

CrowdStrike CrowdStrike- Certified-Cloud-Specialist

CrowdStrike Certified Cloud Specialist (CCCS)

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

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

Question: 1

Which action should an administrator take after identifying privileged accounts without MFA using the CrowdStrike Identity Analyzer?

- A. Apply conditional access policies to enforce MFA for the accounts.
- B. Revoke all privileges from the affected accounts immediately.
- C. Disable the accounts permanently to prevent unauthorized access.
- D. Manually change the passwords of all identified accounts.

Answer: A

Explanation:

Explanation for each answer is given below.

Option A: Enforcing MFA through conditional access policies ensures that privileged accounts remain secure without disrupting legitimate operations. This approach addresses the identified risk directly and aligns with best practices.

Option B: While revoking privileges could mitigate risks, it is often too disruptive and impractical for operational accounts or critical users. Instead, enforcing MFA is a more balanced and effective solution.

Option C: Permanent account disabling is unnecessary and counterproductive unless there is clear evidence of a security breach. This approach does not address the root cause of missing MFA.

Option D: Changing passwords can enhance security but does not address the lack of MFA, leaving the accounts still vulnerable to unauthorized access. This action alone is not comprehensive.

Question: 2

In the context of Falcon Cloud Security, what is the primary difference between managed/unmanaged items (e.g., accounts or containers) and assessed/unassessed items (e.g., container images)?

- A. Managed items refer to container images with vulnerabilities actively managed by CrowdStrike, while unmanaged items are container images that are no longer in use.
- B. Assessed items are accounts or containers with detected vulnerabilities, while unassessed items are accounts or containers with unknown vulnerabilities.
- C. Managed items are accounts or containers actively monitored by Falcon Cloud Security, whereas unmanaged items are accounts or containers not yet under CrowdStrike monitoring.
- D. Assessed items are container images that have been scanned and evaluated for vulnerabilities, while unassessed items are container images awaiting assessment.

Answer: C

Explanation:

Explanation for each answer is given below.

Option A: Managed/unmanaged items do not refer to container images specifically. This conflates the

The status of being managed/unmanaged pertains to whether the item is actively monitored, not the vulnerability state.

Option B: Assessed/unassessed items relate to whether vulnerability assessment has occurred. This choice incorrectly describes their scope and misapplies the terminology to accounts or containers instead of container images.

Option C: Managed items are accounts or containers actively integrated with and monitored by Falcon Cloud Security. Unmanaged items are those outside the scope of Falcon monitoring, often requiring additional steps to bring them under management. This distinction is fundamental to understanding CrowdStrike's coverage capabilities.

Option D: This explanation accurately describes assessed/unassessed items, not managed/unmanaged items. The former pertains to whether a container image has been scanned for vulnerabilities.

Question: 3

What is the primary purpose of the CrowdStrike Cloud Infrastructure Entitlement Manager (CIEM) feature in a cloud environment?

- A. Managing encryption keys for sensitive cloud storage
- B. Managing cloud infrastructure costs by monitoring usage and recommending cost-saving strategies
- C. Automating the deployment of cloud resources across multi-cloud environments
- D. Enforcing least-privilege access by identifying and remediating excessive permissions

Answer: D

Explanation:

Explanation for each answer is given below.

Option A: Key management is typically the responsibility of dedicated tools or services like AWS KMS or Azure Key Vault. CIEM does not manage encryption keys or address data encryption directly.

Option B: While cost optimization is a key consideration in cloud management, CIEM specifically addresses identity and access management, not cost-saving measures. This is a common misconception as some cloud tools provide cost insights, but CIEM does not focus on financial management.

Option C: Automating resource deployment is a function of tools like Infrastructure as Code (IaC) platforms (e.g., Terraform, AWS CloudFormation). CIEM, however, is not designed for resource provisioning or deployment.

Option D: CIEM focuses on improving security posture by identifying and reducing excessive permissions for identities (human and non-human) in cloud environments. This feature aligns with the principle of least privilege, which minimizes the potential attack surface and reduces risks arising from over-privileged accounts or roles.

