CrowdStrike Certified Identity Specialist (IDP) Exam Preparation Guide

To earn CrowdStrike certification, you do not need to become an identity engineer. You must show that you can use CrowdStrike Falcon, CrowdStrike identity protection, and identity threat protection to recognise, investigate, and contain attacks on accounts and access. This is the shortest reliable route.

What the CrowdStrike certification actually tests

The credential is the **CrowdStrike Certified Identity Specialist (CCIS)**; this guide calls it IDP. CrowdStrike's published blueprint uses **60 computer-based, multiple-choice questions**, **90 minutes**, and a **70% overall pass mark**. Questions are timed and scenario-based.

The published score split is:

- CrowdStrike identity protection: **30%**
- Identity threat detection and response: **30%**
- Identity threat hunting: **20%**
- Identity security operations: **20%**

If you fail, you receive a performance report but no credential. Retakes follow current terms, including any waiting period or fee; check them before booking. The report shows which objectives need work.

Knowledge areas: what you must be able to do

CrowdStrike identity protection (30%)

You must explain how identities, policies, sign-ins, and controls work together. Know single sign-on (SSO), multi-factor authentication (MFA), least privilege (minimum necessary access), and risky application grants. Example: choose a control for a cloud administrator who grants an unapproved application powerful access.

Identity threat detection and response (30%)

You must triage a Falcon identity alert, correlate account activity with other records, contain the threat, and preserve evidence. Example: given stolen sign-in sessions, decide whether to revoke access, isolate a device, reset credentials, or combine those actions.

Identity threat hunting (20%)

You must form a hypothesis, search identity and device activity, and move across related events to prove or disprove it. Example: contrast legitimate administrator behaviour with a compromised account registering a new MFA method.

Identity security operations (20%)

You must prioritise alerts, record evidence and actions, choose a response, and escalate or close consistently. Example: decide whether an alert after an approved access change is a false positive—legitimate activity—and what proves it.

Traps that quietly cost marks

Four costly mistakes

- **Confusing identity protection with endpoint security.** This produces the wrong control: one manages users, accounts, sessions, and access; the other protects computers and phones.
- **Memorising menus without workflows.** You lose cause-and-effect items because you know where to click, not why the action fits.
- **Containing before establishing scope.** You may destroy evidence or miss another affected account.
- **Ignoring baselines.** You may mislabel legitimate administrator behaviour or miss an account takeover.

Each can cost several scenario items; wrong answers simply lose the credit for those items.

A realistic study plan

An eight-week route at 7–9 hours a week

1. **Weeks 1–2:** Learn identity fundamentals and CrowdStrike identity protection. Use CrowdStrike training; make a one-page architecture map.
2. **Weeks 3–4:** Drill detection and response. Together they carry 60%, so give them the most study time.
3. **Week 5:** Practise hunting by stating a hypothesis, listing expected evidence, and checking it.
4. **Week 6:** Cover operations, records, escalation, integrations, and weak objectives.
5. **Weeks 7–8:** Take mixed sets under time pressure. From week 3, do two timed blocks weekly; from week 7, one full simulation weekly. Log every miss and the correct rule.

The final 48 hours

Revise, practise, then stop

Revise the weights, detection and response steps, policy logic, and error log. Do one timed set and analyse it. Skip obscure menus, unblueprinted details, and new material. Protect sleep; fatigue causes more mistakes than a final night of reading.

Conclusion and FAQ

Conclusion

Master the workflow, not the interface. CrowdStrike certification rewards you for connecting identity threat protection, Falcon records, detection, response, and hunting. If you can explain why each action fits, you are ready.

Frequently asked questions

Is it beginner-level? No; it assumes basic security operations and identity concepts.

Do I need administrator experience? Helpful, but the exam tests applied judgement.

Can I pass by memorising? No; scenario questions punish guesswork without workflow.

How many can I miss? With 60 equally weighted questions, 42 correct gives 70%.

What if I fail? You receive a score report; review weak objectives, then follow the current retake policy.

Do I need a home lab? No, although hands-on practice makes unfamiliar workflows easier to reason about.

How much study time is enough? Eight weeks at 7–9 hours weekly is a sound target, not a promise.

CrowdStrike

IDP Exam

CrowdStrike Certified Identity Specialist (CCIS) Exam

Thank you for Downloading IDP exam PDF Demo

You can also try our IDP Full Version Download

https://www.certkillers.net/Exam/IDP

Version: 4.0

Question: 1

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

A. Timeline

B. Activity

C. Asset

D. Risk

Answer: D

Explanation:

In CrowdStrike Falcon Identity Protection, the Risk tab within a user or account entity provides administrators with direct visibility into why an account has a specific risk score and what actions can be taken to reduce that score. This functionality is a core component of the User Assessment and Risk Assessment sections of the CCIS (CrowdStrike Identity Specialist) curriculum.

