Overview

Brightwheel is hosted on AWS making extensive use of tools within the AWS ecosystem. The goal of this exercise is to assess AWS knowledge & fluency, and to provide a showcase for implementation design and decision making.

Background

Brightwheel uses infrastructure as code, has multiple development teams with specific areas of product focus, and each of these teams requires access to AWS tools and technology.

In order to ensure the integrity and reliability of the entire AWS ecosystem, we'd like you to design an IAM RBAC implementation that focuses on supporting each of brightwheel's engineering teams. The solution should prevent any privilege escalation attacks within IAM and should consider Cost Analysis, Security, Automation, Monitoring and Logging. Assume that Brightwheel has three different environments: Dev, QA and Production

Assume that each environment uses the same set of AWS Services:

- CloudFront
- EKS
- Redshift

Consider the implementation for the following teams:

- Frontend Engineering - Requires access to CloudFront
- Backend Engineering - Requires access to EKS
- Data Engineering - Requires access to Redshift
- Site Reliability Engineering - Administrators

Implementation Requirements

The solution should be delivered as a Github project consisting of one or more of the following:
- CloudFormation templates
- CDK implementation
- Terraform Implementation
- Any other solution that creates an RBAC implementation in AWS.

Please include a README file in the repository that contains the following information:

- High-level Overview of the Implementation
- How users of the system are managed
- Any additional assumptions that were made

Please spend no more than two hours on the implementation, and include a brief write-up (or outline) in the README describing what the next steps in the project would be, given more time.

How We'll Review

Functionality: Does the solution provided implement RBAC?
Organization: Is the project well structured and easy to understand?
Extensibility: Is the project easy to extend for future needs?
Security: Does the solution protect production customer information?