Question: 4

In the context of CrowdStrike Falcon Cloud Security, what is a “sensor”?

- A. A standalone module designed to integrate directly with third-party threat intelligence platforms.
- B. A physical device deployed to monitor network traffic at the perimeter.
- C. A lightweight agent deployed on endpoints or cloud workloads to collect telemetry data.
- D. A tool that analyzes encrypted traffic within the cloud for threats.

Answer: C

Explanation:

Explanation for each answer is given below.

Option A: While Falcon integrates with threat intelligence platforms, a sensor is not a standalone module for such integrations. Sensors are integral components of the Falcon platform for data collection and analysis.

Option B: Sensors in the CrowdStrike ecosystem are not physical devices but lightweight software agents installed on endpoints or cloud workloads to gather telemetry data.

Option C: This is the accurate definition of a sensor within the Falcon platform. These agents collect data, such as process execution, file access, and user activity, and send it to the CrowdStrike cloud for analysis.

Option D: CrowdStrike sensors do not focus on analyzing encrypted traffic. Instead, they monitor activity at the endpoint level to detect suspicious behavior.

Question: 5

What is the recommended practice when deleting a container registry connection from Falcon Cloud Security?

- A. Delete the connection directly without verifying its usage in any workflows.
- B. Revoke all tokens associated with the registry immediately after deletion.
- C. Notify all team members and pause all security assessments before deletion.
- D. Ensure the registry is no longer referenced in any active policies or integrations before deletion.

Answer: D

Explanation:

Explanation for each answer is given below.

Option A: Deleting the connection without verification can break dependent workflows and cause image assessments or security scans to fail.

Option B: Revoking tokens is a good practice but should occur after deletion is confirmed to avoid disrupting ongoing access prematurely.

Option C: Notifying the team is optional and pausing assessments is unnecessary, as deleting the

Option D: Before deleting a registry connection, it's critical to verify that it is no longer referenced in policies, workflows, or integrations to prevent disruption or errors in Falcon Cloud Security operations.

Question: 6

Which of the following commands initiates a manual image scan using CrowdStrike's command-line tool?

- A. `csccli image scan --registry <registry_url> --image <image_name>`
- B. `falcon-image-scan --registry <registry_url> --image <image_name>`
- C. `crowdstrike-image --scan --registry <registry_url> --image <image_name>`
- D. `falconctl scan-image --url <registry_url> --img <image_name>`

Answer: B

Explanation:

Explanation for each answer is given below.

Option A: While this syntax might resemble a generic CLI tool, `csccli` is not the command-line tool used by CrowdStrike for image assessment. This option confuses CrowdStrike tools with other third-party solutions.

Option B: This is the correct command syntax for manually scanning container images using CrowdStrike's command-line tool. The `falcon-image-scan` command is specifically designed for this purpose and requires flags like `--registry` and `--image` to specify the image's location and name. This ensures proper configuration for the scan to target the desired image in the specified registry.

Option C: This command structure is fictional and does not align with any CrowdStrike CLI tool or syntax. It might mislead users into assuming the availability of a nonexistent utility.

Option D: `alconctl` is a valid CrowdStrike tool, but it is used for endpoint configuration, not container image scanning. This command incorrectly combines the wrong tool with a scanning function.

Question: 7

An organization wants to create a custom Indicator of Misbehavior (IOM) rule in Falcon Cloud Security to detect and alert when a container attempts to write to a restricted file system directory, such as `/etc/passwd`. What is the correct step to achieve this?

- A. Modify the default Falcon Container Sensor YAML file.
- B. Create the custom IOM rule in the Falcon Cloud Security Console under the "IOM Rules" section.
- C. Define the rule in the Kubernetes Admission Controller manifest.
- D. Use AWS IAM policies to block write attempts to the `/etc/passwd` file.

Answer: B

Explanation:

Explanation for each answer is given below.

Option A: The Falcon Container Sensor YAML file is used to deploy the sensor itself and cannot be modified to create custom IOM rules.

Option B: Falcon Cloud Security provides a dedicated section for creating and managing custom IOM rules. This is the appropriate place to define rules for detecting specific misbehavior, such as unauthorized file system writes.

