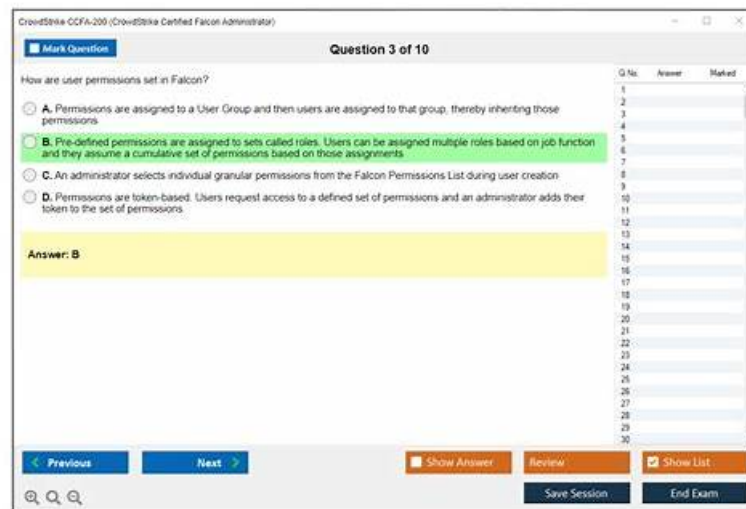


CrowdStrike IDP Exam Questions 2026 in PDF Format



Market is a dynamic place because a number of variables keep changing, so is the practice materials field of the IDP practice exam. Our IDP exam dumps are indispensable tool to pass it with high quality and low price. By focusing on how to help you effectively, we encourage exam candidates to buy our IDP practice test with high passing rate up to 98 to 100 percent all these years. Our CrowdStrike exam dumps almost cover everything you need to know about the exam. As long as you practice our IDP Test Question, you can pass exam quickly and successfully. By using them, you can not only save your time and money, but also pass IDP practice exam without any stress.

Our IDP exam simulation is a great tool to improve our competitiveness. After we use our study materials, we can get the CrowdStrike certification faster. This certification gives us more opportunities. Compared with your colleagues around you, with the help of our IDP preparation questions, you will also be able to have more efficient work performance. Our IDP Study Materials can bring you so many benefits because they have the following features. I hope you can use a cup of coffee to learn about our IDP training engine. Perhaps this is the beginning of your change.

>> Online IDP Test <<

CrowdStrike IDP Latest Exam Cost | IDP Valid Exam Dumps

Our CrowdStrike IDP exam dumps give help to give you an idea about the actual CrowdStrike Certified Identity Specialist(CCIS) Exam (IDP) exam. You can attempt multiple CrowdStrike Certified Identity Specialist(CCIS) Exam (IDP) exam questions on the software to improve your performance. TorrentValid has many CrowdStrike Certified Identity Specialist(CCIS) Exam (IDP) practice questions that reflect the pattern of the real CrowdStrike Certified Identity Specialist(CCIS) Exam (IDP) exam. TorrentValid allows you to create a CrowdStrike Certified Identity Specialist(CCIS) Exam (IDP) exam dumps according to your preparation. It is easy to create the CrowdStrike IDP practice questions by following just a few simple steps. Our CrowdStrike Certified Identity Specialist(CCIS) Exam (IDP) exam dumps are customizable based on the time and type of questions.

CrowdStrike Certified Identity Specialist(CCIS) Exam Sample Questions (Q11-Q16):

NEW QUESTION # 11

To enforce conditional access policies with Identity Verification, an MFA connector can be configured for different authentication methods such as:

- A. Pull
- **B. Push**
- C. Alarm
- D. Page

Answer: B

Explanation:

Falcon Identity Protection integrates with third-party MFA providers through MFA connectors to support conditional access and identity verification. The CCIS documentation explains that these connectors allow organizations to enforce MFA challenges based on identity risk, authentication behavior, or policy conditions.

One of the supported MFA authentication methods is Push, where a notification is sent to a registered device or application for user approval. Push-based MFA is widely used due to its balance of usability and security and is fully supported by Falcon Identity Protection when integrated with compatible MFA providers.

The other options are not valid MFA authentication methods within Falcon:

* Page and Pull are not recognized MFA mechanisms.

* Alarm is related to alerting, not authentication.

By enabling push-based MFA through an MFA connector, organizations can dynamically enforce identity verification in alignment with Zero Trust principles. Therefore, Option B is the correct and verified answer.

NEW QUESTION # 12

Any countries or regions included in the _ will trigger a geolocation detection.

- A. Allowlist
- B. Dictionary
- C. Blocklist
- D. Exclusion

Answer: C

Explanation:

Falcon Identity Protection supports geolocation-based detection to identify potentially risky authentication activity originating from unexpected or prohibited locations. According to the CCIS curriculum, any countries or regions added to the Blocklist will automatically trigger a geolocation-based detection when authentication traffic is observed from those locations.

The Blocklist is designed to explicitly define disallowed geographic regions. When an authentication attempt originates from a blocklisted country or region, Falcon treats the activity as suspicious and generates a detection or contributes to increased identity risk.

By contrast:

* An Allowlist defines approved locations and suppresses detections.

* A Dictionary is used for password-related analysis.

* An Exclusion suppresses detections rather than generating them.

Because geolocation detections are triggered by blocklisted locations, Option A is the correct answer.

NEW QUESTION # 13

What is the recommended action for the "Guest Account Enabled" risk?

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

Answer: C

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 recommends disabling Guest accounts on all endpoints as the primary remediation action. This is because guest accounts often bypass standard identity governance processes and violate the principles of least privilege and Zero 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 prioritizes elimination 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 C is the correct and verified answer.

NEW QUESTION # 14

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

Answer: C

Explanation:

Falcon Identity Protection follows a correlation and enrichment model where 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 typically added to the existing incident, provided they fall within the incident's correlation and suppression window.

This behavior allows Falcon to present a single evolving incident, showing the full progression of an identity attack rather than fragmenting activity into multiple incidents. Therefore, statement A 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 A is the correct answer.

NEW QUESTION # 15

The events are excluded by default while Low, Medium, and High detections are visible.

- A. Internal
- B. Inferior
- C. Informational
- D. Indiscrete

Answer: C

Explanation:

In Falcon Identity Protection, Informational detections represent low-impact events that provide context but do not indicate elevated identity risk. According to the CCIS curriculum, Informational events are excluded by default from standard detection views to reduce noise and allow analysts to focus on higher-risk activity.

By default, Low, Medium, and High severity detections remain visible, as these contribute directly to identity risk scoring, incident formation, and investigative workflows. Informational detections can still be viewed if filters are adjusted, but they are intentionally hidden in default views.

This design supports efficient threat triage by prioritizing detections that are more likely to represent real security concerns. The other options listed are not valid detection severity classifications within Falcon Identity Protection.

Because Informational events are excluded by default while higher-severity detections remain visible, Option A is the correct and verified answer.

NEW QUESTION # 16

.....

The free demo CrowdStrike IDP exam questions are available for instant download. Download the CrowdStrike Certification Exams dumps demo free of cost and explore the top features of CrowdStrike Certified Identity Specialist (CCIS) Exam (IDP) exam questions and if you feel that the IDP exam questions can be helpful in CrowdStrike IDP exam preparation then take your buying decision. Best of luck!!!

IDP Latest Exam Cost: <https://www.torrentvalid.com/IDP-valid-braindumps-torrent.html>

- [illegible]