CrowdStrike
CCCS-203b
CrowdStrike Certified Cloud Specialist Exam

For More Information – Visit link below:
https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**

Latest Version: 6.0

Question: 1

What activities are carried out during the cloud inventory phase of image assessment?

A. Expand the image layers, identify vulnerabilities, and update the image metadata
B. Collect only the list of application packages installed on the image
C. Expand the image layers, collect the hash for all binary objects, and list OS packages
D. Only collect the hash for all binary objects without other assessments

Answer: C

During the cloud inventory phase of image assessment in CrowdStrike Falcon Cloud Security, the platform performs a deep, non-runtime analysis of container images to establish a complete software and binary inventory. This phase is designed to build visibility and context before vulnerability analysis or enforcement occurs.
Falcon expands all container image layers to inspect their contents individually. This layered expansion is critical because vulnerabilities and malicious artifacts can exist in any layer, including inherited base images. During this process, Falcon collects cryptographic hashes for all binary objects found within the image. These hashes allow Falcon to uniquely identify binaries, correlate them with known threats, and support future detection and investigation workflows.
In addition to binary hashing, Falcon enumerates and lists operating system (OS) packages installed in the image. This includes system libraries and dependencies provided by the base operating system, which are essential for accurate vulnerability mapping and exposure analysis later in the assessment lifecycle.
Importantly, vulnerability identification does not occur during the inventory phase. That activity is handled in subsequent analysis stages. The inventory phase focuses exclusively on expansion, identification, and cataloging of image contents to ensure complete visibility and accuracy.
Therefore, the correct answer is Option C, as it precisely reflects the documented activities performed during the cloud inventory phase of image assessment in CrowdStrike Falcon Cloud Security.

Question: 2

You receive an alert for suspicious network traffic from a container environment over destination port 1337.
What is the most efficient way to find which container and pod the connections are sourcing from using Cloud Security?

A. Within Monitor > Kubernetes and Containers, review the dashboard for active network connections
B. Within Advanced Event Search, search for #event_simpleName = NetworkConnectIP4 | RemotePort = 1337
C. Within Network Events, search for events involving remote port 1337

D. Within Network Events, search for connections involving local port 1337

Answer: C

In CrowdStrike Falcon Cloud Security, the most efficient and direct way to identify which container and Kubernetes pod are responsible for suspicious outbound traffic is by using Network Events and filtering on the remote (destination) port.
When a container initiates outbound network communication, the destination port represents the service being contacted externally. Since the alert specifically references destination port 1337, filtering Network Events for remote port 1337 immediately surfaces the relevant telemetry. Falcon automatically enriches these events with container ID, container name, Kubernetes pod name, namespace, node, and cluster context, allowing rapid attribution.
Using Advanced Event Search is technically possible but less efficient, as it requires manual query construction and does not provide the same streamlined Kubernetes-focused workflow as Network Events. Reviewing dashboards alone is insufficient for precise attribution and forensic analysis.
Filtering on local port 1337 would be incorrect in this scenario, as it would only identify processes listening locally rather than outbound connections sourcing from the container.
Therefore, Option C is correct because it aligns with Falcon Cloud Security's design for container-aware network telemetry, providing the fastest and most accurate path to identifying the originating container and pod.

Question: 3

How can you prevent a container process from altering the container's expected behavior?

A. Enable container drift prevention on the Linux sensor
B. Create a custom IOA with automated remediation
C. Enable process modification protection on the Kubernetes Admission Controller
D. Create an Image Assessment policy to block container drift

Answer: A

In CrowdStrike Falcon Cloud Security, preventing a container process from altering its expected behavior is achieved through container drift prevention enforced by the Falcon Linux sensor at runtime.
Container drift occurs when a running container deviates from its original image state, such as when new binaries are written, files are modified, or unexpected processes execute. Drift is a strong indicator of compromise, misconfiguration, or malicious activity.
By enabling container drift prevention on the Linux sensor, Falcon enforces runtime immutability, ensuring that containers only execute binaries and processes that were present at image build time. Any unauthorized modifications or executions are either detected or actively blocked, depending on policy configuration.
Creating a custom IOA is not the most effective approach because IOAs are reactive and behavior-based rather than enforcing immutability. The Kubernetes Admission Controller operates at deployment time, not runtime, and cannot prevent post-deployment process changes. Image Assessment policies only affect image deployment decisions and do not control runtime behavior.

Therefore, Option A is correct because container drift prevention is specifically designed to protect runtime container integrity, ensuring containers behave exactly as expected throughout their lifecycle.

Question: 4

What is needed to achieve visibility into the latest AWS IAM 1020 restricted use of AWS CloudShell with the latest CIS Foundations Benchmarks for AWS, Azure, and Google Cloud?

A. Leverage existing IOA policy
B. Create custom IOA policy
C. Create custom IOM policy
D. Leverage existing IOM policy

Answer: D

Visibility into AWS IAM controls, including restricted use of AWS CloudShell (CIS IAM 1.20), is provided through CrowdStrike Falcon Cloud Security posture management using Indicators of Misconfiguration (IOMs). These checks continuously evaluate cloud resources against industry-standard benchmarks, including the CIS Foundations Benchmarks for AWS, Azure, and Google Cloud.
CrowdStrike maintains prebuilt, managed IOM policies that are automatically updated to reflect the latest CIS guidance. Leveraging existing IOM policies ensures immediate coverage without the operational risk or overhead of creating and maintaining custom rules. These policies assess IAM configurations, permissions usage, service access controls, and policy enforcement related to CloudShell usage.
IOAs are designed for runtime behavioral detections and are not suitable for posture or configuration validation. Creating custom IOMs is unnecessary for CIS-aligned controls because CrowdStrike already provides validated, benchmark-mapped policies maintained by CrowdStrike security research.
Therefore, leveraging existing IOM policies is the correct and recommended approach to maintain continuous, benchmark-aligned visibility across multi-cloud environments.

Question: 5

Your company uses more than one cloud for cost optimization to avoid being locked in to one vendor. It saves the company money but adds complexity and visibility issues for your team.
Where can you find all of your compute assets that are managed and unmanaged by CrowdStrike across all supported cloud providers?

A. Image Assessment Dashboard
B. Compliance Dashboard
C. Application Security Posture Inventory
D. Cloud Asset Inventory

Answer: D

The Cloud Asset Inventory in CrowdStrike Falcon Cloud Security provides a centralized, normalized view of all compute assets across AWS, Azure, and Google Cloud, regardless of whether they are managed or unmanaged by the Falcon sensor.

This inventory aggregates metadata from cloud provider APIs and Falcon telemetry to present unified visibility into virtual machines, cloud instances, container hosts, and workloads. Security teams can filter assets by cloud provider, account, region, operating system, sensor status, and risk posture, making it essential for multi-cloud environments.

Other dashboards serve specialized purposes: the Image Assessment Dashboard focuses on container images, the Compliance Dashboard maps findings to regulatory frameworks, and Application Security Posture Inventory focuses on application-level risk. None of these provide the full compute asset view required for cross-cloud operational awareness.

Therefore, Cloud Asset Inventory is the correct location for maintaining visibility across complex, multicloud environments.

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/