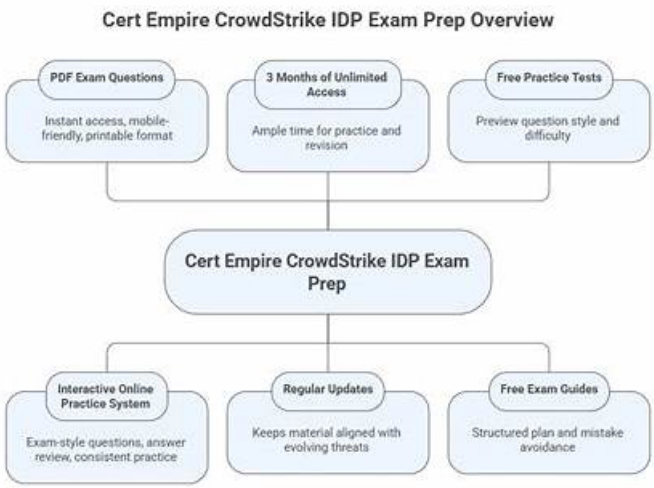
Quiz Unparalleled CrowdStrike - IDP Exam Bootcamp



BTW, DOWNLOAD part of ITExamDownload IDP dumps from Cloud Storage: https://drive.google.com/open?id=1p1LhVSDVbx6nz0OlRfgg_n6WR0QTG0ks

For the complete CrowdStrike Certified Identity Specialist(CCIS) Exam exam preparation and success, the ITExamDownload IDP exam practice test questions are the best choice. With the CrowdStrike IDP Exam Questions, you will get everything that you need to learn, prepare and succeed in the CrowdStrike Certified Identity Specialist(CCIS) Exam certification exam. You must add CrowdStrike IDP Exam Questions in your preparation and should not ignore them.

CrowdStrike IDP Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• Risk Assessment: Covers entity risk categorization, risk and event analysis dashboards, filtering, user risk reduction, custom insights versus reports, and export scheduling.
Topic 3	• 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 4	• 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 5	• Falcon Fusion SOAR for Identity Protection: Explores SOAR workflow automation including triggers, conditions, actions, creating custom • templated • scheduled workflows, branching logic, and loops.
Topic 6	• 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 7	• 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.

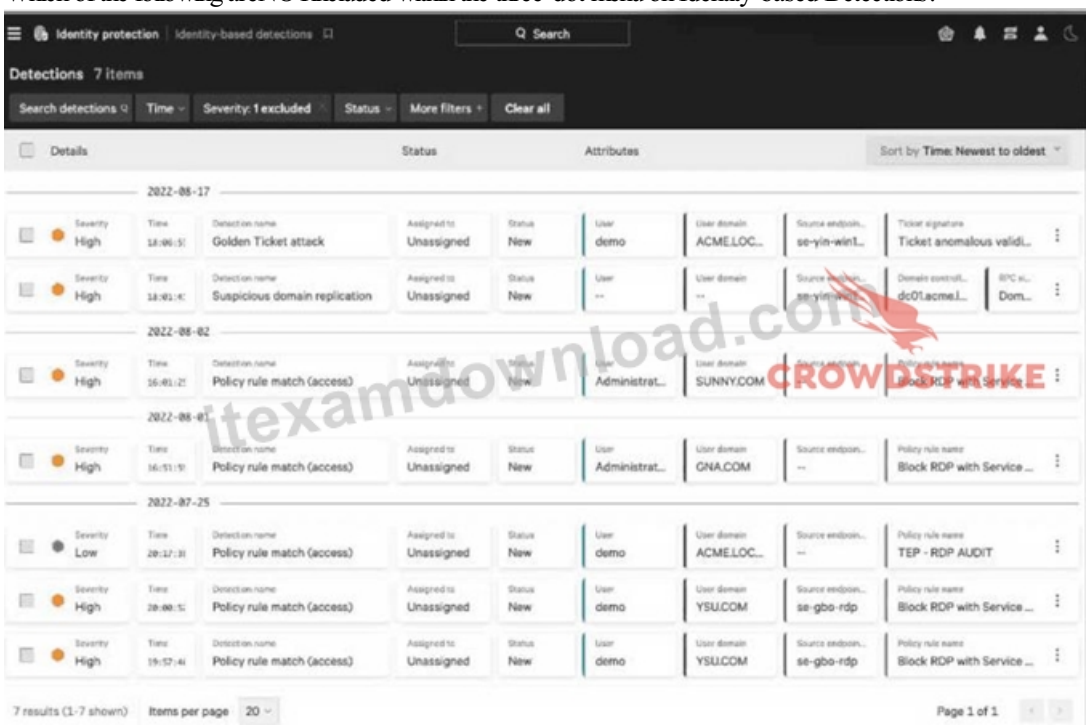
Topic 8	• Risk Management with Policy Rules: Covers creating and managing policy rules and groups, triggers, conditions, enabling • disabling rules, applying changes, and required Falcon roles.
Topic 9	• Identity Protection Tenets: Examines Falcon Identity Protection's architecture, domain traffic inspection, EDR complementation, human vulnerability protection, log-free detections, and identity-based attack mitigation.
Topic 10	• GraphQL API: Covers Identity API documentation, creating API keys, permission levels, pivoting from Threat Hunter to GraphQL, and building queries.

