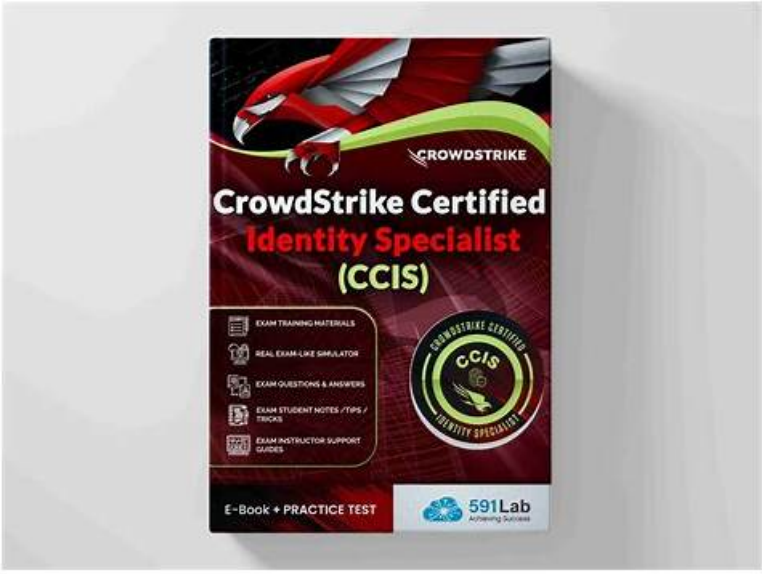
Free PDF 2026 The Best IDP: CrowdStrike Certified Identity Specialist(CCIS) Exam Test Questions Fee



What's more, part of that ITdumpsfree IDP dumps now are free: https://drive.google.com/open?id=1gcpTEunsGu--3D9keURjU3U3m6OovqRj

Users don't need to install any plugins or software to attempt the CrowdStrike IDP practice exam. All operating systems support this format. The third and last format is CrowdStrike Certified Identity Specialist(CCIS) Exam IDP desktop software that can be used on Windows computers. The customers that have Windows laptops or computers can attempt the practice exam and prepare for it efficiently. These formats are in use by a lot of applicants currently and they are preparing for their best future on daily basis. Even the customers who have used it in the past for the preparation of CrowdStrike IDP Certification Exam have rated our product as one of the best.

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	• Falcon Fusion SOAR for Identity Protection: Explores SOAR workflow automation including triggers, conditions, actions, creating custom • templated • scheduled workflows, branching logic, and loops.
Topic 3	• Risk Assessment: Covers entity risk categorization, risk and event analysis dashboards, filtering, user risk reduction, custom insights versus reports, and export scheduling.
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	• 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	• User Assessment: Examines user attributes, differences between users • endpoints • entities, risk baselining, risky account types, elevated privileges, watchlists, and honeytoken accounts.

>> IDP Test Questions Fee <<

Get Latest CrowdStrike IDP Practice Test For Quick Preparation

We provide you with our best CrowdStrike IDP exam study material, which builds your ability to get high-paying jobs. CrowdStrike IDP Exam Dumps includes CrowdStrike IDP Dumps PDF format, desktop IDP practice exam software, and web-based IDP practice test software.

CrowdStrike Certified Identity Specialist(CCIS) Exam Sample Questions (Q48-Q53):

NEW QUESTION # 48
Which of the following Falcon rolesCANNOTenable and disable policy rules?

- A. Identity Protection Policy Manager
- B. Identity Protection Domain Administrator
- C. Identity Protection Administrator
- D. Falcon Administrator

Answer: B

Explanation:
Falcon Identity Protection enforcesrole-based access control (RBAC)to ensure that only authorized users can create, modify, or manage policy rules. Policy rules directly impact identity enforcement actions, making proper role separation critical.
According to the CCIS documentation, the ability toenable and disable policy rulesis granted to theIdentity Protection Policy Managerand theFalcon Administratorroles. These roles are explicitly designed to manage enforcement logic, triggers, and automated identity controls.
TheIdentity Protection Domain Administratorrole, however, is limited todomain-level visibility and management, such as reviewing domain configurations, monitoring risks, and assessing posture. This role doesnothave permissions to modify or control policy enforcement behavior.
This separation prevents accidental or unauthorized changes to identity enforcement rules. Therefore,Option Ais the correct and verified answer.

