

CrowdStrike CrowdStrike- Certified-Identity-Specialist

CrowdStrike Certified Identity Specialist (CCIS)

**Thank You for Downloading CrowdStrike-Certified-Identity-
Specialist Updated Exam Questions**

<https://certs4sale.com/CrowdStrike/crowdstrike-certified-identity-specialist-pdf-exam-dumps>

Question: 1

Which of the following best describes the key difference between Falcon Identity Protection's log-free detection and traditional Endpoint Detection and Response (EDR) solutions?

- A. Falcon Identity Protection is limited to monitoring Active Directory, while traditional EDR solutions monitor a broader range of identity systems.
- B. Falcon Identity Protection leverages behavioral analysis of identity events without requiring endpoint logs, while traditional EDR solutions rely on endpoint activity logs to detect threats.
- C. Falcon Identity Protection exclusively monitors cloud-based identity systems, whereas traditional EDR focuses only on on-premises infrastructure.
- D. Falcon Identity Protection detects identity-based threats only after successful logins, while traditional EDR detects threats during the attack execution stage.

Answer: B

Explanation:

Explanation for each option is given below.

Option A: Falcon Identity Protection supports multiple identity systems, including cloud and hybrid infrastructures. Traditional EDR does not specialize in identity monitoring, so this is an inaccurate comparison.

Option B: Falcon Identity Protection identifies anomalies in identity usage and behavior patterns in real time without relying on traditional log-based data collection. Traditional EDR solutions, on the other hand, monitor endpoint activity through log aggregation and analysis. This makes Falcon Identity Protection particularly effective against advanced identity-based threats like credential theft and lateral movement that may not leave direct traces in endpoint logs.

Option C: While Falcon Identity Protection can monitor cloud and on-premises identity systems (e.g., Active Directory, Azure AD), traditional EDR solutions are also capable of monitoring activities in hybrid environments. The distinction is not about scope but rather the mechanism of threat detection.

Option D: Falcon Identity Protection focuses on detecting anomalies throughout the authentication process, including failed and suspicious login attempts, not just after successful authentication. Traditional EDR also works across various stages of an attack, such as execution and exfiltration.

Question: 2

Which of the following best describes the principle of "continuous validation" in a Zero Trust Architecture?

- A. Continuously monitoring and validating users, devices, and transactions regardless of previous authentication.
- B. Periodically re-authenticating users and devices based on time intervals.
- C. Allowing unlimited access once a user or device is authenticated.
- D. Validating credentials once during login and assuming trust thereafter.

Answer: A

Explanation:

Explanation for each option is given below.

Option A: This aligns with Zero Trust principles, which emphasize ongoing validation of identity, device health, and behavior to ensure secure access.

Option B: While periodic checks are better than none, continuous validation requires ongoing checks in real-time, not just at fixed intervals, to mitigate evolving threats.

Option C: This contradicts the Zero Trust principle of “never trust, always verify.” Continuous validation ensures that access is reassessed dynamically, and unlimited access creates security vulnerabilities if a device is compromised.

Option D: This is characteristic of legacy security models, such as castle-and-moat, which Zero Trust explicitly aims to replace to reduce the risk of lateral movement by attackers.

Question: 3

A company is setting up an Identity-as-a-Service (IDaaS) platform to centralize identity management and streamline Single Sign-On (SSO) for its employees. During configuration, the IT administrator must ensure that applications integrated with the IDaaS platform enforce role-based access control (RBAC). Which configuration step is essential to achieve this?

- A. Require mandatory approval workflows for every new account creation.
- B. Enable adaptive authentication for all users.
- C. Synchronize user attributes and roles from the organization's directory service.
- D. Configure application-specific access rules directly in each application.

Answer: C

Explanation:

Explanation for each option is given below.

Option A: Approval workflows ensure that account creation is monitored, but they do not enforce RBAC within applications after account provisioning.

Option B: Adaptive authentication enhances security by adjusting authentication requirements based on user behavior and context. While useful, it does not directly enforce RBAC for applications.

Option C: Role-based access control (RBAC) requires accurate role and attribute information for users. Synchronizing these attributes from a directory service like Active Directory or Azure AD ensures that applications can enforce access controls based on the user's role.

Option D: While this can enforce access, it defeats the purpose of centralizing management through IDaaS. It also increases administrative overhead and potential misconfigurations.

Question: 4

A security analyst is configuring a workflow in Falcon Fusion for Identity Protection to detect and respond to suspicious user logins from foreign IP addresses. The analyst wants the workflow to trigger only when a login attempt satisfies all of the following conditions:

- The login originates from a country not in the allowlist.
- The login occurs during non-business hours.
- The user belongs to a specific Active Directory (AD) group.

Which set of conditions should the analyst configure in Falcon Fusion to achieve this?

