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 : **CCCS-203b**

Title : CrowdStrike Certified Cloud Specialist - 2025 Version

Version : DEMO

1.What is the primary advantage of using the Falcon Kubernetes Sensor in a containerized cloud environment?
A. It does not support managed Kubernetes services like EKS or GKE.
B. It eliminates the need for a kernel-based agent on each node.
C. It can directly monitor container registries for vulnerabilities.
D. It only works in on-premise Kubernetes environments.
Answer: B
Explanation:
Option A: The Falcon Kubernetes Sensor is designed to integrate seamlessly with managed Kubernetes services such as Amazon EKS, Google GKE, and Azure AKS, providing runtime protection for containers in these environments.
Option B: The Falcon Kubernetes Sensor operates as a privileged container and does not rely on installing a kernel module on each node. This is particularly beneficial in environments where kernel-level changes are restricted, such as managed Kubernetes services. This approach simplifies deployment and enhances compatibility.
Option C: While Falcon can provide container security and vulnerability management through other components like Falcon Container, the Kubernetes Sensor itself focuses on runtime protection within Kubernetes clusters, not direct monitoring of registries.
Option D: The Falcon Kubernetes Sensor works in both cloud-based and on-premise Kubernetes environments, making it a flexible solution for diverse deployment scenarios.

2.A company using CrowdStrike Falcon Cloud Security wants to ensure that all container images deployed in their cloud environment are scanned for vulnerabilities before deployment.
Which image assessment policy should they implement?
A. Enforce pre-deployment scanning to block images with critical vulnerabilities from being deployed.
B. Allow all container images to be deployed, regardless of vulnerabilities, but notify administrators if an image contains high-severity vulnerabilities.
C. Only assess images manually when security teams request a scan.
D. Enable post-deployment scanning to assess vulnerabilities after an image has already been running in production.
Answer: A
Explanation:
Option A: Pre-deployment scanning with enforcement ensures that only secure images are deployed, blocking those with critical vulnerabilities. This helps mitigate security risks before they reach production.
Option B: While notifying administrators about vulnerabilities is useful, allowing all images regardless of severity increases risk by deploying insecure workloads.
Option C: Relying on manual assessments makes security processes inefficient and inconsistent, leading to gaps in protection.
Option D: Post-deployment scanning is useful for continuous monitoring, but it does not prevent vulnerable images from being deployed in the first place.

3.Which of the following best describes the process of identifying unassessed images in production using CrowdStrike Falcon?
A. Use the Falcon console to generate a report from the Image Assessment dashboard.

B. Deploy a custom script to parse container logs for unassessed image information.
C. Configure the runtime protection policy to block all unassessed images from running.
D. Enable auto-deletion of unassessed images directly from the Falcon console.
Answer: A
Explanation:
Option A: The Falcon console includes an Image Assessment dashboard that provides a comprehensive overview of container images in use, including identifying those that have not been scanned. This report helps teams address security gaps proactively.
Option B: While custom scripts might extract relevant details, the Falcon console already provides built-in tools to identify unassessed images more efficiently and accurately.
Option C: Runtime protection policies can prevent the execution of specific images based on policies, but they do not inherently identify or block all unassessed images automatically. Identification requires analysis via the Image Assessment dashboard.
Option D: The Falcon console does not offer an auto-deletion feature for unassessed images. Actions related to unassessed images require manual intervention or automated workflows outside of Falcon.

4.You are reviewing accounts using the CrowdStrike CIEM/Identity Analyzer and need to ensure MFA compliance.
Which account configuration demonstrates proper MFA implementation?
A. An account with no login activity in the last 30 days and no additional authentication factors.
B. An account that uses password authentication and an authenticator app for a one-time password (OTP).
C. An account configured with biometric authentication only.
D. An account that allows users to bypass additional authentication steps on trusted devices.
Answer: B
Explanation:
Option A: The inactivity period and absence of additional authentication factors disqualify this account from demonstrating proper MFA implementation. This account would likely need further review for security compliance.
Option B: This setup meets the definition of MFA, combining two factors: "something you know" (password) and "something you have" (authenticator app). This ensures robust security against unauthorized access.
Option C: While biometric authentication ("something you are") is a strong factor, MFA requires combining at least two different factors. Biometric authentication alone does not meet this standard.
Option D: Allowing bypass of additional steps compromises the integrity of MFA and introduces vulnerabilities. Proper MFA should always require multiple factors, even on trusted devices.

5.Which of the following best describes the difference between managed and unmanaged items in the context of Falcon Cloud Security?
A. Managed items are fully patched systems, while unmanaged items are systems that have pending updates.
B. Managed items refer to accounts or containers with CrowdStrike agents installed, while unmanaged items lack such direct control.
C. Managed items are actively assessed for vulnerabilities, while unmanaged items are not assessed at

all.
D. Managed items are those integrated into the Falcon platform, while unmanaged items are only monitored externally.
Answer: B
Explanation:
Option A: The terms managed and unmanaged do not directly relate to the patching status of systems. Both managed and unmanaged items could be fully patched or have pending updates.
Option B: Managed items refer to accounts or containers where CrowdStrike agents or direct integrations are applied, giving the Falcon platform control and visibility. Unmanaged items, by contrast, lack direct integration, meaning the platform can monitor them but not control them directly. This differentiation is critical for managing risks in hybrid environments.
Option C: Managed and unmanaged items are not defined by their vulnerability assessment status. Even unmanaged items can be assessed for risks through other tools or indirect integrations.
Option D: While managed items are integrated into the Falcon platform, unmanaged items are not merely "externally monitored." The key distinction lies in the presence or absence of direct CrowdStrike agent or integration.