CrowdStrike CCIS IDP Practice Questions

Shared by Gill on 22-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

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

Answer:

D

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 an application identifier (Client/Application ID) and secret keys to 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.

Question 2

Question Type: MultipleChoice

Within Domain Security Overview, what Goal incorporates all risks into one security assessment report?

Options:

A- Pen Testing
B- AD Hygiene
C- Reduce Attack Surface
D- Privileged User Management

Answer:

C

Explanation:

Within the Domain Security Overview, Goals are used to tailor how identity risks are grouped, evaluated, and reported. The Reduce Attack Surface goal is the only option that incorporates all identity risks into a single, comprehensive security assessment.

The CCIS curriculum explains that Reduce Attack Surface provides a holistic view of identity exposure by aggregating risks related to authentication paths, account hygiene, privileges, misconfigurations, and legacy identity weaknesses. This goal is designed for organizations seeking an overall understanding of their identity security posture rather than focusing on a specific domain such as privileged users or directory hygiene.

Other goals are more specialized:

AD Hygiene focuses on directory configuration issues.

Privileged User Management concentrates on high-privilege identities.

Pen Testing aligns more with adversarial simulation than continuous risk assessment.

Reduce Attack Surface aligns directly with Zero Trust principles, helping organizations identify and eliminate unnecessary identity access paths. Therefore, Option C is the correct and verified answer.

Question 3

Question Type: MultipleChoice

Which of the following actions under the Investigate menu will pivot to Falcon Identity Protection from an identity-based detection?

Options:

A- Investigate involved users
B- Search for involved entities in Threat Hunter
C- Search for events in Threat Hunter
D- Investigate involved endpoints

Answer:

B

Explanation:

Falcon Identity Protection integrates directly with Threat Hunter to enable deeper investigation of identity-based activity. According to the CCIS curriculum, selecting Search for involved entities in Threat Hunter allows analysts to pivot from an identity-based detection into Threat Hunter while preserving identity context.

This pivot enables analysts to examine related users, service accounts, endpoints, and authentication behavior using advanced queries and timelines. Importantly, this action maintains the identity-centric investigation flow, bridging detections with broader hunting capabilities.

The other options do not perform this specific pivot:

Investigating users or endpoints remains within entity views.

Searching for events in Threat Hunter does not preserve entity context.

Because Search for involved entities in Threat Hunter is the correct pivot action, Option B is the verified answer.

Question 4

Question Type: MultipleChoice

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

Options:

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

Answer:

C

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.

Question 5

Question Type: MultipleChoice

Which of the following MFA providers are NOT supported by Falcon Identity?

Options:

A- Firebase
B- Azure (Entra) MFA
C- Symantec VIP
D- DUO

Answer:

A

Explanation:

Falcon Identity Protection integrates with a defined set of supported MFA providers to enforce identity verification and conditional access based on identity risk. According to the CCIS curriculum, supported MFA providers include Azure (Entra) MFA, Cisco Duo, and Symantec VIP, which are commonly used enterprise-grade MFA solutions.

These integrations allow Falcon Identity Protection to evaluate authentication attempts and dynamically enforce MFA challenges when risky behavior is detected. The supported providers expose the necessary APIs and authentication workflows required for Falcon to trigger MFA challenges as part of Policy Rules and Zero Trust enforcement.

Firebase is not a supported MFA provider within Falcon Identity Protection. Firebase is primarily a mobile and application development platform and does not function as an enterprise MFA provider compatible with Falcon's identity enforcement model. As such, it cannot be used to enforce conditional access or identity verification through Falcon Identity Protection.

Because Falcon only supports specific, enterprise MFA integrations validated by CrowdStrike, Option A is the correct and verified answer.

Question 6

Question Type: MultipleChoice

When creating an API client, which scope with Write permissions must be enabled prior to using Identity Protection API?

Options:

A- Identity Protection Assessment
B- Identity Protection Health
C- There is no need for Write permissions in order to use IDP API
D- Identity Protection GraphQL

Answer:

D

Explanation:

To interact with Falcon Identity Protection using GraphQL, the API client must be created with the appropriate permission scopes. According to the CCIS curriculum, the Identity Protection GraphQL scope with Write permissions must be enabled prior to using the Identity Protection API.

This scope allows the API client to execute GraphQL queries and mutations related to identity detections, incidents, users, and risk data. Even when performing read-only operations, CrowdStrike requires the GraphQL Write scope to authorize GraphQL query execution within the Falcon platform.

The other options are incorrect because:

Identity Protection Assessment and Health are read-only data scopes.