- A. (Login Country = NOT IN [Allowlist]) OR (Time = Non-Business Hours) OR (AD Group = Specific Group)
- B. (Login Country = IN [Allowlist]) OR (Time = Non-Business Hours) AND (AD Group = Specific Group)
- C. (Login Country = NOT IN [Allowlist]) AND (Time = Non-Business Hours) AND (AD Group = Specific Group)
- D. (Login Country = IN [Allowlist]) AND (Time = Business Hours) AND (AD Group = Any Group)

Answer: C

Explanation:

Explanation for each option is given below.

Option A: Using OR for all conditions causes the workflow to trigger if any single condition is met, defeating the requirement for all conditions to be satisfied.

Option B: The OR operator between (Login Country = IN [Allowlist]) and (Time = Non-Business Hours) creates an overly permissive condition, allowing the workflow to trigger even if the login is from an allowed country.

Option C: This condition combines all three criteria using logical AND operators, ensuring the workflow triggers only if all specified conditions are met: the login originates from an unallowed country, occurs during non-business hours, and involves a user in the specified AD group.

Option D: This condition fails on multiple levels: it uses IN [Allowlist] instead of NOT IN [Allowlist] for the country and allows any AD group rather than the specified group.

Question: 5

A security analyst at your organization is reviewing the Risk Score for a domain, which is flagged as high risk in CrowdStrike's Identity Protection Dashboard. The analyst wants to understand what this Risk Score represents and how it is calculated to prioritize mitigation efforts. You are tasked with explaining the significance of this score. What does the Risk Score for a domain represent in the context of CrowdStrike Identity Protection?

- A. The effectiveness of the domain's firewall policies in blocking external threats.
- B. The aggregated measure of vulnerabilities, misconfigurations, and suspicious activity associated

- C. The likelihood that the domain's Active Directory will experience a breach within the next 30 days.
- D. The percentage of endpoints within the domain that are currently unprotected by endpoint detection and response (EDR) solutions.

Answer: B

Explanation:

Explanation for each option is given below.

Option A: Firewall policies address external threats, whereas the Risk Score evaluates identity-related risks, which include internal misconfigurations and vulnerabilities.

Option B: The Risk Score represents a comprehensive evaluation of the domain's security posture in terms of identity infrastructure. It takes into account factors such as exposed vulnerabilities, risky configurations, and detected identity-related threats. This helps organizations prioritize mitigation efforts effectively. Common misconceptions include thinking it's focused only on external threats or endpoint-specific issues, which are incorrect.

Option C: While the Risk Score helps identify domains at higher risk, it does not predict specific timelines for breaches. It is an indicator of overall risk, not a probabilistic forecast.

Option D: The Risk Score focuses on identity security, not endpoint protection. Though endpoint security contributes to overall domain safety, it is not the primary factor in calculating the Risk Score.

Question: 6

Your organization has recently experienced a series of phishing attacks targeting users in multiple domains. You are tasked with updating the "Goal" in the Domain Security Overview of CrowdStrike's Identity Protection platform to better address this threat. Which goal should you select?

- A. Ensure Secure Privileged Access
- B. Strengthen Kerberos Encryption
- C. Enhance Password Hygiene
- D. Detect Suspicious Authentication Activity

Answer: D

Explanation:

Explanation for each option is given below.

Option A: This goal focuses on securing high-privilege accounts and limiting their misuse. While valuable, it does not directly address the broader need to monitor authentication patterns across the organization to identify phishing-related activities.

Option B: While improving Kerberos encryption enhances security, it is more relevant for securing ticket exchanges in the authentication process. This goal does not specifically target phishing or the misuse of credentials obtained through phishing.

does not address the immediate need to detect suspicious authentication activity resulting from phishing.

Option D: Detecting suspicious authentication activity is crucial for identifying anomalous behaviors, such as unauthorized access attempts or patterns that align with phishing-related credential misuse. This goal focuses on flagging and mitigating unusual authentication events, which are common after successful phishing attacks. It aligns directly with the need to monitor and react to authentication anomalies caused by phishing threats.

Question: 7

Your organization has deployed CrowdStrike Falcon to monitor activity on its domain controllers (DCs). As a security analyst, you need to confirm that each DC in your domain is correctly configured and visible in the Falcon Console. You also want to ensure reporting on endpoints managed by each DC. What steps should you take to verify visibility and reporting for your domain controllers?

- A. Check the Domain Controllers tab in the Falcon Console to verify each DC's reporting status and associated endpoints.
- B. Use the Threat Hunting module to create a custom query that tracks all login events across your domain controllers.
- C. Go to the Endpoint Management tab, filter by operating system, and manually match domain controller activity to endpoint logs.
- D. Install a separate monitoring agent on each domain controller and check their status in the third-party management tool.

Answer: A

Explanation:

Explanation for each option is given below.