Valid IDP Exam Tutorial - IDP Download Pdf

Facing the incoming CrowdStrike IDP Exam, you may feel stained and anxious, suspicious whether you could pass the exam smoothly and successfully. Actually, you must not impoverish your ambition. Our suggestions are never boggle at difficulties. It is your right time to make your mark.

CrowdStrike Certified Identity Specialist(CCIS) Exam Sample Questions (Q33-Q38):

NEW QUESTION # 33
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 comment
- B. Edit status
- C. Add to Watchlist
- D. Add exclusion

Answer: C

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 # 34
Under which CrowdStrike documentation category could you find Identity Protection API information?

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

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 # 35
Which of the following would cause an identity-based incident type to change?

- A. A user linked detections to the incident in the console
- B. An exclusion added to the incident
- C. Detections related to the incident
- D. A user changed the incident type in the console

Answer: C

Explanation:
In Falcon Identity Protection,identity-based incidents are dynamicand can evolve over time as additional detections are associated with them. According to the CCIS curriculum, an incident'stype is automatically recalculatedbased on thedetections related to the incident, not by manual user actions.
As new identity-based detections are generated-such as credential misuse, lateral movement attempts, or abnormal authentication behavior-the platform continuously reassesses the incident. If the newly added detections indicate a different or more severe attack pattern, Falcon may automaticallychange the incident typeto better reflect the observed threat activity.
Manual actions such as adding exclusions or linking detections do not directly change the incident type.
Similarly, users cannot manually override an incident's classification. The classification logic is driven entirely by Falcon's analytics engine to ensure consistent, objective threat categorization.
This automated behavior is emphasized in CCIS training to highlight Falcon's ability toadapt incident context as attacks progress, makingOption Dthe correct answer.

NEW QUESTION # 36
What is the recommended action for the"Guest Account Enabled"risk?

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

Answer: D

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 # 37
Which section of the Falcon menu is used to investigate the Event Analysis dashboard?

- A. Enforce
- B. Configure
- C. Threat Hunter
- D. Explore

Answer: D

Explanation:
In Falcon Identity Protection, theExploresection of the Falcon menu is used to investigate analytical views such as theEvent Analysis dashboard. This aligns with the CCIS framework, which defines Explore as the primary area forinteractive investigation, analytics, and risk explorationacross identity data.
The Event Analysis dashboard is designed to help administrators analyzeidentity-related authentication events, behavioral patterns, and anomalous activity derived from domain traffic inspection and domain controller telemetry. These analytical capabilities are intentionally placed underExplorebecause this menu category supports hypothesis-driven investigation rather than enforcement or configuration actions.
By contrast:
* Enforceis used to apply policy rules and automated controls.
* Threat Hunteris focused on proactive hunting using queries and detection pivots.
* Configureis used to manage settings, connectors, policies, and integrations.
The CCIS documentation explicitly associates dashboards such asRisk AnalysisandEvent Analysiswith the Explore menu, emphasizing its role in understandingwhyrisk exists before taking action. Therefore,Option C (Explore)is the correct and verified answer.

