

Latest CrowdStrike IDP Test Pdf, New IDP Dumps



DOWNLOAD the newest Lead2Passed IDP PDF dumps from Cloud Storage for free: <https://drive.google.com/open?id=1rKeALGvGU4bcenSZ7fLFOGL-1tr8HzYK>

Full refund is available if you fail to pass the exam in your first attempt after buying IDP exam bootcamp from us, and we will refund your money. In addition, IDP exam dumps contain both questions and answers, and it's convenient for you to check the answers after practicing. IDP exam botcamp cover most of the knowledge points of the exam, and you can master the major knowledge points as well as improve your professional ability in the process of training. We have online and offline chat service for IDP Exam Dumps, and if you have any questions, you can consult us.

All the materials in IDP exam torrent can be learned online or offline. You can use your mobile phone, computer or print it out for review. With IDP practice test, if you are an office worker, you can study on commute to work, while waiting for customers, and for short breaks after work. If you are a student, IDP Quiz guide will also make your study time more flexible. With IDP exam torrent, you don't need to think about studying at the time of playing. You can study at any time you want to study and get the best learning results with the best learning status.

>> Latest CrowdStrike IDP Test Pdf <<

New IDP Dumps - IDP Exam Dump

After seeing you struggle, Lead2Passed has come up with an idea to provide you with the actual and updated CrowdStrike IDP practice questions so you can pass the IDP certification test on the first try and your hard work doesn't go to waste. Updated IDP Exam Dumps are essential to pass the CrowdStrike Certified Identity Specialist(CCIS) Exam (IDP) certification exam so you can advance your career in the technology industry and get a job in a good company that pays you well.

CrowdStrike Certified Identity Specialist(CCIS) Exam Sample Questions (Q31-Q36):

NEW QUESTION # 31

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

- A. New incident
- B. New endpoint detection
- C. Spotlight user action > Host
- **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 # 32

Which of the following is NOT an available Goal within the Domain Security Overview?

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

Answer: B

Explanation:

The Domain Security Overview in Falcon Identity Protection uses Goals to 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, the available Goals include Privileged Users Management, AD Hygiene, Pen Testing, and Reduce Attack Surface. These goals are predefined by CrowdStrike and determine how risks are grouped, weighted, and presented in reports.

Business Privileged Users Management is not an available Goal within the Domain Security Overview.

While Falcon Identity Protection does support the concept of business privileges and 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 between Goals (which control reporting and assessment views) and business privilege modeling (which influences risk scoring). Therefore, Option B is the correct and verified answer.

NEW QUESTION # 33

Which of the following is NOT a default insight but can be created with a custom insight?

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

Answer: D

Explanation:

In Falcon Identity Protection, default insights are 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 the Risk Analysis and Insights areas and are designed to surface well-known identity exposure patterns without requiring customization. Examples of default insights include Using 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, is not 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 using custom 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 that custom insights extend beyond default coverage, enabling deeper, organization-specific identity risk analysis. Therefore, Option D is the correct answer.

NEW QUESTION # 34

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

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

Answer: A

Explanation:

The Domain Security Overview page in Falcon Identity Protection presents domain risks in a prioritized, descending order, based on a combination of severity, likelihood, and consequence. The CCIS curriculum emphasizes that organizations should address risks from 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's Zero Trust-driven identity risk scoring methodology, making Option A the correct answer.

NEW QUESTION # 35

Which of the following demonstrates a detection is enabled?

- A. The detection has a Disabled tag next to it
- B. The detection has an Enabled tag next to it
- C. The toggle next to the Detection Enabled is marked in gray
- D. The toggle next to the Detection Enabled is marked in green

Answer: D

Explanation:

In Falcon Identity Protection, detection status is visually indicated using a toggle control within the detection configuration interface. According to the CCIS documentation, when a detection is enabled, the toggle next to Detection Enabled is displayed in green.

A green toggle indicates that the detection logic is active and that Falcon will generate detections when the defined conditions are met. When the toggle is gray, the detection is disabled and will not generate alerts or contribute to incident formation.

Falcon does not rely on textual "Enabled" or "Disabled" tags to indicate detection status. Instead, the toggle color provides a clear, immediate visual indicator to administrators.

Because a green toggle explicitly represents an enabled detection, Option B is the correct and verified answer.

NEW QUESTION # 36

.....

One of the biggest advantages of our IDP learning guide is that if you won't lose anything if you have a try with our IDP study materials. You can discover the quality of our exam dumps as well as the varied displays that can give the most convenience than you can ever experience. Both of the content and the displays are skillfully designed on the purpose that IDP Actual Exam can make your learning more targeted and efficient.

New IDP Dumps: <https://www.lead2passed.com/CrowdStrike/IDP-practice-exam-dumps.html>

But now you can set your mind at rest since with our App version of our IDP exam dump files, you can enjoy the simulation to your heart's content. Our CrowdStrike IDP exam torrent: CrowdStrike Certified Identity Specialist (CCIS) Exam can help you pass the exam and gain the CrowdStrike certificate. If you are worried about your IDP get freedumps review and have no much time to practice IDP vce dumps, you don't need to take any stress about it. CrowdStrike Latest IDP Test Pdf It is a good choice to take IT certification test which can not only help you master more skills, also can get the certificate to prove your ability.

As many of my friends passed the IDP exam only by studying the premium bundle, I also purchased it. The feedback collected was used to design our products through interviews with top CrowdStrike Certified Identity Specialist (CCIS) Exam IDP Exam professionals.

