CrowdStrike CCCS-203b Practice Questions

Shared by Richards on 22-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What cloud-conscious attacker behavior is used to allow them to stay hidden in the environment?

Options:

A- Storage Account Networking changed to All Networks
B- CloudTrail logging disabled
C- Certificate added to an application registration
D- EC2 Default security group does not block all traffic

A common cloud-conscious attacker technique used to remain hidden in a compromised environment is disabling CloudTrail logging. AWS CloudTrail records API activity across an account, providing critical visibility into actions taken by users, roles, and services. By disabling or tampering with CloudTrail, attackers significantly reduce the likelihood of detection.
CrowdStrike Falcon Cloud Security classifies this behavior as a high-risk indicator because it directly impacts monitoring, forensics, and incident response. Without CloudTrail logs, security teams lose audit trails that are essential for identifying malicious actions such as privilege escalation, data exfiltration, or persistence mechanisms.
Other options represent misconfigurations or changes that may increase exposure but do not directly suppress visibility. For example, modifying storage networking or security groups increases attack surface, while adding certificates may support persistence---but none are as directly linked to stealth as disabling logging.
Therefore, CloudTrail logging disabled is the correct answer and a well-documented cloud attack tactic used to evade detection.

Answer:

B

Question 2

Question Type: MultipleChoice

You are a cloud security analyst concerned about adversaries obtaining admin privileges in your cloud environments.

Which Cloud Identity Analyzer category should you look at first?

Options:

A- Defense Evasion
B- Execution
C- Persistence
D- Privilege Escalation
If the primary concern is adversaries obtaining administrator or elevated privileges, the first Cloud Identity Analyzer category to review is Privilege Escalation. This category focuses on techniques and misconfigurations that allow attackers to gain higher-level permissions than initially granted.
Privilege escalation in cloud environments often involves overly permissive IAM roles, abuse of service principals, misconfigured trust relationships, or exploitation of identity federation mechanisms. CrowdStrike Cloud Identity Analyzer maps these behaviors to established attack frameworks and highlights identities that could be abused to gain admin-level access.
Other categories address different stages of the attack lifecycle. Execution focuses on running malicious actions, Persistence on maintaining access, and Defense Evasion on hiding activity. While all are important, privilege escalation represents the most direct path to full environment compromise.
Therefore, the correct starting point is Privilege Escalation.

Answer:

D

Question 3

Question Type: MultipleChoice

You are using the Packages dashboard to identify all Python packages found on assessed container images. You must provide a list of those packages to a team member who is not a Falcon user.

Which option meets these requirements?

Options:

A- Filter by package name & version: PYTHON and export to CSV or JSON
B- Filter by package type: PYTHON and create a saved filter for your team member to view
C- Filter by package name & version: PYTHON and create a saved filter for your team member to view
D- Filter by package type: PYTHON and export to CSV or JSON
In Falcon Cloud Security, the Packages dashboard allows filtering package inventory by package type, such as Python, Java, or OS-level packages.
To share results with a team member who is not a Falcon user, the data must be exported. Creating saved filters does not grant access to non-users. Filtering by package type: PYTHON ensures all Python-related packages are included regardless of name or version, providing complete coverage.
Exporting the filtered results to CSV or JSON enables easy sharing, offline analysis, and

integration into other tools.
Therefore, the correct option is Filter by package type: PYTHON and export to CSV or JSON.

Answer:

D

Question 4

Question Type: MultipleChoice

The internal audit team is preparing for an internal review. You have been asked to provide a list of configuration policy breaches against the NIST benchmark.

Where can you access this list?

Options:

A- Export Cloud Posture -- Cloud indicators of attack
B- Export Cloud Posture -- Indicators of misconfiguration
C- Export Cloud Posture -- Remediation status
D- Export Cloud Posture -- Cloud Posture dashboard
In CrowdStrike Falcon Cloud Security, configuration policy breaches aligned to regulatory and security frameworks such as NIST are tracked as Indicators of Misconfiguration (IOMs). These findings represent deviations from best-practice configurations and compliance benchmarks.
To provide an auditable list of NIST-related configuration violations, the correct location is Export Cloud Posture -- Indicators of misconfiguration. This export includes detailed records of misconfigured resources, associated benchmarks (NIST, CIS, etc.), affected cloud accounts, severity, and remediation guidance. It is specifically designed to support internal and external audit requirements.
Cloud Indicators of Attack focus on threat activity, not compliance. Remediation status reports focus on fix progress rather than raw policy violations. The Cloud Posture dashboard provides a high-level summary but does not deliver the detailed, exportable list required for audits.
Therefore, Export Cloud Posture -- Indicators of misconfiguration is the correct and documented source.

Answer:

B

Question 5

Question Type: MultipleChoice

Which action is required when creating a new image registry connection that accesses a privately hosted registry?

