**Scenaios 2:Security Compliance Checks Using AWS Lambda**

**Scenario**

**You need to automatically enforce security policies across multiple AWS accounts and regions to ensure compliance with organizational standards. For example:**

* **No overly permissive security groups (e.g., 0.0.0.0/0 on SSH port 22)**
* **S3 buckets should not be publicly accessible**
* **IAM roles and policies follow least privilege principles**

**Manual auditing is error-prone and time-consuming, so you want an automated solution.**

**Solution Overview**

* **Use AWS Lambda functions to run compliance scans on schedules (e.g., daily or hourly).**
* **Lambda checks security configurations like Security Groups, S3 bucket policies, IAM policies, etc.**
* **Lambda generates compliance reports.**
* **If violations are detected, Lambda can remediate automatically (e.g., revoke open access) or send alerts (email, Slack, SNS).**
* **Use AWS Config rules or CloudWatch Events to trigger Lambda.**
* **Centralized monitoring dashboard via CloudWatch, SNS, or third-party tools.**

**Architecture Diagram (Conceptual)**

**less**

**CopyEdit**

**[CloudWatch Event Schedule] ---> [AWS Lambda Compliance Checker] --->**

**/ | \**

**Checks SGs, S3, IAM Reports violations via SNS/Email Applies auto-remediation**

**Step-by-Step Workflow**

1. **Triggering the Lambda Function**
   * **Set up a CloudWatch Event Rule to trigger Lambda on a schedule (e.g., every day at midnight).**
   * **Lambda runs with an IAM role that has permissions to describe security groups, S3 bucket policies, IAM roles, and more.**
2. **Security Group Scanning**
   * **Lambda uses EC2 APIs (describe-security-groups) to fetch all security groups.**
   * **For each security group, inspect inbound/outbound rules.**
   * **Flag rules with overly permissive CIDRs (e.g., 0.0.0.0/0) on sensitive ports (SSH 22, RDP 3389, database ports).**
3. **S3 Bucket Policy Checks**
   * **Lambda lists all S3 buckets (list-buckets).**
   * **For each bucket, retrieves bucket policy and ACL.**
   * **Check for public access blocks, public read/write permissions.**
   * **Flag buckets violating policies.**
4. **IAM Policy Checks**
   * **Use IAM APIs (list-roles, get-role-policy) to examine roles and attached policies.**
   * **Identify policies with wildcard actions or overly permissive permissions.**
   * **Flag risky configurations.**
5. **Report Generation**
   * **Compile a structured report (JSON or CSV) with details of violations.**
   * **Store the report in S3 or send directly via email/SNS.**
6. **Automatic Remediation (Optional)**
   * **Based on severity, Lambda can revoke risky permissions:**
     + **Remove open CIDRs from Security Groups.**
     + **Apply public access block on S3 buckets.**
     + **Disable or detach risky IAM policies.**
   * **Record actions taken in logs for audit.**
7. **Notification and Auditing**
   * **Send alerts with summary via Amazon SNS, email, or integrate with Slack using webhooks.**
   * **Log all compliance check results and remediation actions in CloudWatch Logs or a centralized logging system (e.g., ELK stack).**