**Vendor:** CrowdStrike

**Exam Code:** CCCS-203b

**Exam Name:** CrowdStrike Cloud Specialist

**Version:** DEMO

**QUESTION 1**
You do not have access to the kernel and are using ECS Fargate. Which Falcon Sensor installation should you use to protect Linux-based containers?

A. CrowdStrike Falcon Helmchart
B. Falcon Container Sensor for Linux
C. Falcon Sensor for Linux
D. Falcon Sensor for Windows

**Answer:** B
**Explanation:**
ECS Fargate does not provide kernel-level host access, so the standard host-based Falcon Sensor for Linux is not appropriate. For Linux containers in Fargate, use the Falcon Container Sensor for Linux.

**QUESTION 2**
Your organization has a policy stating that all containers must be launched via a Kubernetes Orchestrator. How can you efficiently identify containers that are breaching this policy?

A. Use the Unidentified Containers Dashboard and look for containers where Visible to K8s is No
B. Use the Unidentified Containers Dashboard and look for containers where Unassessed Images is greater than 0
C. Use the Containers Dashboard and look for containers whose cluster name does not match those used by your organization
D. Use the Containers Dashboard and look for container image IDs that do not match those used by your organization

**Answer:** A
**Explanation:**
If containers must be launched through Kubernetes, containers not visible to Kubernetes indicate they may have been started outside the orchestrator. The Unidentified Containers Dashboard helps identify these non-orchestrated or rogue containers.

**QUESTION 3**
Which methodology should you use to install the Falcon Sensor for Linux on a Kubernetes cluster as Daemonset?

A. Deploy the Falcon Sensor with 1-click Sensor deployment
B. Deploy the Falcon Sensor using Snapshot
C. Deploy the Falcon sensor for Linux with a Helm Chart
D. Deploy the Falcon Container sensor for Linux with a Helm Chart

**Answer:** C
**Explanation:**
To install the Falcon Sensor for Linux across Kubernetes nodes as a DaemonSet, the standard deployment method is using the Falcon Helm Chart. The container sensor option is different and is used for containerized environments where host/kernel-level deployment is not available.

**QUESTION 4**
When utilizing Image Assessment at Runtime (IAR), which installation mode is recommended when your environment supports it?

A. Helm Mode
B. Kubernetes Mode
C. Watcher Mode
D. Socket Mode

**Answer:** D
**Explanation:**
Socket Mode is the recommended IAR installation mode when supported because it directly observes container runtime activity through the container runtime socket. Watcher Mode is typically used as an alternative when Socket Mode is not available.

**QUESTION 5**
Your organization has a policy to assess all container images before deploying them to production. You identified several unassessed images currently in use. How can you ensure compliance and address these unassessed images?

A. Rely on host-based security tools to monitor for threats from unassessed images in production
B. Remove all unassessed images from production and block users from deploying new containers
C. Assume unassessed images are safe if no incidents have been reported and focus on scanning future images
D. Scan the unassessed images using Falcon's runtime Image Assessment feature

**Answer:** D
**Explanation:**
Runtime Image Assessment helps identify and assess container images already running in the environment. This is the correct way to address images that are currently in use but were not assessed before deployment.

**QUESTION 6**
A process on one of your virtual machines is attempting to execute a script that connects to an unfamiliar external IP address. This activity matches patterns of known malicious behavior. What action should you take to identify any associated persistence mechanisms?

A. Focus solely on network traffic to identify other potential malicious connections
B. Immediately terminate the virtual machine to stop the suspicious activity
C. Review the startup scripts and scheduled tasks on the virtual machine for unauthorized entries

**Answer:** C
**Explanation:**
Persistence mechanisms commonly use startup scripts, cron jobs, scheduled tasks, services, or autorun entries to survive reboots and continue execution. Reviewing these locations is the most direct way to identify persistence related to the suspicious script activity.

**QUESTION 7**
When reviewing the Cloud Security Posture Management dashboard, you notice 16 Critical IOMs. There is traffic between ELB (Elastic Load Balancer) that is not encrypted. Which policy will notify you of this misconfiguration?

A. ELB configured publicly with TLS/SSL disabled
B. ELB configured with a vulnerable SSL protocol

C. ELB Classic attached to a security group with no outbound rules
D. ELB Classic with cross-zone disabled

**Answer:** A
**Explanation:**
Unencrypted traffic on an ELB indicates that TLS/SSL is not enabled where it should be. The matching misconfiguration policy is the one that detects an ELB exposed publicly with TLS/SSL disabled.

**QUESTION 8**
An application team is working on a group of cloud accounts. They are having trouble identifying their assets when analyzing findings within Cloud Security. What can be done to help the team filter for their assets?

