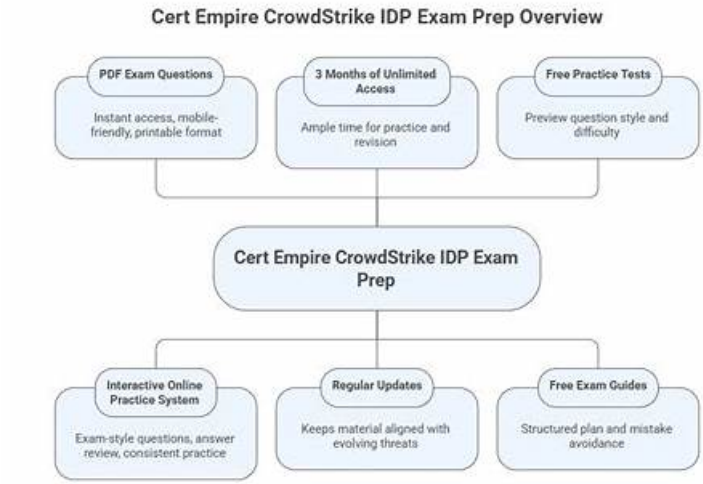
IDP Authentic Exam Questions & Reliable IDP Exam Registration



Allowing for your problems about passing the exam, our experts made all necessary points into our IDP training materials, making it the most efficient way to achieve success. They can alleviate your pressure, relieve you of tremendous knowledge and master the key points with the least time. As customer-oriented company, we believe in satisfying the customers at any costs. Instead of focusing on profits, we determined to help every customer harvest desirable outcomes by our IDP Training Materials. So our staff and after-sales sections are regularly interacting with customers for their further requirements and to know satisfaction levels of them.

CrowdStrike IDP Exam Syllabus Topics:

Topic	Details
Topic 1	• Falcon Fusion SOAR for Identity Protection: Explores SOAR workflow automation including triggers, conditions, actions, creating custom • templated • scheduled workflows, branching logic, and loops.
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	• 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	• 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 5	• 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 6	• 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 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.

>> IDP Authentic Exam Questions <<

Reliable IDP Exam Registration & New IDP Test Tutorial

Successful people are never satisfying their current achievements. So they never stop challenging themselves. If you refuse to be an ordinary person, come to learn our IDP preparation questions. Our IDP study materials will broaden your horizons and knowledge. Many people have benefited from learning our IDP learning braindumps. Most of them have realized their dreams and became successful.

CrowdStrike Certified Identity Specialist(CCIS) Exam Sample Questions (Q23-Q28):

NEW QUESTION # 23
How should an organization address the domain risk score found in the Domain Security Overview page?

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

Answer: D

Explanation:
TheDomain Security Overviewpage in Falcon Identity Protection presents domain risks in aprioritized, descending order, based on a combination ofseverity, likelihood, and consequence. The CCIS curriculum emphasizes that organizations should address risksfrom 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'sZero Trust-driven identity risk scoring methodology, makingOption Athe correct answer.

NEW QUESTION # 24
What is the purpose behind creating Policy Rules?

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

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 # 25
How many days will an identity-based incident be suppressed if new events related to the same incident occur?

- A. 14 days
- B. 7 days
- C. 30 days
- D. 5 days

Answer: D

Explanation:
Falcon Identity Protection usesincident suppression windowsto prevent alert fatigue while still maintaining accurate incident tracking. According to the CCIS documentation, whennew events related to an existing identity-based incident occur, the incident issuppressed for 5 days.
This suppression means that Falcon does not generate a new incident for the same activity during this window. Instead, additional detections areadded to the existing incident, allowing analysts to view the full progression of the threat in a single investigative context.
The 5-day suppression window ensures that ongoing identity attacks-such as repeated authentication abuse or lateral movement-are consolidated rather than fragmented across multiple incidents. This improves investigation efficiency and aligns with Falcon's incident lifecycle management approach.
Because the suppression period is fixed at5 days,Option Dis the correct and verified answer.

NEW QUESTION # 26
The configuration of the Azure AD (Entra ID) Identity-as-a-Service connector requires which three pieces of information?

- A. Tenant Domain, Client Secret, User Identifier
- B. Tenant Domain, Application ID, Application Secret
- C. Tenant Domain, Application ID, Scope
- D. Tenant Domain, Token, Configuration File

Answer: B

Explanation:
To integrate Falcon Identity Protection withAzure AD (Entra ID)as an Identity-as-a-Service (IDaaS) provider, specific application-level credentials are required. According to the CCIS curriculum, the connector configuration requiresTenant Domain,Application (Client) ID, andApplication Secret.
These values are generated when registering an application in Azure AD and are used to authenticate Falcon Identity Protection securely via OAuth-based API access. This method ensures least-privilege access and allows the connector to ingest cloud authentication activity and apply SSO-related policy enforcement.
Other options list incomplete or incorrect credential combinations. Therefore,Option Dis the correct and verified answer.

NEW QUESTION # 27
To enforce conditional access policies with Identity Verification, an MFA connector can be configured for different authentication methods such as:

- A. Push
- B. Alarm
- C. Pull
- D. Page

Answer: A

Explanation:
Falcon Identity Protection integrates with third-party MFA providers throughMFA connectorsto support conditional access and identity verification. The CCIS documentation explains that these connectors allow organizations to enforce MFA challenges based on identity risk, authentication behavior, or policy conditions.
One of the supported MFA authentication methods isPush, where a notification is sent to a registered device or application for user approval. Push-based MFA is widely used due to its balance of usability and security and is fully supported by Falcon Identity Protection when integrated with compatible MFA providers.
The other options are not valid MFA authentication methods within Falcon:
* Page and Pull are not recognized MFA mechanisms.
* Alarm is related to alerting, not authentication.
By enabling push-based MFA through an MFA connector, organizations can dynamically enforce identity verification in alignment with Zero Trust principles. Therefore,Option Bis the correct and verified answer.

NEW QUESTION # 28
.....