# How to integrate your application with Amazon GuardDuty using AWS CLI

## Step 1: Install and Configure AWS CLI

Install AWS CLI :

- On windows, download the installer from AWS CLI Installation and follow the instructions.
- On macOS, use Homebrew:

```
Brew install awscli
```

- On Linux, use the package manager for your distribution.

Configure AWS CLI: Open your terminal and run

```
Aws configure
```

Follow the prompts to enter your AWS Access Key, Secret Key, region and output format.

## Step 2: Set Up AWS Config

Create a Configuration Recorder:

```
Aws configservice
put-configuration-recorder-configuration-recorder
```

```
name=default,roleARN=arn:aws:iam::YOUR_ACCOUNT_ID:role/ROLE_NAME,recordingGroup={allSupported=true}
```

Replace YOUR_ACCOUNT_ID and ROLE_NAME with your account ID and IAM role name.

Start the Configuration Recorder :

```
Aws configservice
start-configuration-recorder—-configuration-recorder-name default
```

Step 3: Select Resources to Record

Step up Delivery Channel :

```
Aws configservice put-delivery-channel
—-delivery-channel name=default,
s3BucketName=YOUR_S3_BUCKET,snsTopicARN=arn:aws:sns:YOUR_REGION:YOUR_ACCOUNT_ID:YOUR_SNS_TOPIC
```

Replace YOUR_S3_BUCKET, YOUR_REGION, YOUR_ACCOUNT_ID and YOUR_SNS_TOPIC with your specific details .

Step 4 : Define Configuration Rules

Create a Config Rule :

```
Aws configservice put-config-rule —-config-rule
file://rule.json
```

Create a rule.json file with the necessary rule definition. For example

```
{
 “ConfiguRuleName”: “s3-bucket-public-read-prohibited”,
“Source”: {
“SourceIdentifier”:”S3_BUCKET_PUBLIC_READ_PROHIBITED”
},

“Scope”: {
“ComplianceResourceTypes”:[“AWS::S3::Bucket”]
}
}
```

Step 5: Monitor Configuration Changes

View Configuration History

```
Aws configservice describe-configration-recorder-status
```

Set Up Notifications : Use AWS SNS to set up notifications for compliance changes

```
Awssns subscribe —-topic-arn
arn:aws:sns:YOUR_REGION:YOUR_ACCOUNT_ID:YOUR_SNS_TOPIC
—-protocol email —-notification-endpoint YOUR_EMAIL
```

Replce YOUR_REGION, YOUR_ACCOUNT_ID, YOUR_SNS_TOPIC and YOUR_EMAIL with your details.

## Step 6: Implement Security Best Practices

Ensure Least Privilege Access: Review and update IAM policies to grant only necessary permissions.
Encrypt Data : Ensure your S3 bucket and other resources have encryption enabled.

## Step 7: Integrate with Other AWS Services

AWS Security Hub:

```
Aws securityhub enable-security-hub
```

Follow the prompts to enable and configure AWS Security Hub.

Automated Remediation: Create Lambda function for automatic remediation of non-compliant resources and trigger them using AWS Config rules.