Options:

A- Verify the registry URL
B- Confirm expiration date of the secret for any used service accounts
C- Add CrowdStrike IP addresses to registry allowlists
D- Verify the token and secret

When configuring a new image registry connection for a privately hosted container registry in CrowdStrike Falcon Cloud Security, the required and most critical action is to verify the token and secret used for authentication. Private registries require explicit credentials so Falcon can securely access and assess container images for vulnerabilities, malware, and misconfigurations.

CrowdStrike supports multiple private registry types (such as private Docker registries or cloud-native registries with restricted access). In all cases, Falcon relies on valid authentication credentials---typically a token, username/password, or service account secret---to pull image metadata and layers. If these credentials are incorrect, expired, or misconfigured, image assessment will fail even if the registry connection appears configured.

Other options may be relevant in specific environments but are not universally required at creation time. Registry URLs are validated during setup, and allowlisting IP addresses may be necessary only if strict network controls are in place. Secret expiration checks are a maintenance concern, not a mandatory creation step.

Therefore, the required action when creating a private registry connection is to verify the token and secret.

Answer:

D

Question 6

Question Type: MultipleChoice

You are troubleshooting an issue with an Azure account registered in Falcon Cloud Security. The registration appeared to be successful but certain CSPM operations, including asset inventories and IOM detection, are failing.

How can you securely test the hypothesis that these failed CSPM operations are related to your firewall configuration?

Options:

A- Check that you have allowlisted the IP addresses provided in the public-facing CrowdStrike documentation
B- Begin investigating another hypothesis as there is no way blocked traffic could be responsible
C- Temporarily open up the firewall to all inbound traffic for testing purposes
The secure and recommended approach to validate whether firewall restrictions are causing CSPM failures is to confirm that CrowdStrike's documented IP addresses are allowlisted. Falcon Cloud Security relies on outbound API connectivity to cloud providers, and blocked traffic can disrupt asset inventory collection and IOM detection even if registration succeeds.
CrowdStrike publishes required IP ranges and endpoints for each cloud region. Verifying firewall rules against this documentation is a low-risk, best-practice troubleshooting step that preserves security controls while validating connectivity assumptions.
Opening firewalls broadly is insecure and unnecessary, and dismissing firewall-related causes without verification can delay resolution. Therefore, the correct answer is Check that you have allowlisted the IP addresses provided in the public-facing CrowdStrike documentation.

Answer:

A

Question 7

Question Type: MultipleChoice

Your team wants to review container vulnerabilities on a weekly basis. Not all members of the team reviewing the information will have access to the Falcon console.

How can you automatically distribute the vulnerable container information from Cloud Security?

Options:

A- Create a scheduled report to list vulnerable container data from the last 24 hours
B- Create a scheduled report to list vulnerable container data from the last 7 days
C- Create a query using Advanced Event Search and run the query once a week
D- Create a dashboard displaying the vulnerable container information and share the link
CrowdStrike Falcon Cloud Security supports scheduled reporting as the preferred mechanism for automatically distributing security findings to stakeholders who may not have direct access to the Falcon console. When container vulnerabilities need to be reviewed on a weekly basis, the correct and most operationally efficient approach is to create a scheduled report covering the last 7 days.
Scheduled reports can be configured to run automatically and delivered via email to designated recipients, including users without Falcon console access. This makes them ideal for cross-functional teams, auditors, or management who require regular visibility into container risk without interactive access.
Using Advanced Event Search requires console access and manual execution, which does not meet the requirement for automatic distribution. Dashboards also require console access and cannot be securely shared externally. A 24-hour report would not align with the stated weekly

review cadence and could result in incomplete visibility.
CrowdStrike documentation and best practices recommend scheduled reports for recurring compliance, vulnerability, and risk reporting use cases. Therefore, the correct solution is to create a scheduled report to list vulnerable container data from the last 7 days.

Answer:

B

Question 8

Question Type: MultipleChoice

You are troubleshooting an issue with an Azure account registered in Falcon Cloud Security. The registration appeared to be successful, but certain CSPM operations---including asset inventories and IOM detection---are failing.

How can you securely test the hypothesis that these failed CSPM operations are related to your firewall configuration?

Options:

A- Check that you have allowlisted the IP addresses provided in the public-facing CrowdStrike documentation
B- Begin investigating another hypothesis as there is no way blocked traffic could be responsible
C- Temporarily open up the firewall to all inbound traffic for testing purposes
The secure and recommended way to test whether firewall restrictions are causing CSPM operation failures is to verify that the required CrowdStrike IP addresses are allowlisted. Falcon Cloud Security relies on outbound API communication between CrowdStrike and the cloud provider. If firewall rules block this traffic, asset inventory collection and IOM detection can fail even though registration appears successful.
CrowdStrike publishes a list of IP addresses and endpoints that must be permitted for proper operation. Validating firewall allowlists against this documentation is a low-risk, best-practice troubleshooting step that preserves security controls while testing connectivity assumptions.
Temporarily opening firewalls to all inbound traffic is insecure and strongly discouraged. Dismissing firewall-related causes without validation can delay resolution. Therefore, the correct and secure approach is to check that the CrowdStrike IP addresses are allowlisted.