NEW QUESTION # 49
What is the recommended action for the"Guest Account Enabled"risk?

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

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 # 50
Which of the following statements isNOTtrue as it relates to Identity Events, Detections, and Incidents?

- A. A detection can become an element of an incident that preceded it in time
- B. Events related to an incident that occur after the incident is marked In Progress will create a new incident
- C. An event can become an element of a detection that preceded it in time
- D. Not all events are security events that become elements of detections

Answer: B

Explanation:
Falcon Identity Protection follows acorrelation and enrichment modelwhere events, detections, and incidents are dynamically linked over time. According to the CCIS curriculum,events that occur after an incident is marked In Progress do not automatically create a new incident. Instead, related events and detections are typicallyadded to the existing incident, provided they fall within the incident's correlation and suppression window.
This behavior allows Falcon to present asingle evolving incident, showing the full progression of an identity attack rather than fragmenting activity into multiple incidents. Therefore, statementA is not true.
The other statements are correct:
* Detections can be retroactively associated with incidents that occurred earlier if correlation logic determines relevance.
* Events can be linked to detections even if the detection is created after the event occurred.
* Not all events are security-relevant; many remain informational and never become detections.
This adaptive correlation model is a core concept in CCIS training and supports efficient investigation and incident lifecycle management. Hence,Option Ais the correct answer.

NEW QUESTION # 51
What basic configuration fields are typically required for cloud Multi-Factor Authentication (MFA) connectors?

- A. Domain controller host name and IP address
- B. Connector application identifier and secret keys
- C. Service account user name and password
- D. Domain Administrator user name and password

Answer: B

Explanation:
Cloud-based MFA connectors integrate Falcon Identity Protection with third-party MFA providers using application-based authentication, not user credentials. As outlined in the CCIS curriculum, these connectors require anapplication identifier (Client/Application ID)andsecret keysto securely authenticate API communications.
This approach follows modern security best practices by avoiding the use of privileged user credentials and instead leveraging scoped, revocable application secrets. The connector uses these credentials to trigger MFA challenges and exchange authentication context securely.
Options involving usernames, passwords, or domain controller details are incorrect, as Falcon Identity Protection does not store or require privileged account credentials for MFA integrations. Therefore,Option D is the correct answer.

NEW QUESTION # 52
Within the Falcon Identity Protection portal, which page allows you to enable/disable Policy Rules?

- A. Identity-Based Detections
- B. Policy Enforcement
- C. Configure

- D. Enforce

Answer: D

Explanation:
In Falcon Identity Protection, Policy Rules are managed within the Enforce section of the portal. The CCIS documentation explains that Enforce is the operational area where administrators create, enable, disable, and manage Policy Rules and Policy Groups.
This section is specifically designed for identity enforcement logic, allowing security teams to activate or suspend rules without modifying underlying configurations or analytics. Enabling or disabling a Policy Rule immediately affects how identity conditions are enforced across the environment.
Other sections serve different purposes:
Configure manages connectors, domains, subnets, and risk settings.
Identity-Based Detections is used for investigation and monitoring.
Policy Enforcement is not a standalone navigation section in Falcon Identity Protection.
Because rule activation and enforcement control reside exclusively in Enforce, Option B is the correct and verified answer.

NEW QUESTION # 53
.....

In order to serve you better, we have do what we can do for you. Before buying IDP exam torrent, we offer you free demo for you to have a try, so that you can have a deeper understanding of what you are going to buy. If you want the IDP exam materials after trying, you just need to add them to cart and pay for them, then you can get downloading link and password within ten minutes, if you don't receive the IDP Exam Torrent, just contact us, and we will solve the problem for you. We have after-service stuff, and you can ask any questions about IDP exam dumps after buying.

Downloadable IDP PDF: https://www.itdumpsfree.com/IDP-exam-passed.html

P.S. Free & New IDP dumps are available on Google Drive shared by ITdumpsfree: https://drive.google.com/open?id=1gcpTEunsGu--3D9keURjU3U3m6OovqRj