EC2 Security Group Audit & Tagging - AWS Lambda

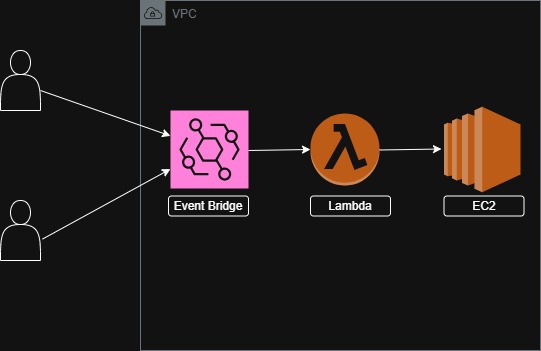
# 1. Index

1. Index  
2. Description  
3. Architecture  
4. Functionality

# 2. Description

This project uses an AWS Lambda function to scan all running EC2 instances and identify those using security groups that allow unrestricted access (i.e., 0.0.0.0/0 or ::/0). If such a group is found attached to an instance, the instance is tagged with InsecureSecurityGroup=NeedsReview. This supports CIS Benchmark 4.1 compliance.

# 3. Architecture Diagram

****

# 4. Functionality

1. Scans all running EC2 instances.  
2. Retrieves their attached security groups.  
3. Detects any overly permissive ingress rules (0.0.0.0/0 or ::/0).  
4. Tags instances with InsecureSecurityGroup=NeedsReview.  
5. Skips instances that are already tagged.  
6. Logs the tagging and skipping in CloudWatch Logs.  
7. Optionally, you can visualize execution metrics using CloudWatch and Grafana.