Cloud Security Engineer Home Task

Practical task
Configure security features for a newly created AWS account using Terraform (where possible). This exercise aims to assess your ability to implement fundamental security measures and manage infrastructure as code. Feel free to use an existing account or create a new one. Please note that you may be required to show what you have done to better explain your thought process as well as make live changes to your code during the follow-up interview.

NB! Please ensure that nothing you will perform for the task will incur costs on your AWS account. Bonus points if you do this by using free tier usage alerts.

What you need to do:

- Create a free-tier AWS account using https://aws.amazon.com/free
- Create a code repository using GitHub or similar to store your terraform code

On the AWS account:

- Enable AWS Organizations (always free)
- Enable & configure AWS IAM Identity Center (always free)
  - Creating a few test users would be useful to show the effectiveness of your IAM policies
- Enable security hub (always-free)
- Enable CloudTrail (1 trail is within free-tier, S3 up to 5gb is within free-tier)
- Create and enable SCPs that would prevent people from
  - Disabling security hub (except for the root account)
  - Disabling CloudTrail (except for the root account)
  - Exposing CloudTrail S3 bucket publicly

Provide a link to your terraform code for the task. If you would rather keep the repository private, please let us know and we will give you account names to add as collaborators.

Bonus:

- Create an EC2 instance (t2.micro), deploy a simple web application and:
  - protect access to the instance (as in only specific users can access the server)
  - protect access to the web application (with security groups)
- Provide a description and diagram of your AWS resources architecture in the README file of your code repository

Theoretical task

Choose any **one** of the questions below and provide an answer in written format.

1. You are architecting a scalable and secure web application using AWS CloudFront as the CDN. Describe how you would integrate AWS WAF with CloudFront and an Application Load Balancer to enhance the security posture of the application.
2. As part of a cloud risk management strategy, explain how continuous monitoring and auditing are implemented. Provide examples of cloud-native tools and services used for monitoring and auditing, and discuss how they contribute to identifying and mitigating risks.
3. Discuss how the AWS Shared Responsibility Model applies to the security of Elastic Container Service and what specific security measures should be considered.

Be as specific as you wish.

Take as much time as you need to complete the tasks. Feel free to send an email if you have any questions.

Good luck!