The statement that Write permissions are not required is explicitly false per CCIS documentation.

Because GraphQL access requires the Identity Protection GraphQL (Write) scope, Option D is the correct and verified answer.

Question 7

Question Type: MultipleChoice

Which of the following would cause an identity-based incident type to change?

Options:

A- An exclusion added to the incident
B- A user linked detections to the incident in the console
C- A user changed the incident type in the console
D- Detections related to the incident

Answer:

D

Explanation:

In Falcon Identity Protection, identity-based incidents are dynamic and can evolve over time as additional detections are associated with them. According to the CCIS curriculum, an incident's

type is automatically recalculated based on the detections related to the incident, not by manual user actions.

As new identity-based detections are generated---such as credential misuse, lateral movement attempts, or abnormal authentication behavior---the platform continuously reassesses the incident. If the newly added detections indicate a different or more severe attack pattern, Falcon may automatically change the incident type to better reflect the observed threat activity.

Manual actions such as adding exclusions or linking detections do not directly change the incident type. Similarly, users cannot manually override an incident's classification. The classification logic is driven entirely by Falcon's analytics engine to ensure consistent, objective threat categorization.

This automated behavior is emphasized in CCIS training to highlight Falcon's ability to adapt incident context as attacks progress, making Option D the correct answer.

Question 8

Question Type: MultipleChoice

Refer to exhibit.



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

Options:

A- The user was found logging into five endpoints
B- The user has endpoints that they are considered owners of
C- The user has a risk score of 6.4

D- The user has recent logon activity on ETIS-WS03

Answer:

B

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.

Question 9

Question Type: MultipleChoice

Which option can be selected from the Threat Hunter menu to open the current Threat Hunter query in a new window as Graph API format?

Options:

A- Export to API Builder
B- Save as Custom Query
C- Save as Custom Report
D- Open Query in API Builder

Answer:

D

Explanation:

Falcon Threat Hunter provides a direct integration with the API Builder to support advanced investigation workflows and automation. According to the CCIS curriculum, analysts can take an existing Threat Hunter query and convert it into a GraphQL-compatible format by selecting Open Query in API Builder from the Threat Hunter menu.

This option opens the current query in a new window within API Builder, automatically translating the query structure into GraphQL syntax where applicable. This enables security teams to reuse validated hunting logic for automation, reporting, or external integrations without rewriting queries from scratch.

The other menu options serve different purposes:

Export to API Builder is not a valid menu action.

Save as Custom Query stores the query for reuse inside Threat Hunter.

Save as Custom Report generates a reporting artifact, not an API query.

Because Open Query in API Builder is the only option that opens the query in GraphQL format in a new window, Option D is the correct and verified answer.

Question 10

Question Type: MultipleChoice

Which option best is NOT a default insight but can be created with a custom insight?

Options:

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 11

Question Type: MultipleChoice

Where would a Falcon administrator enable authentication traffic inspection (ATI) for Domain Controllers?

Options:

A- Identity configuration policies
B- Identity management settings
C- Identity detection configuration
D- Identity protection settings

Answer:

A

Explanation:

Authentication Traffic Inspection (ATI) is a foundational capability of Falcon Identity Protection that enables the platform to analyze authentication traffic from domain controllers. According to the CCIS documentation, ATI is enabled through Identity configuration policies.

Identity configuration policies define how the Falcon sensor captures and inspects authentication-related traffic, including Kerberos, NTLM, LDAP, and other identity protocols. Enabling ATI at this level ensures that domain controllers provide the necessary telemetry for identity risk analysis, detections, and behavioral profiling.

The other options are incorrect because:

Identity management settings focus on identity governance and administration.

Identity detection configuration controls detection logic, not traffic inspection.

Identity protection settings manage high-level configuration but do not directly enable ATI.

Because ATI must be explicitly enabled via Identity configuration policies, Option A is the correct and verified answer.

Question 12

Question Type: MultipleChoice

Which of the following users would most likely have a HIGH risk score?

Options:

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

Answer:

B

Explanation:

Falcon Identity Protection calculates user risk scores based on a combination of privilege level, credential exposure, and behavioral indicators. According to the CCIS curriculum, a privileged user with a compromised password represents 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.

Because credential compromise combined with privilege dramatically increases attack potential, Option B is the correct and verified answer.

Question 13

Question Type: MultipleChoice

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

Options:

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

Answer:

A

Explanation:

Falcon Identity Protection supports geolocation-based detections 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.

To Get Premium Files for IDP Visit

https://www.p2pexams.com/products/idp

For More Free Questions Visit

https://www.p2pexams.com/crowdstrike/pdf/idp

