IDP Valid Guide Files | Latest IDP Test Answers

One of the main unique qualities of ActualCollection CrowdStrike Certified Identity Specialist(CCIS) Exam Exam Questions is its ease of use. Our practice exam simulators are user and beginner friendly. You can use CrowdStrike Certified Identity Specialist(CCIS) Exam (IDP) PDF dumps and Web-based software without installation. CrowdStrike IDP PDF Questions work on all the devices like smartphones, Macs, tablets, Windows, etc. We know that it is hard to stay and study for the CrowdStrike Certified Identity Specialist(CCIS) Exam (IDP) exam dumps in one place for a long time.

CrowdStrike IDP Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• GraphQL API: Covers Identity API documentation, creating API keys, permission levels, pivoting from Threat Hunter to GraphQL, and building queries.
Topic 3	• 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 4	• Falcon Fusion SOAR for Identity Protection: Explores SOAR workflow automation including triggers, conditions, actions, creating custom • templated • scheduled workflows, branching logic, and loops.
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	• 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.

>> IDP Valid Guide Files <<

Advantages Of These CrowdStrike IDP Exam Questions Formats

This cost-effective exam product is made as per the current content of the CrowdStrike IDP examination. Therefore, using ActualCollection the actual CrowdStrike IDP dumps will guarantee your successful attempt at the IDP Certification Exam. For the

convenience of customers, we have designed IDP pdf dumps, desktop CrowdStrike IDP practice exam software, and CrowdStrike IDP web-based practice test.

CrowdStrike Certified Identity Specialist(CCIS) Exam Sample Questions (Q21-Q26):

NEW QUESTION # 21
Within the Falcon Identity Protection portal, which page allows you to enable/disable Policy Rules?

- A. Enforce
- B. Identity-Based Detections
- C. Configure
- D. Policy Enforcement

Answer: A

Explanation:
In Falcon Identity Protection, Policy Rules are managed within the Enforce section of the portal. The CCIS documentation explains that Enforce is the operational area where administrators create, enable, disable, and manage Policy Rules and Policy Groups.
This section is specifically designed for identity enforcement logic, allowing security teams to activate or suspend rules without modifying underlying configurations or analytics. Enabling or disabling a Policy Rule immediately affects how identity conditions are enforced across the environment.
Other sections serve different purposes:
Configure manages connectors, domains, subnets, and risk settings.
Identity-Based Detections is used for investigation and monitoring.
Policy Enforcement is not a standalone navigation section in Falcon Identity Protection.
Because rule activation and enforcement control reside exclusively in Enforce, Option B is the correct and verified answer.

NEW QUESTION # 22
Which of the following Falcon rolesCANNOTenable and disable policy rules?

- A. Identity Protection Administrator
- B. Identity Protection Domain Administrator
- C. Identity Protection Policy Manager
- D. Falcon Administrator

Answer: B

Explanation:
Falcon Identity Protection enforcesrole-based access control (RBAC)to ensure that only authorized users can create, modify, or manage policy rules. Policy rules directly impact identity enforcement actions, making proper role separation critical.
According to the CCIS documentation, the ability toenable and disable policy rulesis granted to theIdentity Protection Policy Managerand theFalcon Administratorroles. These roles are explicitly designed to manage enforcement logic, triggers, and automated identity controls.
TheIdentity Protection Domain Administratorrole, however, is limited todomain-level visibility and management, such as reviewing domain configurations, monitoring risks, and assessing posture. This role doesnothave permissions to modify or control policy enforcement behavior.
This separation prevents accidental or unauthorized changes to identity enforcement rules. Therefore,Option Ais the correct and verified answer.

NEW QUESTION # 23
Which menu option isNOTincluded in Falcon Identity Threat Detection (ITD)?

- A. Privileged Identities
- B. Settings
- C. Event Analysis
- D. Policy Rules

Answer: D

Explanation:
Falcon Identity Threat Detection (ITD) providesvisibility, analytics, and detectionof identity-based threats but doesnot include enforcement capabilities. According to the CCIS curriculum, ITD customers have access to investigative and analytical features such asEvent Analysis,Privileged Identities, and relevant Settingsfor visibility and monitoring.
Policy Rules, however, are part ofIdentity Threat Protection (ITP)and reside in theEnforcesection of the Falcon console. Policy Rules enable automated responses and enforcement actions, such as blocking access or enforcing MFA, which are not available under ITD-only subscriptions.
This distinction is critical in the CCIS material:
* ITD = Detect and analyze identity threats
* ITP = Detect + enforce policy actions
Because ITD does not include enforcement functionality,Policy Rules are not available, makingOption Dthe correct answer.

NEW QUESTION # 24
What does a modern Zero Trust security architecture offer compared to a traditional wall-and-moat (perimeter- based firewall) approach?

- A. Secures the perimeter of a network and does not allow access to any entities deemed "zero trust"
- B. Applies machine learning to gauge the trustworthiness of any external entities
- C. Continuously authenticates entities regardless of origin
- D. Issues trust certificates to internal entities and zero trust certificates to external entities

Answer: C

Explanation:
A modern Zero Trust security architecture fundamentally differs from the traditional wall-and-moat model by eliminating implicit trust based on network location. As defined inNIST SP 800-207and reinforced in the CCIS curriculum, Zero Trust requirescontinuous authentication and authorization of all entities, regardless of whether they originate from inside or outside the network.
Traditional perimeter-based security assumes that users and devices inside the network are trusted, focusing defenses at the boundary. This approach fails in modern environments where cloud access, remote work, and compromised credentials allow attackers to operate internally without triggering perimeter controls.
Zero Trust replaces this assumption with continuous validation using identity, behavior, device posture, and risk signals. Falcon Identity Protection operationalizes this concept by continuously inspecting authentication traffic and reassessing trust throughout a session, not just at login time.
Because Zero Trust applies universally and continuously,Option Dis the correct and verified answer.

NEW QUESTION # 25
For false positives, the Detection details can be set to new"Actions"using:

- A. recommendations
- B. remediations
- C. exceptions
- D. exits

Answer: C

Explanation:
When an identity-based detection is determined to be afalse positive, Falcon Identity Protection allows administrators to take corrective action usingexceptions. According to the CCIS curriculum, exceptions are the mechanism by which detections can be suppressed for specific entities or conditions without disabling the detection entirely.
Exceptions are configured from theDetection detailsview and are intended to handle known, acceptable behavior that would otherwise continue to trigger detections. This allows security teams to reduce noise while maintaining visibility into true threats.
Exceptions are especially valuable in environments with complex authentication patterns or legacy configurations.
The other options are incorrect:
* Exitsare not a detection control mechanism.
* Remediationsrefer to corrective actions, not suppression logic.
* Recommendationsprovide guidance but do not change detection behavior.
By usingexceptions, Falcon ensures that false positives are handled in a controlled and auditable way, aligning with best practices outlined in the CCIS material. Therefore,Option Cis the correct answer.

NEW QUESTION # 26
......

You don't need to install any separate software or plugin to use it on your system to practice for your actual CrowdStrike Certified Identity Specialist(CCIS) Exam (IDP) exam. CrowdStrike web-based practice software is supported by all well-known browsers like Chrome, Firefox, Opera, Internet Explorer, etc.

Latest IDP Test Answers: https://www.actualcollection.com/IDP-exam-questions.html