IDP Valid Test Guide & IDP Testdump

As the talent competition increases in the labor market, it has become an accepted fact that the IDP certification has become an essential part for a lot of people, especial these people who are looking for a good job, because the certification can help more and more people receive the renewed attention from the leaders of many big companies. So it is very important for a lot of people to gain the IDP Certification. We must pay more attention to the certification and try our best to gain the IDP certification.

CrowdStrike IDP Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• Configuration and Connectors: Addresses domain controller monitoring, subnet management, risk settings, MFA and IDaaS connectors, authentication traffic inspection, and country-based lists.
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	• Risk Assessment: Covers entity risk categorization, risk and event analysis dashboards, filtering, user risk reduction, custom insights versus reports, and export scheduling.
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	• Falcon Fusion SOAR for Identity Protection: Explores SOAR workflow automation including triggers, conditions, actions, creating custom • templated • scheduled workflows, branching logic, and loops.
Topic 7	• 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 8	• 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.

Pass Guaranteed 2026 IDP: CrowdStrike Certified Identity Specialist(CCIS) Exam –The Best Valid Test Guide

The latest CrowdStrike Certified Identity Specialist(CCIS) Exam IDP exam and exam study guide is reliable, CrowdStrike Certified Identity Specialist(CCIS) Exam IDP with reasonable exam price and guaranteed questions answers. CrowdStrike offers actual CrowdStrike Certified Identity Specialist(CCIS) Exam to sure your success in IDP Exam. Don't worry, this CrowdStrike Certified Identity Specialist(CCIS) Exam IDP test price is benefit and content is 365 days updates!

CrowdStrike Certified Identity Specialist(CCIS) Exam Sample Questions (Q55-Q60):

NEW QUESTION # 55
Which entity tab will show an administrator how to lower the account's risk score?

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

Answer: C

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 # 56
Which of the following isNOTan available Goal within the Domain Security Overview?

- A. Pen Testing
- B. Privileged Users Management
- C. AD Hygiene
- D. Business Privileged Users Management

Answer: D

Explanation:
The Domain Security Overview in Falcon Identity Protection usesGoalsto frame identity risks into focused security assessment perspectives. These goals allow organizations to evaluate identity posture based on specific security priorities such as directory hygiene, privilege exposure, or overall attack surface reduction.
According to the CCIS curriculum, theavailable GoalsincludePrivileged Users Management,AD Hygiene, Pen Testing, andReduce Attack Surface. These goals are predefined by CrowdStrike and determine how risks are grouped, weighted, and presented in reports.
Business Privileged Users Managementisnot an available Goalwithin the Domain Security Overview.
While Falcon Identity Protection does support the concept ofbusiness privilegesand evaluates their impact on users and entities, this concept is handled through risk analysis and configuration-not as a selectable Domain Security Goal.
The CCIS documentation clearly distinguishes betweenGoals(which control reporting and assessment views) andbusiness privilege

modeling(which influences risk scoring). Therefore,Option Bis the correct and verified answer.

NEW QUESTION # 57

The CISO of your organization recently read a report about the increased usage of identity brokers and is interested in finding a solution for the company. Which of the following makes Falcon Identity a valid solution for the organization?

- A. Gives the organization the ability to proactively mitigate risks, as well as protect critical Active Directory infrastructure through Policy Rules
- B. Provides the ability to audit and record sessions across multiple methods, such as SSH, RDP, and SMB
- C. Falcon Identity is able to be a middleware between Active Directory and a Human Resource Information System (HRIS)
- D. Allows administrators to store and delegate passwords to application servers

Answer: A

Explanation:

Falcon Identity Protection is designed to address the growing threat ofidentity brokers, which act as intermediaries that abuse identity infrastructure to facilitate lateral movement, privilege escalation, and persistent access. The CCIS curriculum emphasizes that Falcon Identity Protection providesproactive identity risk mitigationrather than reactive session monitoring or password vaulting. The platform continuously inspects authentication traffic and identity behavior across Active Directory and Azure AD environments, building behavioral baselines and identifying abnormal activity associated with brokered identity attacks. ThroughPolicy Rules, organizations can automatically enforce controls such as blocking risky authentications, enforcing MFA, or triggering remediation workflows when identity abuse is detected.

The incorrect options describe capabilities associated withPrivileged Access Management (PAM)orIAM middleware, which are not the focus of Falcon Identity Protection. Falcon does not record interactive sessions, act as an HRIS bridge, or store delegated credentials. Instead, it protects identity infrastructure by detecting and preventing identity misuse in real time.

This proactive enforcement model aligns directly with Zero Trust principles and makes Falcon Identity Protection a strong solution against identity broker activity. Therefore,Option Cis the correct and verified answer.

NEW QUESTION # 58

In the Predefined ReportsSubjectdropdown, which category is associated with endpoints?

- A. Insights
- B. Incidents
- C. Accounts
- D. Events

Answer: D

Explanation:

Within Falcon Identity Protection,Predefined Reportsallow administrators to generate standardized reports based on specific data subjects. TheSubject dropdowndetermines the type of data the report will be built from, such as identity risks, authentication activity, or endpoint-related telemetry.

The category associated withendpointsin the Subject dropdown isEvents. Endpoint-related data-such as authentication attempts, logons, protocol usage, and domain controller-observed activity-is captured and represented aseventswithin Falcon. These events form the foundational telemetry used for identity detections, investigations, and reporting.

By contrast:

* Insightsrepresent aggregated analytical findings derived from events.
* Incidentsgroup multiple detections into a single investigative narrative.
* Accountsfocus on identity entities such as users and service accounts.

Endpoint visibility in reporting is therefore tied directly toEvents, as events reflect the raw and enriched activity observed on endpoints and domain controllers. This structure aligns with Falcon's identity-first security model, where endpoint-observed authentication behavior feeds identity risk scoring and Zero Trust decisions.

The CCIS curriculum explicitly associatesendpoint-related reportingwith theEventssubject, makingOption Bthe correct and verified answer.

NEW QUESTION # 59

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

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

Answer: A

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 # 60
......

Our company aimed to provide you with professional team, high quality service and reasonable price on our IDP exam questions. In order to help most customers solve their problems, our company always insist on putting them first and providing valued service on our IDP training braindump. It has helped so many candidates passed their IDP exam. We deeply believe that the IDP test torrent of our company will help you pass the IDP exam and get your certification successfully in a short time too.

IDP Testdump: https://www.practicetorrent.com/IDP-practice-exam-torrent.html