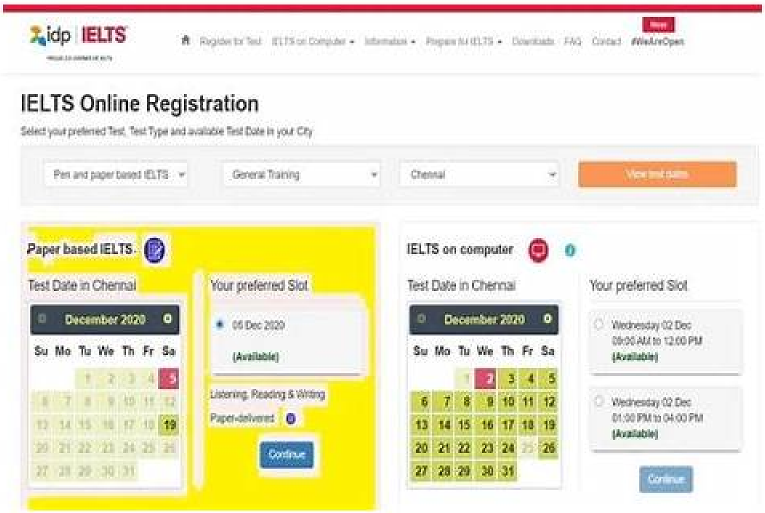
Mock IDP Exam, Reliable IDP Exam Registration



IELTS Online Registration

Select your preferred Test, Test Type and available Test Date in your City

Pen and paper based IELTS | General Training | Chennai

Paper based IELTS

Test Date in Chennai

December 2020

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

Your preferred Slot

● 05 Dec 2020 (Available)

Listening, Reading & Writing

Paper-delivered

IELTS on computer

Test Date in Chennai

December 2020

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

Your preferred Slot

○ Wednesday 02 Dec 09:00 AM to 12:00 PM (Available)

○ Wednesday 02 Dec 01:00 PM to 04:00 PM (Available)

You will stand at a higher starting point than others if you buy our IDP exam braindumps. Why are IDP practice questions worth your choice? I hope you can spend a little time reading the following content on the website, I will tell you some of the advantages of our IDP Study Materials. Firstly, our pass rate for IDP training guide is unmatched high as 98% to 100%. Secondly, we have been in this career for years and became a famous brand.

The operation of our IDP exam torrent is very flexible and smooth. Once you enter the interface and begin your practice on our windows software. You will easily find there are many useful small buttons to assist your learning. The correct answer of the IDP exam torrent is below every question, which helps you check your answers. We have checked all our answers. You just need to wait a few seconds before knowing your scores. The scores are calculated by every question of the IDP Exam guides you have done. So the final results will display how many questions you have answered correctly and mistakenly. You even can directly know the score of every question, which is convenient for you to know the current learning condition.

>> Mock IDP Exam <<

Best CrowdStrike Mock IDP Exam Help You Pass Your CrowdStrike CrowdStrike Certified Identity Specialist(CCIS) Exam Exam From The First Try

There is considerate and concerted cooperation for your purchasing experience on our IDP exam braindumpsaccompanied with patient staff with amity. You can find IDP simulating questions on our official website, and we will deal with everything once your place your order. You will find that you can receive our IDP training guide in just a few minutes, almost 5 to 10 minutes. And if you have any questions, you can contact us at any time since we offer 24/7 online service for you.

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	• 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 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	- 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	- 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 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.
Topic 8	- Risk Assessment: Covers entity risk categorization, risk and event analysis dashboards, filtering, user risk reduction, custom insights versus reports, and export scheduling.

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

NEW QUESTION # 33
Which entity tab will show an administrator how to lower the account's risk score?

