

# Latest IDP Exam Cost | IDP Test Practice



Time is life, time is speed, and time is power. You have to spend less time reaching your goals before you can walk ahead and seize more opportunities. Now, if you use our IDP preparation materials, you only need to learn twenty to thirty hours to go to the exam. And this data is provided and tested by our worthy customers. For they have passed the exam with the help of our IDP Exam Questions in such a short time and as 98% to 100% of them passed. The pass rate is also unmatched in the market!

Competition appear everywhere in modern society. There are many way to improve ourselves and learning methods of IDP exams come in different forms. Economy rejuvenation and social development carry out the blossom of technology; some IDP practice materials are announced which have a good quality. Certification qualification IDP Exam Materials are a big industry and many companies are set up for furnish a variety of services for it. And our IDP study guide has three different versions: PDF, Soft and APP versions to let you study in varied and comfortable ways.

>> Latest IDP Exam Cost <<

## IDP Test Practice, Examcollection IDP Vce

The data that come up with our customers who have bought our IDP actual exam and provided their scores show that our high pass rate of our IDP exam questions is 98% to 100%. This is hard to find and compare with in the market. And numerous enthusiastic feedbacks from our worthy clients give high praises not only on our IDP study torrent, but also on our sincere and helpful 24 hours customer services online. All of these prove that we are the first-class vendor in this career and have authority to ensure your success in your first try on IDP exam.

## CrowdStrike Certified Identity Specialist(CCIS) Exam Sample Questions (Q51-Q56):

### NEW QUESTION # 51

Which of the following BEST indicates that this user has an established baseline?

- A. The user has endpoints that they are considered owners of
- B. The user was found logging into five endpoints
- C. The user has a risk score of 6.4
- D. The user has recent logon activity on ETIS-WS03

**Answer: A**

**Explanation:**

In Falcon Identity Protection, a user baseline is established by observing consistent and repeatable behavior over time, including authentication patterns, endpoint associations, and usage context. According to the CCIS curriculum, one of the strongest indicators that a user has an established baseline is the presence of endpoints for which the user is identified as an owner.

Endpoint ownership is determined through historical authentication behavior and usage frequency. When Falcon identifies that a user consistently logs into specific endpoints over time, those endpoints are marked as owned, which signifies that sufficient historical data exists to confidently model the user's normal behavior.

This ownership relationship is only created after Falcon has observed the user long enough to establish a reliable baseline.

The other options do not definitively indicate a baseline:

- \* Logging into multiple endpoints may occur during initial discovery or anomalous activity.
- \* A risk score reflects current risk posture, not baseline maturity.
- \* Recent logon activity alone does not imply historical consistency.

Because endpoint ownership requires sustained, predictable behavior over time, it is the clearest indicator that Falcon has successfully established a user baseline. Therefore, Option B is the correct and verified answer.

### NEW QUESTION # 52

Which of the following are NOT included 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 exclusion
- B. Edit status
- C. Add comment
- D. Add to Watchlist

**Answer: D**

Explanation:

In Falcon Identity Protection, the three-dot (#) action menu on an identity-based detection provides analysts with a limited set of actions that apply directly 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 Watchlist is not included in this menu because watchlists are applied to entities (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 between entity-centric actions and detection-centric actions. Because watchlists operate at the entity level, Option B is the correct and verified answer.

### NEW QUESTION # 53

By using compromised credentials, threat actors are able to bypass the Execution phase of the MITRE ATT&CK framework and move directly into:

- A. Discovery
- B. Lateral Movement
- C. Weaponization
- D. Initial Access

**Answer: A**

Explanation:

The CCIS curriculum highlights a critical identity-security concept: when attackers use compromised credentials, they often bypass traditional malware-based attack phases, including the Execution phase of the MITRE ATT&CK framework. Because no malicious code needs to be executed, attackers can immediately begin interacting with the environment as a legitimate user.

As a result, threat actors move directly into the Discovery phase. During Discovery, attackers enumerate users, groups, privileges, systems, domain relationships, and trust paths to understand the environment and plan further actions. This behavior is commonly observed in identity-based attacks and living-off-the-land techniques.

Falcon Identity Protection is specifically designed to detect this behavior by monitoring authentication traffic, privilege usage, and anomalous identity activity—areas where traditional EDR tools may have limited visibility.

The other options are incorrect:

- \* Initial Access has already occurred via credential compromise.
- \* Weaponization and Execution are not required.
- \* Lateral Movement typically follows Discovery.

Because compromised credentials allow attackers to jump straight into Discovery, Option C is the correct and verified answer.

#### NEW QUESTION # 54

Which of the following statements is NOT true as it relates to Identity Events, Detections, and Incidents?

- A. Not all events are security events that become elements of detections
- **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. A detection can become an element of an incident that preceded it in time

**Answer: B**

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 # 55

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

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

**Answer: A**

Explanation:

In Falcon Identity Protection, the Explore section of the Falcon menu is used to investigate analytical views such as the Event Analysis dashboard. This aligns with the CCIS framework, which defines Explore as the primary area for interactive investigation, analytics, and risk exploration across identity data.

The Event Analysis dashboard is designed to help administrators analyze identity-related authentication events, behavioral patterns, and anomalous activity derived from domain traffic inspection and domain controller telemetry. These analytical capabilities are intentionally placed under Explore because this menu category supports hypothesis-driven investigation rather than enforcement or configuration actions.

By contrast:

- \* Enforce is used to apply policy rules and automated controls.
- \* Threat Hunter is focused on proactive hunting using queries and detection pivots.
- \* Configure is used to manage settings, connectors, policies, and integrations.

The CCIS documentation explicitly associates dashboards such as Risk Analysis and Event Analysis with the Explore menu, emphasizing its role in understanding why risk exists before taking action. Therefore, Option A (Explore) is the correct and verified answer.

#### NEW QUESTION # 56

.....

Everyone wants to have a good job and decent income. But if they don't have excellent abilities and good major knowledge they are hard to find a decent job. Passing the test IDP certification can make you realize your dream and find a satisfied job. Our IDP study materials are a good tool that can help you pass the IDP Exam easily. You needn't spend too much time to learn it. Our IDP exam guide is of high quality and if you use our product the possibility for you to pass the IDP exam is very high as 99% to 100%.

**IDP Test Practice:** <https://www.prepawayete.com/CrowdStrike/IDP-practice-exam-dumps.html>

- [illegible]