Option C: Kubernetes Admission Controller policies are used for validating or mutating objects during deployment, not for runtime threat detection like monitoring file system activity.

Option D: AWS IAM policies manage access permissions for AWS resources but cannot monitor or prevent runtime file system access in containers.

Question: 8

After reviewing IAM findings from CrowdStrike CIEM, you observe the following issues:

- Multiple users have excessive permissions beyond their job requirements.
- Several accounts have been inactive for more than six months.
- Roles with administrative privileges are assigned to temporary contractors.

Which of the following remediation actions should be prioritized to address these findings?

- A. Disable all inactive accounts and enforce MFA for all users.
- B. Reassign administrative privileges from temporary contractors to permanent employees and monitor them closely.
- C. Delete all roles with administrative privileges immediately.
- D. Revoke excessive permissions and implement a role-based access control (RBAC) policy.

Answer: D

Explanation:

Explanation for each answer is given below.

Option A: Disabling inactive accounts and enforcing MFA are important steps, but they do not address the excessive permissions issue, which poses a more immediate risk. These measures can be part of a broader remediation strategy but are not the top priority.

Option B: Reassigning privileges might reduce some risks but does not address the root cause of excessive permissions or inactive accounts. A comprehensive RBAC policy is a more effective solution.

Option C: Deleting all administrative roles indiscriminately can disrupt operations and is not a practical solution. Instead, roles should be reviewed and adjusted based on necessity and security requirements.

Option D: Revoking excessive permissions directly addresses the risk of privilege escalation and unauthorized access. Implementing RBAC ensures that users only have the permissions necessary for their roles, reducing the attack surface and improving overall security posture. These actions provide a proactive approach to addressing IAM issues effectively.

Question: 9

A team is deploying the CrowdStrike Falcon sensor on a Linux server hosting Kubernetes workloads. The sensor fails to install, and the logs indicate an error:

1. "Kernel version not supported."

What is the most likely cause of this issue?

- A. The Falcon sensor requires the iptables package, which is missing on the server.
- B. The Linux server is running a kernel version not compatible with the Falcon sensor.
- C. The Linux server's firewall is blocking communication with CrowdStrike cloud endpoints.
- D. The Falcon sensor requires Docker to be installed on the Linux server.

Answer: B

Explanation:

Explanation for each answer is given below.

Option A: While certain Linux configurations might benefit from iptables, its absence does not directly cause kernel compatibility errors. The Falcon sensor operates at the kernel level, making the kernel version the critical factor.

Option B: The Falcon sensor requires a supported Linux kernel version to function properly. If the kernel version is outdated or incompatible, the installation will fail with errors like the one described. The compatibility matrix provided by CrowdStrike should always be consulted before deployment.

Option C: Firewall misconfigurations can prevent the sensor from communicating with the CrowdStrike cloud but do not affect the installation itself. The error specifically mentions kernel compatibility, not connectivity.

Option D: Docker is not a requirement for installing the Falcon sensor on Linux. The sensor operates independently of container runtimes, though it can monitor containers if deployed properly.

Question: 10

What is the primary benefit of using automated remediation in a cloud security workflow?

- A. Reducing response time by taking immediate action on detected threats
- B. Ensuring compliance with industry regulations without manual checks
- C. Increasing cloud environment performance by optimizing resource utilization
- D. Eliminating the need for human oversight during incident response

Answer: A

Explanation:

Explanation for each answer is given below.

threats as soon as they are detected, significantly reducing response time. This minimizes the potential impact of threats by containing them before they can escalate or cause further damage.

Option B: While automated remediation can support compliance by addressing security gaps promptly, it does not fully replace manual checks, audits, or detailed compliance reviews.

Option C: Automated remediation is focused on security incident response, not resource optimization. While securing the environment may have indirect performance benefits, this is not the primary goal.

Option D: Automated remediation complements, but does not replace, human oversight. Security teams still need to review actions, analyze complex incidents, and refine policies to ensure proper functionality.

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

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

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

Money Back Guarantee



Click The Link Below

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