Reliable IDP Test Questions | New IDP Study Guide

BTW, DOWNLOAD part of DumpsTorrent IDP dumps from Cloud Storage: https://drive.google.com/open?id=1eHssaGq3qH8GmVUcWfOaOmQSpYYpTVy4

Many people prefer to buy our IDP valid study guide materials because they deeply believe that if only they buy them can definitely pass the test. The reason why they like our IDP guide questions is that our study materials' quality is very high. For years we always devote ourselves to perfecting our IDP Study Materials. We boost the leading research team and the top-ranking sale service. We boost the expert team to specialize in the research and production of the IDP guide questions and professional personnel to be responsible for the update of the IDP study materials.

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

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.
Topic 9	- 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 10	- 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.

New IDP Study Guide - Valid IDP Torrent

A lot of IT people want to pass CrowdStrike certification IDP exams. Thus they can obtain a better promotion opportunity in the IT industry, which can make their wages and life level improved. But in order to pass CrowdStrike certification IDP exam many people spent a lot of time and energy to consolidate knowledge and didn't pass the exam. This is not cost-effective. If you choose DumpsTorrent's product, you can save a lot of time and energy to consolidate knowledge, but can easily pass CrowdStrike Certification IDP Exam. Because DumpsTorrent's specific training material about CrowdStrike certification IDP exam can help you 100% pass the exam. If you fail the exam, DumpsTorrent will give you a full refund.

CrowdStrike Certified Identity Specialist(CCIS) Exam Sample Questions (Q24-Q29):

NEW QUESTION # 24
Under which CrowdStrike documentation category could you find Identity Protection API information?

- A. CrowdStrike APIs
- B. CrowdStrike Store
- C. Falcon Management
- D. Tools and Reference

Answer: A

Explanation:
Identity Protection API documentation is part of CrowdStrike's centralized API documentation structure.
According to the CCIS curriculum,Identity Protection API information is located under the
"CrowdStrike APIs" documentation category.
This category includes:
* API authentication and scopes
* Identity Protection GraphQL schemas
* Query examples for detections, incidents, users, and risk
* Usage guidance and limitations
CrowdStrike consolidates all API-related documentation in one location to ensure consistent access and maintenance across Falcon modules. Identity Protection APIs are not documented under Falcon Management, Store, or general reference sections.
Because all product APIs-including Identity Protection-are documented underCrowdStrike APIs,Option Dis the correct and verified answer.

NEW QUESTION # 25
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. Issues trust certificates to internal entities and zero trust certificates to external entities
- C. Applies machine learning to gauge the trustworthiness of any external entities

- D. Continuously authenticates entities regardless of origin

Answer: D

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 # 26
Which of the following IDaaS connectors will allow Identity to ingest cloud activity along with applying SSO Policy?

- A. SAML
- B. Azure NPS
- C. Okta SSO
- D. ADFS

Answer: C

Explanation:
Falcon Identity Protection integrates withIdentity-as-a-Service (IDaaS)providers to ingest cloud authentication activity and enforce identity-based policies. According to the CCIS curriculum,Okta SSOis a supported IDaaS connector that enables Falcon to ingestcloud authentication eventswhile also applying Single Sign-On (SSO) policies.
Okta SSO provides rich identity telemetry, including login attempts, device context, and authentication outcomes. This data allows Falcon Identity Protection to correlate on-premises and cloud-based identity activity, extending identity risk analysis beyond Active Directory.
The other options are incorrect:
* ADFSis an on-premises federation service, not a cloud IDaaS.
* Azure NPSis used for RADIUS-based MFA, not SSO ingestion.
* SAMLis a protocol, not an IDaaS connector.
Because Okta SSO provides both cloud activity ingestion and SSO enforcement,Option Bis the correct and verified answer.

NEW QUESTION # 27
The NIST SP 800-207 framework for Zero Trust Architecture defines validation and authentication standards for users in which network locations?

- A. All users both inside and outside of the network
- B. Only those users outside the network
- C. Only those users inside the network
- D. Only those users accessing the network remotely over VPN

Answer: A

Explanation:
TheNIST SP 800-207 Zero Trust Architectureframework fundamentally rejects the concept of implicit trust based on network location. As outlined in both NIST guidance and reinforced in the CCIS curriculum,all users must be continuously validated and authenticated regardless of whether they are inside or outside the network perimeter.
Zero Trust assumes that threats can originate from anywhere, including internal networks. Therefore, authentication and authorization decisions must be made dynamically using identity, device posture, behavior, and risk signals-not network placement.
Falcon Identity Protection aligns directly with this principle by continuously evaluating identity behavior for all users, whether they authenticate from internal corporate networks, remote locations, or cloud environments.
Because Zero Trust applies universally,Option Cis the correct and verified answer.

NEW QUESTION # 28
When an endpoint that has not been used in the last90 daysbecomes active, a detection forUse of Stale Endpointis reported.

- A. 60 days
- B. 30 days
- C. 90 days
- D. 180 days

Answer: C

Explanation:
Falcon Identity Protection identifiesstale endpointsas systems that have not authenticated or shown activity for an extended period and then suddenly become active. According to the CCIS curriculum, an endpoint that has been inactive for90 daysand then resumes activity will trigger aUse of Stale Endpointdetection.
This detection is important because attackers frequently exploit dormant or forgotten systems to re-enter environments, evade monitoring, or move laterally. A long period of inactivity followed by sudden authentication activity is considered a strong identity risk signal.
The 90-day threshold is used to establish a reliable inactivity baseline while minimizing false positives.
Shorter timeframes could incorrectly flag normal usage patterns, while longer timeframes could delay detection of genuine threats.
Because Falcon explicitly defines stale endpoint activity using a90-day inactivity window,Option Bis the correct answer.

NEW QUESTION # 29
......

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, 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, Disposable vapes