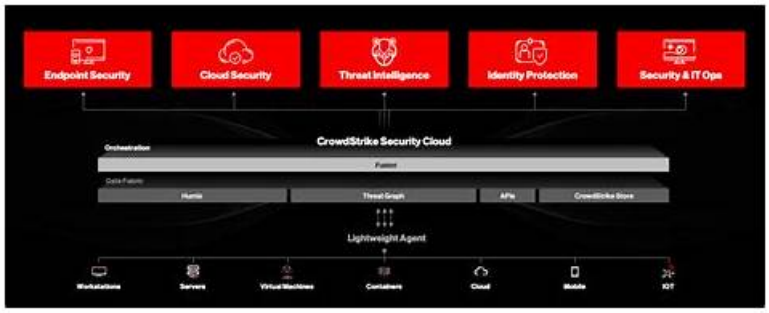
CrowdStrike IDP Exam Experience | IDP Dump Collection



Test4Cram is fully aware of the fact that preparing successfully for the CrowdStrike IDP exam in one go is a necessity because of the expensive registration fee. For applicants like you, success in the CrowdStrike Certified Identity Specialist(CCIS) Exam exam on the first attempt is crucial to saving money and time. Our Free CrowdStrike IDP Exam Questions will help you decide fast to buy the premium ones.

Our CrowdStrike Exam Questions greatly help CrowdStrike Certified Identity Specialist(CCIS) Exam (IDP) exam candidates in their preparation. Our CrowdStrike IDP practice questions are designed and verified by prominent and qualified CrowdStrike Certified Identity Specialist(CCIS) Exam (IDP) exam dumps preparation experts. The qualified CrowdStrike Certified Identity Specialist(CCIS) Exam (IDP) exam questions preparation experts strive hard and put all their expertise to ensure the top standard and relevancy of IDP exam dumps topics.

>> CrowdStrike IDP Exam Experience <<

IDP Exam Preparation: CrowdStrike Certified Identity Specialist(CCIS) Exam & IDP Best Questions

Life is full of ups and downs. We cannot predicate what will happen in the future. To avoid being washed out by the artificial intelligence, we must keep absorbing various new knowledge. Our IDP learning questions will inspire your motivation to improve yourself. Tens of thousands of our loyal customers are benefited from our IDP Study Materials and lead a better life now after they achieve their IDP certification.

CrowdStrike IDP Exam Syllabus Topics:

Topic	Details
Topic 1	• Risk Assessment: Covers entity risk categorization, risk and event analysis dashboards, filtering, user risk reduction, custom insights versus reports, and export scheduling.
Topic 2	• 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 3	• GraphQL API: Covers Identity API documentation, creating API keys, permission levels, pivoting from Threat Hunter to GraphQL, and building queries.
Topic 4	• 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 5	• User Assessment: Examines user attributes, differences between users • endpoints • entities, risk baselining, risky account types, elevated privileges, watchlists, and honeytoken accounts.

Topic 6	• 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 7	• Falcon Fusion SOAR for Identity Protection: Explores SOAR workflow automation including triggers, conditions, actions, creating custom • templated • scheduled workflows, branching logic, and loops.

CrowdStrike Certified Identity Specialist(CCIS) Exam Sample Questions (Q27-Q32):

NEW QUESTION # 27
What setting can be switched under the Domain Security Overview for each Active Directory domain and/or Azure tenant?

- A. Scope
- B. Domains
- C. Goal
- D. Privileged Identities

Answer: A

Explanation:
In the Domain Security Overview,Scopeis a configurable setting that allows administrators toswitch between Active Directory domains and Azure tenants. This capability is essential for organizations managing multiple identity environments, as it enables targeted risk assessment and comparison across different identity infrastructures.
The CCIS documentation explains that Scope determineswhich domain or tenant's identity data is displayedin the Overview dashboard, including risk scores, trends, and prioritized remediation guidance.
Changing the scope does not alter risk calculations; it simply refocuses the analysis on the selected identity environment.
Other options are incorrect because:
* Privileged Identities represent a subset of users, not a switchable setting.
* Domains are entities, not a dashboard control.
* Goal changes how risks are evaluated, not which environment is displayed.
By allowing granular control over which domain or tenant is analyzed, Scope supports accurate identity risk management in complex, hybrid environments. Therefore,Option Dis the correct answer.

