**Activity 9 - Working with AWS CloudTrail(module-09)**

Here are the step-by-step instructions for completing the challenge lab:

1. \*\*Launching the activity environment:\*\*

- Start Lab to launch your lab.

- Wait for the lab status to be "ready", then close the Start Lab panel.

- Choose AWS at the top of the instructions to open the AWS Management Console in a new browser tab.

2. \*\*Task 1: Modify a security group and observe the website:\*\*

- Go to the EC2 service from the Services menu.

- Select Instances, then locate and choose the Cafe Web Server instance.

- Choose the Security tab and select the WebSecurityGroup.

- Edit inbound rules, add a rule for port 22 with source "My IP", and save the rules.

- Observe the Cafe website by copying the Public IPv4 address and navigating to http://<WebServerIP>/mompopcafe/.

3. \*\*Task 2: Create an AWS CloudTrail log and observe the hacked website:\*\*

- Go to the CloudTrail service from the Services menu.

- Choose Trails and create a trail with the name "Monitor".

- Observe the hacked website by refreshing the page and wait for the hack to occur.

4. \*\*Task 3: Analyze the CloudTrail Logs by using grep:\*\*

- Connect to the Cafe Web Server host EC2 instance using SSH.

- Download and extract the CloudTrail logs.

- Analyze the logs using the grep Linux utility.

5. \*\*Task 4: Analyze the CloudTrail logs by using Amazon Athena:\*\*

- Create the Amazon Athena table by going to the CloudTrail service and choosing Event history.

- Choose Create Athena table and configure it to use the CloudTrail logs bucket.

- Analyze the logs using Athena by running SQL queries in the Athena Query Editor.

6. \*\*Task 5: Further Analysis of the Hack and Improving Security:\*\*

- Check the OS users on the Cafe Web Server instance and remove any suspicious users.

- Update SSH security settings by modifying the /etc/ssh/sshd\_config file and restarting the SSH service.

- Fix the website by restoring the original graphic.

- Delete the AWS hacker user from the IAM service in the AWS Management Console.

Follow these steps carefully to complete the challenge lab successfully.