A. Tag hosts within the resource groups as they are created
B. Create a cloud group with the cloud accounts needed for filtering
C. Assign hosts within the resource groups to a new host group to identify the devices

**Answer:** B
**Explanation:**
A cloud group allows related cloud accounts to be grouped together, making it easier for teams to filter findings and focus only on the assets they own or manage. Host groups are for Falcon hosts, not cloud account-level filtering.

**QUESTION 9**
What conditions must exist for a container to be listed under the Most vulnerable exposed running containers widget?

A. Running containers with open ports where the underlying image has a vulnerability
B. Running containers with any vulnerability in the underlying container image
C. Running containers with ports 80 and 443 open
D. Running containers with a critical vulnerability in the underlying container image

**Answer:** A
**Explanation:**
The widget focuses on running containers that are exposed and whose underlying images contain vulnerabilities. Exposure is indicated by open ports, not just by the presence of vulnerabilities alone.

**QUESTION 10**
You want to give your developers time to fix new CVEs. How can this be efficiently done in Falcon Cloud Security while maintaining security of the environment?

A. Create an exclusion of 7 days for newly published vulnerabilities
B. Create an exclusion every time a new CVE is discovered
C. Network contain the hosts affected by the CVE
D. Scan new images 7 days after they are created

**Answer:** A
**Explanation:**
A time-based exclusion for newly published vulnerabilities gives developers a controlled grace

period to remediate new CVEs without repeatedly creating manual exclusions for each CVE. This maintains visibility while reducing unnecessary immediate noise.

**QUESTION 11**
You are concerned about overprivileged containers within your cluster. Which IOM rule for Kubernetes will alert on containers being deployed with excessive permissions?

A. Container(s) without resource limits
B. Workload without securityContext
C. Container(s) with sysadmin capability
D. Malformed sysctl value

**Answer:** C
**Explanation:**
The SYS_ADMIN capability is highly privileged in Linux containers and can allow broad system-level operations. A container deployed with this capability is considered overprivileged and should trigger the related Kubernetes IOM rule.

**QUESTION 12**
Your team is reviewing your Kubernetes cluster to ensure compliance with the latest industry benchmarks. Which is an example of a configuration setting that will be flagged as non-compliant?

A. Disabling unnecessary ports on the host firewall
B. Allowing containers to run with root privileges
C. Using a private container registry for all deployments
D. Enabling role-based access control for Kubernetes API access

**Answer:** B
**Explanation:**
Running containers as root violates Kubernetes security best practices and compliance benchmarks because it increases the impact of container compromise. The other options are generally secure configuration practices.

**QUESTION 13**
Which action should be taken to configure cloud security scan exclusion settings in CrowdStrike?

A. Enable all scans without any exclusions for maximum coverage
B. Exclude all cloud resources to avoid performance issues
C. Define exclusion rules based on file paths to be ignored during scans
D. Only exclude files that have been scanned previously

**Answer:** C
**Explanation:**
Cloud security scan exclusions should be configured by defining specific exclusion rules, such as file paths that should be ignored during scans. This allows targeted exclusions without disabling scan coverage broadly.

**QUESTION 14**
You want to build a custom policy in Microsoft Azure to ensure web application diagnostic logging

is not disabled for your App Service. How do you create a custom Indicator of Misconfiguration?

A. Use Azure Notification Hubs to send an alert to CrowdStrike when logging is disabled
B. Create a JSON formatted file with the conditions you want to alert on
C. Create a new policy that includes custom policy preview

**Answer:** B
**Explanation:**
Custom IOMs are created by defining the misconfiguration logic in a JSON-formatted policy file. This lets Falcon Cloud Security evaluate Azure resources against the specific conditions you want to detect.

**QUESTION 15**
There are storage buckets in your cloud environment that are publicly accessible and exposing sensitive data to potential threats. What action can you take to identify and remediate similar misconfigurations?

A. Use CSPM to scan cloud environments for improperly configured storage buckets
B. Block all external traffic to storage buckets at the network level to prevent unauthorized access
C. Rely on end users to avoid storing sensitive data in publicly accessible buckets

**Answer:** A
**Explanation:**
CSPM identifies cloud misconfigurations such as publicly accessible storage buckets and provides remediation guidance. Blocking all external traffic is too broad, and relying on users is not an effective control.

**QUESTION 16**
What checks are performed on the JSON files during the assessment phase?

A. Checks for OS package vulnerabilities, collects the hash for all binary objects, and updates image metadata
B. Checks for OS package and application package vulnerabilities, AI-related packages or vulnerabilities, and misconfigurations
C. Reviews only application package vulnerabilities without considering misconfigurations or AI-related vulnerabilities

**Answer:** B
**Explanation:**
During the assessment phase, Falcon evaluates the collected image data for vulnerabilities in OS and application packages, AI-related risks, and misconfigurations. Hash collection and metadata updates belong more to inventory/processing, not the assessment checks.

# Thank You for Trying Our Product

## Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

**10% Discount Coupon Code:** **ASTR14**