NEW QUESTION # 38
.....

Overall, IDP is committed to helping candidates achieve success in the CrowdStrike IDP exam. Their goal is to save students time and money, and they guarantee that candidates who use their product will pass the IDP Exam on their first try. With the right study

material and support team, passing the exam at the first attempt is an achievable goal.

Valid IDP Exam Tutorial: https://www.itexamdownload.com/IDP-valid-questions.html

- IDP Reliable Exam Pass4sure □ IDP Technical Training □ Exam IDP Lab Questions □ Open ➽ www.dumpsquestion.com □ enter □ IDP □ and obtain a free download □IDP Technical Training
- Exam IDP Online □ IDP Exam Learning □ IDP Valid Test Pattern □ Easily obtain □ IDP □ for free download through ➡ www.pdfvce.com □□□ □New IDP Test Questions
- Easy to Use and Compatible CrowdStrike IDP Exam Practice Test Questions Formats □ The page for free download of ▸ IDP ◂ on [www.validtorrent.com] will open immediately □Valid IDP Test Answers
- Reliable IDP Exam Materials □ Free IDP Learning Cram □ Valid IDP Test Answers □ Easily obtain free download of ✔ IDP □✔□ by searching on 「 www.pdfvce.com 」 □Reliable IDP Exam Materials
- IDP Valid Test Pattern □ Exam IDP Materials □ IDP Technical Training □ Search for ▹ IDP ◃ and download exam materials for free through ➥ www.prepawaypdf.com □ □100% IDP Correct Answers
- Free IDP Learning Cram □ IDP Braindumps Pdf □ New IDP Test Questions □ Simply search for ➡ IDP □□□ for free download on ➡ www.pdfvce.com □□□ □Testing IDP Center
- IDP Valid Test Answers □ New IDP Test Tips □ IDP Valid Test Pattern □ Immediately open （ www.testkingpass.com ） and search for ➥ IDP □ to obtain a free download □Valid IDP Test Answers
- Latest Released CrowdStrike IDP Exam Bootcamp: CrowdStrike Certified Identity Specialist(CCIS) Exam □ Go to website □ www.pdfvce.com □ open and search for ➥ IDP □ to download for free ⓔIDP New Study Materials
- Hot IDP Exam Bootcamp Offers you Professional Actual CrowdStrike CrowdStrike Certified Identity Specialist(CCIS) Exam Exam Products □ Open website { www.testkingpass.com } and search for □ IDP □ for free download □IDP Valid Test Answers
- IDP Training Materials - IDP Dumps PDF - IDP Exam Cram □ Easily obtain free download of （ IDP ） by searching on （ www.pdfvce.com ） □Reliable IDP Exam Materials
- Hot IDP Exam Bootcamp Offers you Professional Actual CrowdStrike CrowdStrike Certified Identity Specialist(CCIS) Exam Exam Products □ Download □ IDP □ for free by simply searching on ➠ www.practicevce.com □ □Testing IDP Center
- dirstop.com, bookmarksden.com, monicacvag881780.blogdun.com, esmeeijlc671089.bloggactif.com, atozbookmark.com, www.stes.tyc.edu.tw, bookmarkbirth.com, trackbookmark.com, bookmarks-hit.com, blanchecezg345947.loginblogin.com, Disposable vapes

BTW, DOWNLOAD part of ITExamDownload IDP dumps from Cloud Storage: https://drive.google.com/open?id=1p1LhVSDVbx6nz0OlRfgg_n6WR0QTG0ks