DUMPSARENA

CrowdStrike Certified Cloud Specialist

CrowdStrike CCCS-203b

Version Demo

Total Demo Questions: 7

Total Premium Questions: 77

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Cloud Security Fundamentals	1
Topic 2, Cloud Security Posture Management	23
Topic 3, Cloud Workload Protection	38
Topic 4, Cloud Detection and Response	11
Topic 5, Cloud Security Integrations	4
Total	77

QUESTION NO: 1

You are investigating Azure activity that may have disabled a defensive tool. The investigation must be restricted to IOAs mapped to the MITRE ATT&CK technique for Impair Defenses and must exclude activity from AWS and Google Cloud.

Which filter combination should you use on the IOA dashboard?

A. Attack type – Service

B. MITRE Tactic and Technique – Service

C. MITRE Tactic and Technique – Cloud provider

D. Attack type – Cloud provider

ANSWER: C

Explanation:

MITRE Tactic and Technique – Cloud provider is correct because it combines the required behavioral and environment-specific conditions. The MITRE ATT&CK tactic and technique filters identify IOAs mapped to the relevant defense-evasion behavior, while the cloud-provider filter restricts the returned results to Azure.

An attack-type filter is less precise than filtering on the required ATT&CK technique. A service filter could narrow results to a cloud service but would not ensure that only Azure activity is returned. This combination supports a focused investigation of the stated behavior in the required provider environment.

QUESTION NO: 2

An IOM identifies that logging is not enabled for a cloud service. The cloud engineering team asks for implementation guidance that is specific to the affected provider service.

Which IOM detail should you share with the team?

A. The severity value

B. The total finding count for the policy

C. The Remediation link

D. The affected resource name

ANSWER: C

Explanation:

The Remediation link is correct because it provides related cloud-provider documentation for addressing the identified configuration issue. The provider guidance helps the cloud engineering team understand the applicable service setting and implement the supported corrective action.

Severity helps prioritize the issue but does not provide implementation instructions. The total finding count measures scope, and the affected resource name identifies the target, but neither replaces provider-specific remediation guidance.

QUESTION NO: 3

How can you find if there are any remediable vulnerabilities in your running containers?

A. Filter container assets by container running status and vulnerability remediation

B. Filter image detections by container running status and remediation

C. Filter image vulnerabilities by container running status and remediation

D. Filter container assets by container running status and detection remediation

ANSWER: C

Explanation:

Filter image vulnerabilities by container running status and remediation is correct because it combines the two pieces of context required to identify vulnerabilities that warrant immediate action. Image vulnerability results identify known vulnerabilities in the software packages and layers that make up a container image. Applying the container-running-status filter limits those results to images associated with workloads that are currently active, rather than images that are only stored, unused, or associated with stopped containers. Applying the remediation filter then limits the view to findings for which a fix, such as an updated package or version, is available.

This produces an operationally useful set of findings: vulnerabilities affecting currently running containerized workloads that security and engineering teams can address through an available remediation path. The combined view supports risk-based prioritization by connecting image assessment data to runtime relevance and remediation availability. CrowdStrike Cloud Security provides unified visibility across container images, workloads, and vulnerabilities, enabling teams to prioritize and remediate risks in cloud-native environments. See CrowdStrike's Cloud Security overview and its Container Security information for product context.

QUESTION NO: 4

There is a valid sensor update policy for all Linux hosts that is set to n-2. Some of the hosts have not updated their sensor version.

What is the reason for this situation?

A. DaemonSet was used for deployment

B. One-click sensor deployment has not been enabled

C. None of the hosts have been restarted

ANSWER: C

Explanation:

None of the hosts have been restarted is correct because, for Linux endpoints, a Sensor Update Policy determines the sensor version assigned to the host but installation of the assigned update is completed during a host reboot. The `n-2` setting means the policy targets the second-most-recent supported sensor release, rather than requiring every host to use the newest release. Hosts can therefore correctly receive the policy assignment and still report their existing sensor version until their next restart occurs.

This behavior is especially important when maintenance windows are infrequent or servers are designed for long uptime. An administrator should verify that the affected hosts are assigned to the intended update policy, then schedule and perform a controlled reboot in accordance with organizational change-management requirements. After the restart, the Linux sensor can apply the version designated by the policy and the Falcon console will report the updated version after the endpoint checks in. This separates version selection through policy from the operating-system event that finalizes the update. CrowdStrike documentation is available through the CrowdStrike Documentation portal; additional Linux sensor deployment and operational guidance is available from the CrowdStrike Endpoint Security Tech Hub.

QUESTION NO: 5

You are reviewing Top IOMs and find that MFA for Azure has 62 findings indicating MFA has not been configured across all accounts.

Which options provide a more detailed investigation?

A. Identity & Cloud group

B. Event search & Asset graph

C. CloudTrail logging & Application Registration

ANSWER: B

Explanation:

Event search & Asset graph provides the appropriate investigation paths for an Azure MFA misconfiguration identified in Top IOMs. Asset Graph gives investigators an asset-centric view of the affected Azure environment, allowing them to examine the accounts, subscriptions, identity relationships, and relevant cloud-resource context associated with the reported findings. This helps turn the aggregate count of 62 findings into an actionable inventory of the specific identities that require remediation. Event Search complements that context by enabling analysis of relevant cloud and identity activity, such as authentication-related events and account changes, across the selected time range. Together, these capabilities support both scoping the exposure and investigating activity surrounding the affected accounts before or while enforcing MFA. This aligns with Falcon Cloud Security's posture-management approach: identify configuration risks, examine the affected cloud assets and relationships, and use security telemetry to investigate and prioritize remediation. CrowdStrike describes its cloud security capabilities at CrowdStrike Cloud Security and provides platform documentation through the CrowdStrike Falcon Documentation portal.

QUESTION NO: 6

The container-security team holds a vulnerability review every Friday. Several application owners who must participate do not have Falcon console accounts, and the team needs the report to include the vulnerable container information identified during that review week.

What is the most efficient method to meet these requirements?

A. Create a dashboard and share its link with the application owners

B. Create a scheduled report to list vulnerable container data from the last 7 days

C. Create a saved Image Vulnerabilities filter for the application owners

D. Run an Advanced Event Search query manually every Friday

ANSWER: B

Explanation:

Create a scheduled report to list vulnerable container data from the last 7 days is correct because it automates delivery on the required weekly cadence and provides information to stakeholders without requiring Falcon console access. A seven-day reporting period aligns the report content with the weekly review interval.

A dashboard link or saved filter requires the recipient to access the Falcon console. Running an Advanced Event Search query manually each week does not automate distribution and is not the appropriate workflow for recurring vulnerable-container reporting.

QUESTION NO: 7

Your registry retains historical release images for audit purposes, but the security team only wants Falcon Cloud Security to continue assessing images created during the last 60 days. The team does not want to delete the retained images or repeatedly suppress individual findings.

Which configuration should be used?

A. Configure Stop assessing images older than 60 days

B. Delete all registry images older than 60 days

C. Create a Fusion workflow to hide old findings

D. Manually hide vulnerability findings for each historical image

ANSWER: A

Explanation:

Configure Stop assessing images older than 60 days is correct because this Image Assessment setting centrally controls the age threshold for images that continue to receive assessment. It reduces vulnerability noise from stale retained images without requiring the organization to remove those images from the registry.

Deleting registry images changes the organization’s retention state and is not required to change assessment scope. A Fusion workflow can automate actions after events occur, but it is not the direct assessment-age control. Manually hiding findings would be inefficient and would not establish a consistent policy for future historical images.