PassQueen
a.k.a dumpsqueen.com

CrowdStrike Certified Identity Specialist(CCIS) Exam

CrowdStrike IDP

Version Demo

Total Demo Questions: 7

Total Premium Questions: 77

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

Which CrowdStrike documentation category would you search to find GraphQL examples?

A. CrowdStrike APIs

B. Threat Intelligence

C. XDR

D. Identity Protection APIs

ANSWER: D

Explanation:

Identity Protection APIs is the appropriate documentation category for GraphQL examples. CrowdStrike Identity Protection exposes capabilities and identity-related data through its API documentation, including GraphQL-oriented material for constructing queries and working with the identity data model. When looking for query syntax, example requests, fields, filters, variables, or guidance on retrieving identity-protection data programmatically, start within this product-specific API category rather than a general documentation area. This organization helps administrators and developers quickly locate content that applies to Falcon Identity Protection integrations and automation workflows. CrowdStrike's documentation portal provides the product documentation entry point at docs.crowdstrike.com. For background on the query language and its conventions, including queries, variables, and schemas, see the official GraphQL learning documentation. Using the Identity Protection APIs category ensures that the examples and schema context match the CrowdStrike identity functionality being integrated.

QUESTION NO: 2

The configuration of the Azure AD (Entra ID) Identity-as-a-Service connector requires which three pieces of information?

A. Tenant Domain, Token, Configuration File

B. Tenant Domain, Client Secret, User Identifier

C. Tenant Domain, Application ID, Scope

D. Tenant Domain, Application ID, Application Secret

ANSWER: D

Explanation:

Tenant Domain, Application ID, Application Secret is correct because these values identify the Microsoft Entra tenant and provide the application identity Falcon Identity Protection uses to establish authenticated API access to the Identity-as-a-Service provider. The tenant domain specifies the Entra ID directory associated with the organization. The Application ID is the client identifier assigned when the integration application is registered in Entra ID. The Application Secret is the confidential client credential created for that registered application and is used with the application identifier to obtain tokens securely through Microsoft identity platform OAuth flows.

This information allows the connector to authenticate as the registered application rather than as an individual user, supporting controlled, auditable integration between Falcon Identity Protection and Entra ID. Microsoft documents that an app registration exposes an application (client) ID and that client secrets are credentials used by confidential client applications. Tenant information determines the directory against which the application authenticates. These are therefore the essential configuration values for the connector's Entra ID application-based authentication setup. See Microsoft's guidance on registering an application with the Microsoft identity platform and OAuth 2.0 client credentials flow.

QUESTION NO: 3

When creating an API key, which scope should be selected to retrieve Identity Protection detection and incident information?

A. Identity Protection Detections

B. Identity Protection Incidents

C. Identity Protection Assessment

D. Identity Protection Data

ANSWER: A

Explanation:

Identity Protection Detections is the required API-client scope for retrieving Identity Protection detection records and the incident information associated with those detections. Identity Protection exposes these detection-focused data sets through its API and GraphQL capabilities, so the OAuth2 client credentials used for the query must include the detection permission before Falcon will authorize access. This is important for integrations such as SIEM ingestion, case-management enrichment, reporting, and automated response workflows, where the client needs to query identity-related detection attributes and their related incident context.

When creating the API key in Falcon, select the read permission for Identity Protection Detections and use that key's client ID and secret to obtain an access token. The resulting token carries the scope required by Identity Protection API authorization checks. Detection records provide the core security event data, while their incident relationships and metadata enable an integration to correlate activity into the appropriate identity-security investigation context. CrowdStrike's API documentation portal provides the authoritative endpoint and OAuth scope details, and the official FalconPy project demonstrates authenticated use of Falcon APIs: CrowdStrike API Documentation and CrowdStrike FalconPy.

QUESTION NO: 4

Which of the following Falcon roles **CANNOT** enable and disable policy rules?

A. Identity Protection Domain Administrator

B. Identity Protection Administrator

C. Identity Protection Policy Manager

D. Falcon Administrator

ANSWER: A

Explanation:

Identity Protection Domain Administrator is the role that cannot enable or disable Identity Protection policy rules. This role is intended for delegated administration of an assigned Active Directory domain, allowing administrators to work with domain-specific Identity Protection information and configuration within their authorized scope. It does not grant the policy-management privilege required to change the operational state of a policy rule.