Answer:

A

Question 9

Question Type: MultipleChoice

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?

Options:

A- Identity & Cloud group
B- Event search & Asset graph
C- CloudTrail logging & Application Registration

When investigating widespread Indicators of Misconfiguration (IOMs) such as Azure MFA not being enforced, CrowdStrike Falcon Cloud Security provides deeper investigative context through Event Search and Asset Graph. These two capabilities work together to move beyond a high-level finding count and into actionable insight.
Event Search allows analysts to query cloud control plane activity and identity-related events to understand how authentication policies are configured, modified, or bypassed over time. This helps determine whether MFA gaps are due to legacy configurations, recent changes, or specific identities or services.
Asset Graph provides a visual and relational view of cloud identities, subscriptions, roles, and permissions. It enables analysts to see which users, service principals, or resources are affected by missing MFA enforcement and how they are connected across the environment.
The other options do not provide the same depth of investigation. Identity & Cloud Group is primarily used for scoping visibility, while CloudTrail logging is AWS-specific and not applicable to Azure MFA findings. Therefore, the correct answer is Event search & Asset graph.

Answer:

B

Question 10

Question Type: MultipleChoice

When should you enable Drift Prevention for containers?

Options:

A- When containers are used for development and testing
B- When images launch and need to download and install packages

C- When your workloads have been designed to be immutable
D- When deploying a brand new image
CrowdStrike recommends enabling Drift Prevention when container workloads have been designed to be immutable. Immutable infrastructure is a core cloud-native principle where containers are not modified after deployment. Any change to a running container---such as installing packages or modifying files---indicates potential misconfiguration or malicious activity. Drift Prevention enforces this principle by blocking or alerting on runtime changes that deviate from the original container image. This makes it highly effective for production environments where containers should run exactly as built and deployed.
In development or testing environments, containers often change dynamically, making Drift Prevention impractical due to excessive false positives. Similarly, containers that must download or install packages at startup inherently require runtime modification and are not suitable candidates for Drift Prevention.
Enabling Drift Prevention at the wrong time can disrupt legitimate workloads. Therefore, CrowdStrike guidance clearly states that Drift Prevention should be enabled only after workloads are intentionally designed to be immutable, making option C the correct answer.

Answer:

C

Question 11

Question Type: MultipleChoice

What are three valid states for the state of a port under the Network Events dashboard?

Options:

A- Open, Connect, and Closed
B- Listen, Reject, and Connect
C- Connect, Accept, and Listen
D- Accept, Connect, and Reject
In Falcon Cloud Security Network Events, port states reflect how network connections are established and handled at runtime. The platform uses standardized connection state terminology to help analysts understand traffic behavior and intent.
The three valid port states are:
Connect: Indicates an outbound connection attempt initiated by a process or container.
Accept: Represents an inbound connection that was accepted by a listening process.
Listen: Shows that a process is actively listening on a port for incoming connections.
These states provide crucial context for detecting suspicious behavior such as unauthorized listeners, unexpected inbound access, or abnormal outbound communications. Other options include terms not used by Falcon to define port state semantics within Network Events.
Therefore, Connect, Accept, and Listen is the correct answer.

Answer:

C

Question 12

Question Type: MultipleChoice

You want to block privileged containers from being executed in your Kubernetes cluster.

What sensor type should you deploy?

Options:

A- Kubernetes Protection Agent
B- Kubernetes Sensor
C- Kubernetes Image Assessment at Runtime
D- Kubernetes Admission Controller

To block privileged containers before they are executed, CrowdStrike recommends deploying the Kubernetes Admission Controller. This component operates at admission time, intercepting Kubernetes API requests and enforcing security policies before workloads are allowed to run. Privileged containers represent a significant security risk because they can bypass isolation boundaries and access host resources. The Kubernetes Admission Controller can enforce policies that explicitly deny deployments using privileged flags, hostPath mounts, or other high-risk configurations.

Other options do not provide enforcement. Runtime sensors and agents can detect or alert on risky behavior after execution, but they cannot prevent the workload from starting. Image assessment evaluates image content but does not enforce Kubernetes runtime constraints. Therefore, to proactively block privileged containers, the correct and CrowdStrike-recommended solution is the Kubernetes Admission Controller.

Answer:

D

To Get Premium Files for CCCS-203b Visit

https://www.p2pexams.com/products/cccs-203b

For More Free Questions Visit

https://www.p2pexams.com/crowdstrike/pdf/cccs-203b

