Guidance for Baseline Security Assessment on AWS

A baseline security assessment helps customers identify their security vulnerabilities.

1. The AWS user installs the AWS CloudFormation template created for this Guidance. The template deploys an AWS Lambda function along with the necessary AWS Identity and Access Management (IAM) role for the Lambda function.

2. The Lambda function deploys an AWS Well-Architected custom lens.

3. The Lambda function assesses resources in the account and checks if:
   - AWS Secrets Manager is used to store and manage lifecycle of secrets
   - AWS Systems Manager Patch Manager is used for patch management
   - Amazon CloudFront is used to deliver static content
   - Amazon Virtual Private Cloud (Amazon VPC) is configured correctly to setup a secure, isolated network
   - AWS CloudTrail is setup for audit purposes
   - AWS Cost Explorer billing alarms are configured
   - AWS Cost Anomaly Detection is setup
   - Amazon Simple Storage Service (Amazon S3) is configured correctly to prevent public access

4. The AWS Well-Architected custom lens questions are answered by the Lambda function to complete the automated assessment.

5. The AWS user navigates to the console in the AWS Well-Architected Tool to view and download the assessment report.