Option A: This is the correct answer. The Falcon Console includes a dedicated view to monitor the health, reporting status, and endpoints associated with each domain controller, providing direct visibility into the DCs.

Option B: This is partially correct but not sufficient. Threat Hunting queries can identify specific events but do not provide a comprehensive view of DC reporting and associated endpoints.

Option C: This is incorrect because while endpoint logs may contain relevant data, the Falcon Console provides specific tools for monitoring DCs directly without manual matching.

Option D: This is incorrect because CrowdStrike Falcon does not require a separate monitoring agent for domain controllers; the Falcon agent covers this functionality.

Question: 8

While attempting to upload a custom list of compromised passwords to the CrowdStrike Falcon Identity Protection portal, you encounter an error stating: "File format not supported." You must troubleshoot and reformat the file to ensure successful upload. Which of the following steps will most likely resolve the error and allow the file to be uploaded successfully?

- A. Convert the file to a compressed .zip format and re-upload it.
- B. Ensure the file is encoded in UTF-8 and saved as a .txt file with one password per line.
- C. Include usernames associated with each password in a separate column.
- D. Remove special characters and numbers from the passwords in the file.

Answer: B

Explanation:

Explanation for each option is given below.

Option A: This is incorrect because CrowdStrike does not require or support compressed files for custom password list uploads. The platform expects plaintext or specific formats for direct integration.

Option B: This is correct because CrowdStrike typically requires custom password lists to be uploaded in a specific format. The most common supported format is a UTF-8 encoded .txt file, with each password on a new line. Ensuring these formatting requirements are met resolves most upload errors.

Option C: This is incorrect because the custom password list is designed to assess passwords against all accounts universally, without mapping specific passwords to usernames.

Option D: This is incorrect because the presence of special characters and numbers does not affect the file's compatibility. Removing these elements would unnecessarily alter the intended security checks.

Question: 9

A financial institution notices an unusual pattern of access involving privileged accounts. The security team asks you to generate a custom insight to track all privileged account logins flagged as medium or high risk. Additionally, they want to exclude logins from known IP ranges such as internal office networks. Which steps would you take to generate this custom insight?

- A. Navigate to the "Settings" tab, configure a policy that prevents privileged accounts from logging in from unknown IP ranges.
- B. Navigate to the "Threat Graph", create a query for privileged account activity, and exclude internal IP ranges using a custom rule.
- C. Use the "Insights" tab, select "New Insight", and filter logins by medium or high risk. Add a secondary filter to exclude known IP ranges.
- D. Go to the "Activity" tab, apply a filter for privileged account logins, and sort by risk level. Manually exclude known IP ranges by exporting the data.

Answer: C

Explanation:

Explanation for each option is given below.

Option A: Configuring policies in the "Settings" tab affects system behavior but does not generate custom insights. This step addresses prevention, not risk analysis.

Option B: The "Threat Graph" is useful for visualizing threats but not ideal for creating reusable custom

Option C: The "Insights" tab is specifically designed to create new custom insights. Applying a risk level filter and excluding specific IP ranges ensures that the generated report meets the organization's requirements.

Option D: Manually excluding IP ranges after exporting data is a time-consuming process. The "Insights" tab provides built-in options to automate this filtering.

Question: 10

An enterprise wants to integrate their Identity-as-a-Service (IDaaS) provider with CrowdStrike Identity Protection to enable streamlined identity management and MFA. Which of the following IDaaS platforms is supported for integration with CrowdStrike Identity Protection?

- A. OneLogin
- B. Okta
- C. Amazon Cognito
- D. CyberArk

Answer: B

Explanation:

Explanation for each option is given below.

Option A: OneLogin, though popular in the IDaaS market, is not a supported integration partner for CrowdStrike Identity Protection.

Option B: Okta is a widely supported IDaaS provider for integration with CrowdStrike Identity Protection. It enables seamless SSO and MFA, making it a preferred choice for organizations leveraging CrowdStrike.

Option C: Amazon Cognito is a robust IDaaS service from AWS but is not currently listed as a supported connector for CrowdStrike Identity Protection.

Option D: CyberArk is primarily focused on privileged access management and is not considered an IDaaS provider. Therefore, it is not a supported connector for CrowdStrike Identity Protection.

THANK YOU FOR DOWNLOADING CROWDSTRIKE-CERTIFIED-IDENTITY- SPECIALIST UPDATED EXAM QUESTIONS

Note: Thanks For Trying The Demo Of Our CrowdStrike-Certified-Identity-Specialist Exam Product

Visit Our Site to Purchase the Full Set of Actual CrowdStrike-Certified-Identity-Specialist Exam Questions With Answers.

Money Back Guarantee



Click The Link Below

<https://certs4sale.com/CrowdStrike/crowdstrike-certified-identity-specialist-pdf-exam-dumps>