Activity: Analyze the security of a container

Activity Overview

In this activity, you will review the details of a container configuration. You'll use this information to identify security issues in the configuration and provide suggestions for implementing container security best practices.

As you have learned, a **container** is a software package that holds only the components necessary to execute a particular application. Containers are created with an image—a file containing executable code that is used to create the container. Container security is critical because once a malicious actor has access to a container, they can attempt to access other assets in the cloud environment. As a cloud security analyst, you'll likely work with containers at some point in your journey.

Be sure to complete this activity before moving on. The next course item will quiz your comprehension, and then you'll be provided with a completed exemplar to compare to your own work.

Scenario

Review the following scenario. Then, access the supporting materials before moving on to the next course item to take the quiz.

Containers provide many advantages, such as maintaining consistency, enabling rapid development and deployment of new applications and features, and optimizing resource usage. As part of its digital strategy, Cymbal Bank is seeking to adopt containers to more efficiently package, run, and manage their web and mobile banking applications.

While containers offer flexibility, however, they also introduce some complexities. As a cloud security analyst at Cymbal Bank, part of your role includes identifying and remediating vulnerabilities in Cymbal Bank's cloud infrastructure. Your supervisor has tasked you with analyzing the security of the container image of an application. The application is currently being deployed on a staging environment, and the security team wants to test it before deploying it in the production environment. Currently, Cymbal Bank does not have a container-build lifecycle and is seeking to create one with container security in mind.

Your task is to analyze the container configuration and provide suggestions for introducing effective container security practices to protect Cymbal Bank's critical infrastructure and customer data. You will add your suggestions in a checklist that the developers will use in their container-build lifecycle.

Step-By-Step Instructions

Consult the supporting materials to answer the quiz questions in the asset that follows. After you complete the quiz, you can compare your work to the exemplar provided.

Step 1: Access supporting materials

The following supporting materials will help you complete this activity. Keep them open as you proceed to the questions.

RIGHT CLICK LINKS TO OPEN IN NEW TAB

Link to template: Container security checklist template

Link to supporting materials: Container configuration details

Step 2: Analyze the container configuration

The software developers created a **Container configuration details** document that you will use to review the configuration of the container. As you review the document, notice the following details:

- The container image is pulled from a trusted image registry.
- A vulnerability scan revealed a kernel-level vulnerability in the container image.
- There is one Kubernetes service account with unrestricted access.

Review each detail of the configuration and determine whether any security best practices need to be implemented. As a reminder, some best security practices for containers that you've learned about include:

- Use verified and trusted container images.
- Perform vulnerability scanning on container images.
- Use role-based access control to control access for user and service accounts.

Step 3: Provide suggestions for container security

After you've reviewed the container configuration, add your suggestions for how the software developers can improve container security in their development lifecycle to the **Container security checklist** template.

- For each checklist item, write **1–2 sentences** describing a container security best practice. Consider the security best practices that you've learned so far in this course. Refer to the **Techniques to secure containers** video and the **Security in containers** reading available in Course 3, Module 3 to help support you throughout this activity.
- In the **Explanation** section for each item, write **1–2 sentences** summarizing what you found in the container configuration and how this security best practice can remediate it.
- If the container configuration has met the security practices you've outlined (for example, if the container configuration was designed to isolate the container resources in a cluster), check the box.

Step 4: Access the quiz and answer questions about container security

Go to the next course item and answer the quiz questions. Then compare your work to the exemplar provided.

Pro Tip: Save the template

Finally, be sure to save a blank copy of the template you used to complete this activity. You can use it for further practice or in your professional projects. These templates will help you work through your thought processes and demonstrate your experience to potential employers.

What to Include in Your Response

Be sure to address the following criteria in your completed activity:

- 3–4 checklist items with 1–2 sentences describing a container security best practice
- 1–2 sentences providing an explanation for each security best practice
- A check next to each security best practice that has been implemented