, notefolio.net, ronorp.net, Disposable vapes

DOWNLOAD the newest Getcertkey IDP PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1GOcI6eJByiKoJ2kTIzCAVCY9z1QBVtoA