- A. Timeline
- B. Risk
- C. Asset
- D. Activity

Answer: B

Explanation:
In CrowdStrike Falcon Identity Protection, theRisktab within a user or account entity provides administrators with direct visibility intowhy an account has a specific risk score and what actions can be taken to reduce that score. This functionality is a core component of theUser AssessmentandRisk Assessmentsections of the CCIS (CrowdStrike Identity Specialist) curriculum.
The Risk tab aggregates bothanalysis-based risksanddetection-based risks, clearly identifying contributing factors such as compromised passwords, excessive privileges, risky authentication behavior, stale or never- used accounts, and policy violations. It also highlights theseverity, likelihood, and consequenceof each risk factor, allowingadministrators to prioritize remediation efforts effectively. Most importantly, this tab provides actionable guidance, enabling teams to understand which specific remediation steps-such as enforcing MFA, resetting credentials, reducing privileges, or disabling unused accounts-will directly lower the account's overall risk score.
Other entity tabs do not provide this capability. TheTimelinetab focuses on chronological events and detections, theActivitytab displays authentication and behavioral activity, and theAssettab shows associated endpoints and resources. Only theRisktab is designed to explain risk drivers and guide remediation, making Option Dthe correct and verified answer.

NEW QUESTION # 34
Which of the following users would most likely have aHIGHrisk score?

- A. User that recently logged in from a shared endpoint
- B. User that has not logged in recently and is marked as Stale
- C. Privileged user with a Compromised Password
- D. User that is a member of the Domain Admins group

Answer: C

Explanation:

Falcon Identity Protection calculates user risk scores based on a combination ofprivilege level,credential exposure, andbehavioral indicators. According to the CCIS curriculum, aprivileged user with a compromised passwordrepresents one of the highest-risk identity scenarios.

Privileged accounts-such as administrators or service accounts with elevated access-already pose increased risk due to their access scope. When Falcon detects that such an account's credentials have been compromised, the risk escalates significantly because attackers can immediately gain high-impact access without further escalation.

The other options do not inherently represent the same level of risk:

* Logging in from a shared endpoint may increase risk but is context-dependent.

* Stale users are risky but typically lower risk than active compromised credentials.

* Domain Admin group membership alone does not imply compromise.

Becausecredential compromise combined with privilegedramatically increases attack potential,Option Bis the correct and verified answer.

NEW QUESTION # 35

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

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

Answer: C

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 # 36

What does a modern Zero Trust security architecture offer compared to a traditional wall-and-moat (perimeter- based firewall) approach?

- A. Applies machine learning to gauge the trustworthiness of any external entities
- B. Issues trust certificates to internal entities and zero trust certificates to external entities
- C. Continuously authenticates entities regardless of origin
- D. Secures the perimeter of a network and does not allow access to any entities deemed "zero trust"

Answer: C

Explanation:

A modern Zero Trust security architecture fundamentally differs from the traditional wall-and-moat model by eliminating implicit trust based on network location. As defined inNIST SP 800-207and reinforced in the CCIS curriculum, Zero Trust requirescontinuous authentication and authorization of all entities, regardless of whether they originate from inside or outside the network.

Traditional perimeter-based security assumes that users and devices inside the network are trusted, focusing defenses at the boundary. This approach fails in modern environments where cloud access, remote work, and compromised credentials allow attackers to operate internally without triggering perimeter controls.

Zero Trust replaces this assumption with continuous validation using identity, behavior, device posture, and risk signals. Falcon Identity Protection operationalizes this concept by continuously inspecting authentication traffic and reassessing trust throughout a session, not just at login time.

Because Zero Trust applies universally and continuously,Option Dis the correct and verified answer.

NEW QUESTION # 37

Which of the following isNOTan available Goal within the Domain Security Overview?

- A. AD Hygiene
- B. Pen Testing
- C. Business Privileged Users Management
- D. Privileged Users Management

Answer: C

Explanation:
The Domain Security Overview in Falcon Identity Protection usesGoalsto frame identity risks into focused security assessment perspectives. These goals allow organizations to evaluate identity posture based on specific security priorities such as directory hygiene, privilege exposure, or overall attack surface reduction.
According to the CCIS curriculum, theavailable GoalsincludePrivileged Users Management,AD Hygiene, Pen Testing, andReduce Attack Surface. These goals are predefined by CrowdStrike and determine how risks are grouped, weighted, and presented in reports.
Business Privileged Users Managementisnot an available Goalwithin the Domain Security Overview.
While Falcon Identity Protection does support the concept ofbusiness privilegesand evaluates their impact on users and entities, this concept is handled through risk analysis and configuration-not as a selectable Domain Security Goal.
The CCIS documentation clearly distinguishes betweenGoals(which control reporting and assessment views) andbusiness privilege modeling(which influences risk scoring). Therefore,Option Bis the correct and verified answer.

NEW QUESTION # 38

......

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