Condo Daily Report 9-9-21

Wednesday

* Cloudformation
  + S3 stack
    - Perms set
    - Bucket policy creation
      * This allows access into bucket from cloudwatch and cloudtrail
  + Cloud monitoring stack
    - Made a cloud trail log group
      * This is necessary for transporting the logs from acloudtrail to a cloudwatch log group to an s3 bucket
      * Incorporated a flow log
        + Decided to do flow log monitoring by subnet instead

This is useful because it will isolate incidents to resolve the threat faster

* + - * + Made it so the flow log dumps the logs into the s3 bucket from the s3 stack
  + CloudTrail
    - Created a cloudtrail trail to monitor api calls
      * Referenced the log group arn that I created above
      * Needed to create a cloudwatchlogs role
        + This proved difficult because I didn’t know exactly what permissions it needed

The stack kept rolling back and I wasn’t sure why

I didn’t know if it was syntax or a permissions error.

I started playing around with the cloudwatchlogsrole that I created externally of cloudformation in IAM

Regular cloudtrail perms didn’t work

Full cloud trial perms didn’t work

Read only access s3 perms didn’t work

I gave the role admin privileges to check if it was a priv error

The stack built making me believe it was

I decided to pass s3 read, cloudtrail read, and acloudwaatch logs perms and that seemed to do the trick

I may change this in the future to give minimum perms for the task at hand

* + CloudTrail role
    - Used the IAM resource in cloudformation to make the role upon stack creation so it will be deleted when the stack is deleted
      * It worked and I passed the reference to the CloudTrail trail which also worked
* Keeper Call
  + Talked about keeper security integration with SSO
* Kayce Call
  + Talked about milestones to hit
  + Talked about goals for the next year
  + Talked about projects we want to create
  + Talked about CI/CD pipelines that will be crucial for the company
  + Talked about roles that would be necessary