

New CrowdStrike IDP Exam Notes - IDP Test Book



We would like to benefit our customers from different countries who decide to choose our IDP study guide in the long run, so we cooperation with the leading experts in the field to renew and update our IDP study materials. We can assure you that you will get the latest version of our IDP Training Materials for free from our company in the whole year after payment. Do not miss the opportunity to buy the best IDP preparation questions in the international market which will also help you to advance with the times.

The CrowdStrike IDP certification exam is one of the top rated career advancement certification exams in the market. This CrowdStrike Certified Identity Specialist(CCIS) Exam (IDP) exam is designed to prove candidates' skills and knowledge levels. By doing this the CrowdStrike IDP certificate holders can gain multiple personal and professional benefits. These benefits assist the IDP Exam holder to pursue a rewarding career in the highly competitive market and achieve their career objectives in a short time period.

>> New CrowdStrike IDP Exam Notes <<

Quiz CrowdStrike IDP - CrowdStrike Certified Identity Specialist(CCIS) Exam Marvelous New Exam Notes

To keep with the fast-pace social life, we provide the fastest delivery services on our IDP exam questions. As most of the people tend to use express delivery to save time, our IDP preparation exam will be sent out within 5-10 minutes after purchasing. As long as you pay at our platform, we will deliver the relevant IDP Exam Materials to your mailbox within the given time. Our company attaches great importance to overall services, if there is any problem about the delivery of IDP exam materials, please let us know, a message or an email will be available.

CrowdStrike Certified Identity Specialist(CCIS) Exam Sample Questions (Q51-Q56):

NEW QUESTION # 51

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

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

- D. exits

Answer: B

Explanation:

When an identity-based detection is determined to be a false positive, Falcon Identity Protection allows administrators to take corrective action using exceptions. 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 the Detection details view 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:

- * Exits are not a detection control mechanism.
- * Remediations refer to corrective actions, not suppression logic.
- * Recommendations provide guidance but do not change detection behavior.

By using exceptions, Falcon ensures that false positives are handled in a controlled and auditable way, aligning with best practices outlined in the CCIS material. Therefore, Option C is the correct answer.

NEW QUESTION # 52

Which of the following Falcon roles CANNOT enable 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 enforces role-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 to enable and disable policy rules is granted to the Identity Protection Policy Manager and the Falcon Administrator roles. These roles are explicitly designed to manage enforcement logic, triggers, and automated identity controls.

The Identity Protection Domain Administrator role, however, is limited to domain-level visibility and management, such as reviewing domain configurations, monitoring risks, and assessing posture. This role does not have permissions to modify or control policy enforcement behavior.

This separation prevents accidental or unauthorized changes to identity enforcement rules. Therefore, Option A is the correct and verified answer.

NEW QUESTION # 53

When creating an API key, which scope should be selected to retrieve Identity Protection detection and incident information?

- A. Identity Protection Incidents
- B. Identity Protection Assessment
- C. Identity Protection Data
- **D. Identity Protection Detections**

Answer: D

Explanation:

To retrieve identity-based detections and incident-related data using the CrowdStrike APIs, the API key must include the correct permission scope. According to the CCIS curriculum, the Identity Protection Detections scope is required to access identity-based detection and incident information through GraphQL.

This scope allows API queries to retrieve:

- * Identity-based detections
- * Associated incident metadata
- * Detection attributes such as severity, status, and related entities

Incident data in Falcon Identity Protection is derived from detections, making the Detections scope the authoritative permission set

for this information. Without this scope, GraphQL queries related to identity detections and incidents will fail authorization. The other scopes are either too narrow or unrelated to detection retrieval. Therefore, Option A is the correct and verified answer.

NEW QUESTION # 54

What is the purpose behind creating Policy Rules?

- A. Policy Rules determine what actions an admin in the console can take before making adjustments
- **B. Policy Rules determine what actions to take in response to certain triggers/conditions observed within the environment**
- C. Policy Rules determine how the console tracks and learns behavior for users in the environment
- D. Policy Rules determine the scope in which the sensor collects information on the environment

Answer: B

Explanation:

Policy Rules in Falcon Identity Protection are designed to automate enforcement and response actions based on identity-related conditions observed in the environment. According to the CCIS curriculum, Policy Rules evaluate identity signals such as authentication behavior, risk levels, privilege status, and detection outcomes, then execute predefined actions when specific criteria are met.

These actions may include blocking authentication, enforcing MFA, generating alerts, or triggering Falcon Fusion workflows. This design supports Falcon's Zero Trust and continuous validation model, where trust decisions are dynamically enforced rather than statically assigned. Policy Rules therefore act as the operational bridge between identity analytics and enforcement.

The incorrect options confuse Policy Rules with other platform components. Administrative permissions are governed by RBAC, sensor data collection scope is controlled through configuration settings, and behavioral learning is handled by Falcon's analytics engine—not Policy Rules.

The CCIS documentation explicitly defines Policy Rules as logic-based enforcement mechanisms, making Option A the correct and verified answer.

NEW QUESTION # 55

What trigger will cause a Falcon Fusion Workflow to activate from Falcon Identity Protection?

- A. New incident
- B. Spotlight user action > Host
- C. New endpoint detection
- **D. Alert > Identity detection**

Answer: D

Explanation:

Falcon Fusion workflows integrate directly with Falcon Identity Protection through identity-based triggers, allowing automated responses to identity threats. The correct trigger that activates a Falcon Fusion workflow from Identity Protection is Alert > Identity detection.

Identity detections are generated when Falcon observes suspicious or malicious identity behavior, such as credential abuse, abnormal authentication patterns, lateral movement attempts, or policy violations related to identity risk. These detections are distinct from endpoint-only detections or incidents and are specifically designed to represent identity-based attack activity.

While New incident and New endpoint detection are valid Falcon Fusion triggers in other Falcon modules, they are not the primary triggers for identity-focused automation. Similarly, Spotlight user action > Host relates to vulnerability management workflows rather than identity analytics.

The CCIS curriculum emphasizes that Falcon Fusion enables automated identity response, such as notifying security teams, disabling accounts, enforcing MFA, or triggering SOAR actions, based on identity detections.

Therefore, workflows tied to Alert > Identity detection allow organizations to respond quickly and consistently to identity threats, making Option C the correct answer.

NEW QUESTION # 56

.....

VCETorrent offers authentic and actual IDP dumps that every candidate can rely on for good preparation. Our top priority is to give you the most reliable prep material that helps you pass the IDP Exam on the first attempt. In addition, we offer up to three months of

IDP Test Book: <https://www.vcetorrent.com/IDP-valid-vce-torrent.html>

When you create a raster image, you map out the placement and color of IDP Test Book each pixel, and the resulting bitmap is what you see on the screen, Basic Shapes—Triangles, circles, boxes, cylinders, hearts, and many more.

And we have engaged for more than ten years and successfully make every detail of our IDP Practice Braindumps to be perfect, You may know the exam fees are very expensive.

All the experts we have in our team are IDP experienced and professional in the CrowdStrike CCIS certification training industry.

- [illegible]