Download CrowdStrike CCCS-203b Exam Dumps Free

Shared by Porter on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

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

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.

Answer:

A

Question 2

Question Type: MultipleChoice

What is a primary function of the Containers and Images Compliance dashboard in CrowdStrike's Cloud Security platform?

Options:

A- Provides a visual summary of compliance across containers and images
B- Tracks the network performance of containers and provides detailed network usage data
C- Allows users to automatically patch non-compliant containers and images
D- Displays the list of all containers that are unsupported by Falcon Cloud Security with Containers
The Containers and Images Compliance dashboard in Falcon Cloud Security is designed to give security and DevOps teams a visual, aggregated view of compliance posture across container images and running containers.
This dashboard summarizes compliance status against benchmarks such as CIS, organizational policies, and security best practices. It highlights compliant versus non-compliant images and containers, severity distribution, and trending risk, enabling teams to quickly assess overall posture and prioritize remediation.
The dashboard does not perform network monitoring, automatic patching, or unsupported container enumeration. Those functions are handled by other Falcon modules or operational workflows.
Therefore, its primary function is to provide a visual summary of compliance across containers and images, making Option A correct.

Answer:

A

Question 3

Question Type: MultipleChoice

You need to register one AWS account as part of a deployment of Falcon Cloud Security. You decide to complete the registration process in the Falcon UI.

What will be utilized during this process if you choose the recommended method to register an individual AWS account?

Options:

A- AWS Config
B- A Terraform script
C- AWS CloudFormation
D- A Bash script
When registering an individual AWS account in CrowdStrike Falcon Cloud Security using the Falcon UI, the recommended and supported method is AWS CloudFormation. CrowdStrike provides a prebuilt CloudFormation template that automates the creation of required AWS

resources, including IAM roles, permissions, and trust relationships needed for secure, read-only API access.
Using CloudFormation ensures the deployment is consistent, auditable, and aligned with AWS best practices. It minimizes human error by automatically configuring the correct permissions required for Falcon to collect configuration, identity, and resource metadata from AWS. This method also simplifies lifecycle management---resources can be updated or removed cleanly by managing the CloudFormation stack.
Other options are not recommended for this use case. AWS Config is a native AWS compliance service but does not handle Falcon onboarding. Terraform scripts may be used in advanced or large-scale automation scenarios, but they are not the default or recommended approach for single-account registration in the Falcon UI. Bash scripts lack governance, validation, and repeatability.
Therefore, when registering a single AWS account through the Falcon console, AWS CloudFormation is the correct and CrowdStrike-recommended method.

Answer:

C

Question 4

Question Type: MultipleChoice

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?

Options:

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
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.

Answer:

C

Question 5

Question Type: MultipleChoice

What is the first step you should take when troubleshooting issues with cloud account registrations?

Options:

A- Immediately reset all user passwords
B- Disable the account registration feature temporarily
C- Check the email verification process to ensure users receive verification emails
When troubleshooting issues with cloud account registrations in CrowdStrike Falcon Cloud Security, the first step should be to verify the email verification process. Cloud account registration workflows rely on confirmation emails for validation, authorization, and completion of onboarding steps.
If verification emails are delayed, blocked, or misrouted due to email filtering, domain restrictions, or misconfigured mail settings, the registration process can appear to fail even though the underlying configuration is correct. Checking this process is non-disruptive and often resolves the issue quickly.
Resetting user passwords or disabling registration features are intrusive actions that should only be taken after basic validation steps are completed. CrowdStrike best practices emphasize starting with low-impact troubleshooting actions before making broader changes.
Therefore, confirming that users are receiving and completing verification emails is the correct and recommended first step.

Answer:

C

Question 6

Question Type: MultipleChoice

Where can you check the current status of accounts and identify deployment misconfigurations?

Options:

A- Cloud security -- Settings -- Automate
B- Cloud security -- Policies -- Cloud security posture
C- Cloud security -- Settings -- Account registration
D- Cloud security -- Settings -- Cloud posture scan settings

In CrowdStrike Falcon Cloud Security, the Account Registration section is the authoritative location for monitoring the status of onboarded cloud accounts and identifying deployment or configuration issues.
From Cloud Security Settings Account Registration, security teams can view whether AWS, Azure, or GCP accounts are successfully connected, partially configured, or experiencing errors. This view highlights misconfigurations such as missing permissions, failed integrations, or incomplete setup steps that could prevent posture assessments or detections from functioning correctly.
Other settings areas serve different purposes: Automate focuses on remediation workflows, posture policies define compliance logic, and scan settings control assessment frequency. None provide direct visibility into onboarding health and deployment validation.
Therefore, Cloud security -- Settings -- Account registration is the correct and verified answer.

Answer:

C

Question 7

Question Type: MultipleChoice

What is the recommended method to block a specific CVE for 14 days when creating an Image assessment policy exclusion?

Options:

A- Vulnerabilities published recently until 14 days
B- Vulnerability ID & Exclude until 14 days
C- Packages published recently until 14 days
D- Vulnerable ID & Exclude indefinitely

When creating an Image Assessment policy exclusion in CrowdStrike Falcon Cloud Security, the recommended and most precise method to temporarily suppress a specific CVE is Vulnerability ID & Exclude until 14 days.

This approach allows security teams to explicitly reference a known CVE (for example, CVE-2024-XXXX) and suppress enforcement for a defined time window. The 14-day exclusion period is commonly used to allow development teams time to rebuild images, validate patches, or address dependency constraints without permanently weakening security posture.

Broad exclusions based on recently published vulnerabilities or packages can unintentionally suppress unrelated risk and increase exposure. Indefinite exclusions are discouraged unless there is a strong, documented business justification.

CrowdStrike documentation and best practices emphasize time-bound, CVE-specific exclusions to balance operational flexibility with security rigor. Therefore, the correct and recommended option is Vulnerability ID & Exclude until 14 days.

Answer:

B