KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **IDP**

Title : CrowdStrike Certified Identity Specialist

Version : DEMO

1.An account without a phone number, operating system, or role of CEO would typically be defined as:
A. Programmatic
B. Human
C. Enterprise
D. Corporate
Answer: A
Explanation:
Falcon Identity Protection classifies accounts based on observed authentication behavior and associated identity attributes, not solely on naming conventions. According to the CCIS curriculum, programmatic accounts (such as service accounts or application accounts) typically lack human-centric attributes like a phone number, assigned operating system, job title, or executive role (for example, CEO).
Human accounts generally have enriched identity context sourced from directory services and identity providers, including user profile details, interactive login behavior, and endpoint associations. In contrast, programmatic accounts authenticate non-interactively, often on predictable schedules, and do not require personal attributes to function.
Falcon analyzes authentication traffic to automatically identify these characteristics and classify the account accordingly. An account missing human identity signals—such as a phone number or endpoint ownership— strongly aligns with programmatic behavior.
Because the absence of personal attributes and interactive context is a defining indicator of a programmatic account, Option A is the correct and verified answer.

2.The CISO of your organization recently read a report about the increased usage of identity brokers and is interested in finding a solution for the company.
Which of the following makes Falcon Identity a valid solution for the organization?
A. Provides the ability to audit and record sessions across multiple methods, such as SSH, RDP, and SMB
B. Falcon Identity is able to be a middleware between Active Directory and a Human Resource Information System (HRIS)
C. Gives the organization the ability to proactively mitigate risks, as well as protect critical Active Directory infrastructure through Policy Rules
D. Allows administrators to store and delegate passwords to application servers
Answer: C
Explanation:
Falcon Identity Protection is designed to address the growing threat of identity brokers, which act as intermediaries that abuse identity infrastructure to facilitate lateral movement, privilege escalation, and persistent access. The CCIS curriculum emphasizes that Falcon Identity Protection provides proactive identity risk mitigation rather than reactive session monitoring or password vaulting.
The platform continuously inspects authentication traffic and identity behavior across Active Directory and Azure AD environments, building behavioral baselines and identifying abnormal activity associated with brokered identity attacks. Through Policy Rules, organizations can automatically enforce controls such as blocking risky authentications, enforcing MFA, or triggering remediation workflows when identity abuse is detected.
The incorrect options describe capabilities associated with Privileged Access Management (PAM) or IAM middleware, which are not the focus of Falcon Identity Protection. Falcon does not record interactive

sessions, act as an HRIS bridge, or store delegated credentials. Instead, it protects identity infrastructure by detecting and preventing identity misuse in real time.
This proactive enforcement model aligns directly with Zero Trust principles and makes Falcon Identity Protection a strong solution against identity broker activity. Therefore, Option Cis the correct and verified answer.

3.Can a specific detection be excluded altogether or just per entity?
A. Only specific entities can be excluded by using the Identity-Based Detection # Detection Exclusion page
B. Only detections can be disabled using the Identity-Based Detection # Detection Exclusion page
C. All detections can be disabled, some detections support excluding entities
D. Adding an exclusion for a detection creates a security hole, therefore a detection cannot be excluded
Answer: C
Explanation:
Falcon Identity Protection provides flexible control over how identity-based detections are handled through the Detection Exclusions framework. According to the CCIS curriculum, administrators can either disable an entire detection type or, where supported, exclude specific entities such as users, service accounts, or endpoints from triggering that detection.
Not all detections support entity-level exclusions. For detections that do, exclusions allow organizations to suppress known benign behavior without disabling the detection globally. This is particularly useful for service accounts or legacy systems that generate expected but non-malicious activity. When entity-level exclusion is not supported, administrators may choose to disable the detection entirely, which stops it from generating alerts across the environment.
The CCIS documentation clearly explains this dual model:
All detections can be disabled, regardless of type
Only some detections support entity-based exclusions
This approach balances operational flexibility with security integrity and avoids the misconception that exclusions automatically create security gaps.
Therefore, Option Cis the correct and verified answer.

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

5.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:
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 Ais the correct and verified answer.