Enabling or disabling a rule changes whether Falcon Identity Protection actively evaluates the rule and can apply its configured identity-protection response. Because this action can directly affect enforcement across identities and authentication activity, CrowdStrike separates it from domain-scoped administrative responsibilities and reserves it for roles with policy-management or broader Falcon administrative permissions. This RBAC separation supports least-privilege administration: a user can administer relevant domain resources without being able to activate, deactivate, or otherwise control the enforcement status of policy rules.

For general product and identity-security context, see CrowdStrike's Falcon Identity Protection overview and the CrowdStrike Trust Center.

QUESTION NO: 5

How does CrowdStrike Falcon Identity Protection help customers identify different types of accounts in their domain?

A. Implements advanced encryption algorithms for account metadata

B. Assigns a human authorizer to each programmatic account for approval

C. Analyzes authentication traffic and automatically classifies programmatic and human accounts

D. Conducts regular vulnerability assessments on programmatic accounts

ANSWER: C

Explanation:

Analyzes authentication traffic and automatically classifies programmatic and human accounts is correct because Falcon Identity Protection continuously evaluates identity and authentication activity to build context about accounts in an organization's identity environment. Its identity-protection capabilities use behavioral analysis of authentication patterns and account activity to distinguish interactive user behavior from the consistent, non-interactive patterns commonly associated with service and other programmatic accounts. This automatic account classification gives security teams useful visibility without relying solely on manually maintained account labels, which can be incomplete or become outdated.

Accurately identifying account type improves identity-risk analysis because human and programmatic accounts have different normal behaviors, permissions, credential lifecycles, and operational purposes. Falcon Identity Protection can use this context to better prioritize suspicious identity activity, investigate anomalous authentications, and help teams understand where privileged or service-account exposure exists. CrowdStrike describes Falcon Identity Protection as providing continuous visibility and detection across identity systems, while its documentation highlights identity and access behavior analytics as a core capability. See the CrowdStrike Falcon Identity Protection overview and the CrowdStrike identity threat detection and response resource.

QUESTION NO: 6

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

A. Firebase

B. Azure (Entra) MFA

C. Symantec VIP

D. DUO

ANSWER: A

Explanation:

Firebase is the correct selection because it is not an enterprise MFA provider integration supported by Falcon Identity Protection. Firebase is Google's application-development platform, providing services such as application hosting, databases, analytics, and application authentication capabilities. Although Firebase Authentication can implement multifactor authentication within an application that a developer builds, it is not an identity-provider MFA integration used by Falcon Identity Protection for enterprise identity-risk response.

Falcon Identity Protection is designed to detect identity-based attacks and coordinate enforcement through supported enterprise identity and MFA ecosystems. Its MFA-related integrations enable organizations to apply step-up authentication or otherwise respond to risky identity activity using established enterprise authentication services. This requires a supported integration and the associated administrative configuration, permissions, and policy setup; an application-development service alone does not provide that integration path. CrowdStrike describes Falcon Identity Protection as a platform for detecting and stopping identity threats across the enterprise identity environment, including enforcing risk-based controls through integrated identity tooling.

For product context and supported identity-protection capabilities, see CrowdStrike Falcon Identity Protection. Firebase's MFA functionality is documented as an application-authentication feature by Firebase Authentication documentation.

QUESTION NO: 7

A security team wants to identify service accounts with service principal names that also meet the organization's definition of weak protection. The team needs a focused view that combines these conditions rather than relying only on prebuilt insights. What should the administrator create?

A. A detection exclusion

B. A custom insight

C. A Policy Rule

D. A geolocation blocklist

ANSWER: B

Explanation:

A custom insight is correct. A custom insight can combine account attributes and risk context to identify conditions such as poorly protected accounts with SPNs. This helps the team focus on service accounts that may warrant review for Kerberoasting exposure or inadequate account protection.

A detection exclusion suppresses known benign activity, and a Policy Rule defines an enforcement response rather than creating an organization-specific analytical view.