NEW QUESTION # 28
How many days will an identity-based incident be suppressed if new events related to the same incident occur?

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

Answer: B

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 # 29
Which of the following actions under the Investigate menu will pivot to Falcon Identity Protection from an identity-based detection?

- A. Search for events in Threat Hunter
- B. Investigate involved users
- C. Search for involved entities in Threat Hunter
- D. Investigate involved endpoints

Answer: C

Explanation:
Falcon Identity Protection integrates directly withThreat Hunterto enable deeper investigation of identity- based activity. According to the CCIS curriculum, selectingSearch for involved entities in Threat Hunter allows analysts to pivot from an identity-based detection into Threat Hunter while preserving identity context.
This pivot enables analysts to examine related users, service accounts, endpoints, and authentication behavior using advanced queries and timelines. Importantly, this action maintains the identity-centric investigation flow, bridging detections with broader hunting capabilities.
The other options do not perform this specific pivot:
* Investigating users or endpoints remains within entity views.
* Searching for events in Threat Hunter does not preserve entity context.
BecauseSearch for involved entities in Threat Hunteris the correct pivot action,Option Bis the verified answer.

NEW QUESTION # 30
Which of the following areNOTincluded within the three-dot menu on Identity-based Detections?
Which of the following are not included within the three-dot menu on Identity-based Detections?

- A. Add to Watchlist
- B. Add comment
- C. Edit status
- D. Add exclusion

Answer: A

Explanation:
In Falcon Identity Protection, thethree-dot (#) action menuon anidentity-based detectionprovides analysts with a limited set of actions that applydirectly to the detection itself. According to the CCIS curriculum, these actions are designed to support investigation workflow, tuning, and documentation.
The supported actions in the detection-level three-dot menu include:
* Edit status, which allows analysts to update the detection state (for example, New, In Progress, or Closed).
* Add comment, which enables collaboration and documentation directly on the detection.
* Add exclusion, where supported, to suppress future detections that match known benign behavior.
Add to Watchlistisnot includedin this menu because watchlists are applied toentities(such as users, service accounts, or endpoints), not to detections. Watchlists are managed from entity views or investigation workflows and are used to increase visibility and monitoring priority for specific identities-not to act on individual detections.
This distinction is emphasized in CCIS training to reinforce the separation betweenentity-centric actionsand detection-centric actions. Because watchlists operate at the entity level,Option Bis the correct and verified answer.

NEW QUESTION # 31
Where in the Identity Protection module can one view the monitoring status of domain controllers?

- A. System Notifications
- B. Settings
- C. Domains
- D. Connectors

Answer: C

Explanation:
In Falcon Identity Protection, theDomainspage is where administrators can view themonitoring and health status of domain controllers. The CCIS curriculum explains that this page provides visibility into which domain controllers are actively reporting authentication traffic, their inspection status, and whether Authentication Traffic Inspection (ATI) is enabled.
This view is essential for validating coverage and ensuring that Falcon Identity Protection has sufficient visibility into domain authentication activity. Administrators can quickly identify gaps, such as domain controllers that are not reporting or are misconfigured, and take corrective action.
The other options serve different purposes:
* Settingsmanage general configuration.
* System Notificationsdisplay alerts and messages.
* Connectorsmanage integrations such as MFA and IDaaS.
Because domain controller visibility and monitoring health are managed at the domain level,Option C (Domains)is the correct and verified answer.

NEW QUESTION # 32
.....