The Risk tab aggregates both analysis-based risks and detection-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 the severity, likelihood, and consequence of each risk factor, allowing administrators 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. The Timeline tab focuses on chronological events and detections, the Activity tab displays authentication and behavioral activity, and the Asset tab shows associated endpoints and resources. Only the Risk tab is designed to explain risk drivers and guide remediation, making Option D the correct and verified answer.

Question: 2

Which of the following is NOT a default insight but can be created with a custom insight?

A. Using Unmanaged Endpoints

B. GPO Exposed Password

C. Compromised Password

D. Poorly Protected Accounts with SPN

Answer: D

Explanation:

In Falcon Identity Protection, default insights are prebuilt analytical views provided by CrowdStrike to immediately highlight common and high-impact identity risks across the environment. These default insights are automatically available in the Risk Analysis and Insights areas and are designed to surface well-known identity exposure patterns without requiring customization.

Examples of default insights include Using Unmanaged Endpoints, GPO Exposed Password, and Compromised Password. These insights are natively provided because they represent frequent and high-risk identity attack vectors such as credential exposure, unmanaged authentication sources, and password compromise, all of which directly contribute to elevated identity risk scores.

Poorly Protected Accounts with SPN (Service Principal Name), however, is not provided as a default insight. While Falcon Identity Protection does collect and analyze SPN-related risk signals—such as Kerberoasting exposure and weak service account protections—this specific grouping must be created by administrators using custom insight filters. Custom insights allow teams to define precise conditions, combine attributes (privilege level, SPN presence, password age, MFA status), and tailor risk visibility to their organization's threat model.

This distinction is emphasized in the CCIS curriculum, which explains that custom insights extend beyond default coverage, enabling deeper, organization-specific identity risk analysis. Therefore, Option D is the correct answer.

Question: 3

In the Predefined Reports Subject dropdown, which category is associated with endpoints?

A. Insights

B. Events

C. Incidents

D. Accounts

Answer: B

Explanation:

Within Falcon Identity Protection, Predefined Reports allow administrators to generate standardized reports based on specific data subjects. The Subject dropdown determines the type of data the report will be built from, such as identity risks, authentication activity, or endpoint-related telemetry.

The category associated with endpoints in the Subject dropdown is Events. Endpoint-related data—such as authentication attempts, logons, protocol usage, and domain controller–observed activity—is captured and represented as events within Falcon. These events form the foundational telemetry used for identity detections, investigations, and reporting.

By contrast:

Insights represent aggregated analytical findings derived from events.

Incidents group multiple detections into a single investigative narrative.

Accounts focus on identity entities such as users and service accounts.

Endpoint visibility in reporting is therefore tied directly to Events, as events reflect the raw and enriched activity observed on endpoints and domain controllers. This structure aligns with Falcon's identity-first security model, where endpoint-observed authentication behavior feeds identity risk scoring and Zero Trust decisions.

The CCIS curriculum explicitly associates endpoint-related reporting with the Events subject, making Option B the correct and verified answer.

Question: 4

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

A. Enforce

B. Threat Hunter

C. Explore

D. Configure

Answer: C

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 C (Explore) is the correct and verified answer.

Question: 5

What trigger will cause a Falcon Fusion Workflow to activate from Falcon Identity Protection?

A. New endpoint detection

B. New incident

C. Alert > Identity detection

D. Spotlight user action > Host

Answer: C

Explanation:

Falcon Fusion workflows integrate directly with Falcon Identity Protection through identity-based

triggers, allowing automated responses to identity threats. The correct trigger that activates a Falcon Fusion workflow from Identity Protection is Alert > Identity detection.

Identity detections are generated when Falcon observes suspicious or malicious identity behavior, such as credential abuse, abnormal authentication patterns, lateral movement attempts, or policy violations related to identity risk. These detections are distinct from endpoint-only detections or incidents and are specifically designed to represent identity-based attack activity.

While New incident and New endpoint detection are valid Falcon Fusion triggers in other Falcon modules, they are not the primary triggers for identity-focused automation. Similarly, Spotlight user action > Host relates to vulnerability management workflows rather than identity analytics.

The CCIS curriculum emphasizes that Falcon Fusion enables automated identity response, such as notifying security teams, disabling accounts, enforcing MFA, or triggering SOAR actions, based on identity detections. Therefore, workflows tied to Alert > Identity detection allow organizations to respond quickly and consistently to identity threats, making Option C the correct answer.

Thank You for trying IDP PDF Demo

To try our IDP Full Version Download visit link below

https://www.certkillers.net/Exam/IDP

Start Your IDP Preparation

[Limited Time Offer] Use Coupon "CKNET" for Further discount on your purchase. Test your IDP preparation with actual exam questions.