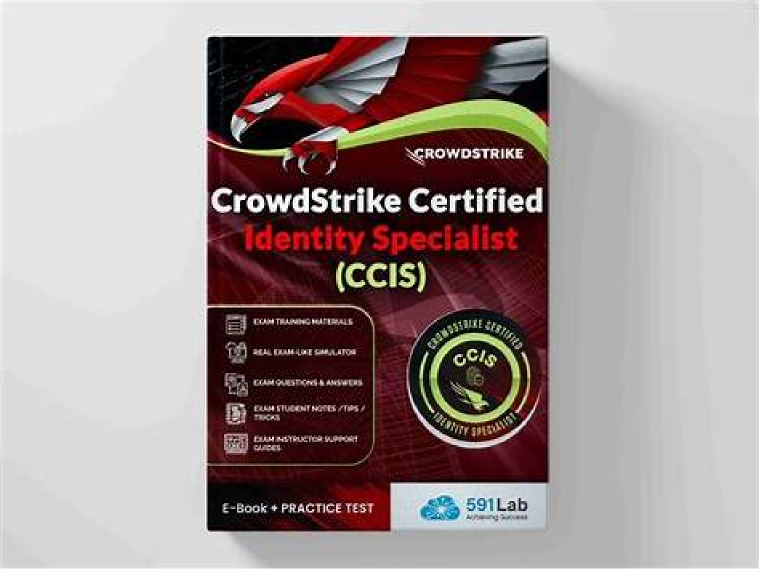
Free PDF The Best CrowdStrike - IDP - Exam Cram CrowdStrike Certified Identity Specialist(CCIS) Exam Pdf



If you buy the IDP study materials of us, we ensure you to pass the exam. Since the IDP study materials have the quality and the accuracy, and it will help you pass exam just one time. Buying IDP exam dumps are pass guaranteed and money back guaranteed for the failure. Furthermore, we choose international confirmation third party for payment for the IDP Exam Dumps, therefore we can ensure you the safety of your account and your money. The refund money will return to your payment account.

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	• User Assessment: Examines user attributes, differences between users • endpoints • entities, risk baselining, risky account types, elevated privileges, watchlists, and honeytoken accounts.
Topic 4	• 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 5	• 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 6	• Risk Assessment: Covers entity risk categorization, risk and event analysis dashboards, filtering, user risk reduction, custom insights versus reports, and export scheduling.

Topic 7	- Configuration and Connectors: Addresses domain controller monitoring, subnet management, risk settings, MFA and IDaaS connectors, authentication traffic inspection, and country-based lists.
Topic 8	- 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.

>> Exam Cram IDP Pdf <<

Quiz 2026 CrowdStrike IDP: CrowdStrike Certified Identity Specialist(CCIS) Exam – Reliable Exam Cram Pdf

At Dumpexams, we are aware that every applicant of the CrowdStrike Certified Identity Specialist(CCIS) Exam (IDP) examination is different. We know that everyone has a distinct learning style, situations, and set of goals, therefore we offer CrowdStrike IDP updated exam preparation material in three easy-to-use formats to accommodate every exam applicant's needs. This article will go over the three formats of the CrowdStrike Certified Identity Specialist(CCIS) Exam (IDP) practice material that we offer.

CrowdStrike Certified Identity Specialist(CCIS) Exam Sample Questions (Q10-Q15):

NEW QUESTION # 10
What is the recommended action for the"Guest Account Enabled"risk?

- A. Disable the endpoint in Active Directory
- B. Disable Guest accounts on all endpoints
- C. Apply a policy rule with an "Access" trigger and "Block" action on the Guest account
- D. Add related endpoints to a watchlist

Answer: B

Explanation:
In Falcon Identity Protection, the"Guest Account Enabled"risk highlights the presence of local or domain guest accounts that remain active across endpoints. Guest accounts are inherently high-risk because they typically lack strong authentication controls, are rarely monitored, and are frequently abused by attackers for lateral movement and persistence.
The CCIS curriculum explicitly recommendsdisabling Guest accounts on all endpointsas the primary remediation action. This is because guest accounts often bypass standard identity governance processes and violate the principles ofleast privilegeandZero Trust, both of which are foundational to Falcon Identity Protection's security model. Disabling these accounts removes an unnecessary and dangerous authentication path from the environment.
Other options are incorrect because:
* Adding endpoints to a watchlist does not remediate the risk.
* Blocking access via a policy rule is less effective than eliminating the account entirely.
* Disabling endpoints in Active Directory does not directly address the guest account exposure.
Falcon Identity Protection prioritizeselimination of weak identity configurations, and disabling guest accounts is a direct, effective action that immediately lowers identity risk scores and reduces attack surface.
Therefore,Option Cis the correct and verified answer.

NEW QUESTION # 11
How many days will an identity-based incident be suppressed if new events related to the same incident occur?

- A. 14 days
- B. 5 days
- C. 30 days
- D. 7 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 # 12

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

Answer: B

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 # 13

Which CrowdStrike documentation category would you search to find GraphQL examples?

- A. CrowdStrike APIs
- B. Identity Protection APIs
- C. XDR
- D. Threat Intelligence

Answer: A

Explanation:

GraphQL is the underlying query technology used by multiple CrowdStrike platforms, including Falcon Identity Protection.

According to the CCIS curriculum,GraphQL examples are documented under the broader "CrowdStrike APIs" documentation category, not limited to a single product.

The CrowdStrike APIs section includes:

* Authentication and API key usage

* GraphQL schema references

* Example GraphQL queries and mutations

* Pagination, filtering, and response handling

While Identity Protection uses GraphQL for identity-specific queries, the examples themselves are centralized underCrowdStrike APIsto provide consistency across Falcon modules. Product-specific use cases are then layered on top of these core examples.

The other options are incorrect:

* Threat Intelligence focuses on adversary data.

* XDR covers detection and correlation concepts.
* Identity Protection APIs describe endpoints and permissions, not general GraphQL usage examples.
Therefore,Option Ais the correct and verified answer.

NEW QUESTION # 14
How does Identity Protection extend the capabilities of existing multi-factor authentication (MFA)?

- A. Identity Protection is not going to detect risky user behavior
- B. Identity Protection does not support on-premises MFA connectors
- C. Identity Protection will replace third-party MFA and trigger as it detects risky or abnormal behaviors
- D. Implementation of a second-layer security control using policy rules as it detects risky or abnormal behaviors

Answer: D

Explanation:
Falcon Identity Protection is designed toextend-not replace-existing MFA solutions. According to the CCIS curriculum, Identity Protection enhances MFA by adding arisk-driven, policy-based enforcement layerthat dynamically triggers MFA challenges when risky or abnormal identity behavior is detected.
Rather than applying MFA uniformly, Falcon evaluates authentication context such as behavioral deviation, privilege usage, and anomaly detection. When risk thresholds are exceeded, Policy Rules can enforce MFA through integrated connectors, providing adaptive, Zero Trust-aligned authentication.
The incorrect options misunderstand Falcon's role. Identity Protection does detect risky behavior, does not replace MFA providers, and fully supports both cloud and on-premises MFA connectors.
Because Falcon adds intelligence-driven enforcement on top of MFA,Option Ais the correct and verified answer.

NEW QUESTION # 15
......

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