AWS Cloud Incident Response Automation Project

This document provides a complete implementation guide and documentation for the AWS Cloud Incident Response Automation Platform project.

## Step 1: Enable Amazon GuardDuty

- Enable GuardDuty via Console or CLI.  
- Collects CloudTrail, VPC Flow Logs, DNS logs.  
- Simulate findings using 'create-sample-findings'.

## Step 2: Enable AWS CloudTrail

- Record API activity across all regions.  
- Store logs in an S3 bucket.  
- Enable log validation and optionally CloudTrail Insights.

## Step 3: Enable AWS Config

- Track resource configuration changes.  
- Store logs in S3.  
- Use AWS managed rules for compliance checks.

## Step 4: Enable AWS Security Hub

- Centralize findings from GuardDuty, Config, etc.  
- Enable AWS Foundational Best Practices and CIS Benchmark.  
- View and filter findings in Security Hub.

## Step 5: Create Amazon SNS for Alerts

- Create an SNS topic and email subscription.  
- Confirm email.  
- Test using manual message.

## Step 6: Create IAM Role for Lambda

- Create role with policies for EC2, SNS, and CloudWatch Logs.  
- Attach role to Lambda function for remediation actions.

## Step 7: Create Lambda Function

- Use Python to stop EC2 instance and send SNS alerts.  
- Parse GuardDuty event to extract instance ID.  
- Log actions in CloudWatch.

## Step 8: Create EventBridge Rule

- Create a rule for GuardDuty findings.  
- Filter for severity >= 5 and EC2 findings.  
- Set Lambda as target.

## Step 9: Simulate GuardDuty Finding

- Use CLI to generate sample findings.  
- Verify automation: EC2 stopped, SNS email received.