Activity: Manage IaC with Terraform

Activity Overview

In this activity, you'll examine a Terraform configuration file used to automate infrastructure and identify how different pieces of code affect the infrastructure. Then, you'll answer a series of quiz questions about how organizations leverage infrastructure as code (IaC) to improve security.

IaC is the practice of provisioning and managing infrastructure using reusable scripts. IaC's automation capabilities are important in cloud computing. Automation reinforces an organization's security posture by incorporating security checks early in the software development process. Automation also helps ensure developers across teams use the same source code when creating infrastructure for virtual machines and applications.

Scenario

Review the following scenario. Then complete the step-by-step instructions.

You've recently joined the Cymbal Bank security team as a junior cloud security analyst. As part of the security team, you're responsible for ensuring that virtual machines (VMs) are correctly configured and deployed using IaC. IaC introduces automation, ensuring that the VMs are consistent across Cymbal Bank's hybrid cloud infrastructure. IaC can also automate security checks from the beginning of the development process. Your awareness of how security risks can translate to the retail industry is an incredible asset to your team. For example, you know that configuration drift and invalid code inputs could cause serious security implications. With Cymbal Bank's global presence online, along with its 170 physical stores, the security of the VMs are extremely important.

You've received a request to provision infrastructure to help with Cymbal Bank's hybrid cloud migration efforts. You've been asked to create server instances, also called virtual machines (VMs), and to install some software based on the standard Terraform installation template.

The Terraform file creates a network with a Google Compute Engine instance. Once Terraform processes this file, it will create the infrastructure. Your task is to review the Terraform file before deploying it. You'll need to determine the file's resources and what these resources create. You'll also need to identify how to update the location of the VMs since the VMs will be

launching globally.

Cymbal Bank's executive leadership has expressed concerns about the security of moving infrastructure to the cloud. To address these concerns, you'll also need to prepare a response that identifies how IaC improves the security of the VMs and the organization's infrastructure as a whole.

Your goals for the project include:

- Goal 1: Examine a Terraform configuration file.

- Goal 2: Describe what cloud resources the different pieces of code create in the file.

- Goal 3: Identify how to change a virtual machine's location.

- Goal 4: Explain how incorporating IaC can improve security.

Step-By-Step Instructions

Consult the supporting materials to review the Terraform configuration file. As a cloud security analyst, it's important to review Terraform configurations for misconfigurations to ensure that they meet both your organization's security requirements. Then, move on to the next course item to answer quiz questions about the material. After you complete the quiz, you can compare your answers to the feedback 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 supporting materials: Terraform configuration file

Step 2: Review and analyze the supporting materials

In the **Terraform configuration file**, analyze each resource block to determine which cloud resources are going to be created. Each resource block will provide you with information about the type of resource being created, the resource's location, and more.

Step 3: Answer questions about IaC and Terraform

Move forward to the next course item to answer quiz questions about the Terraform configuration file.