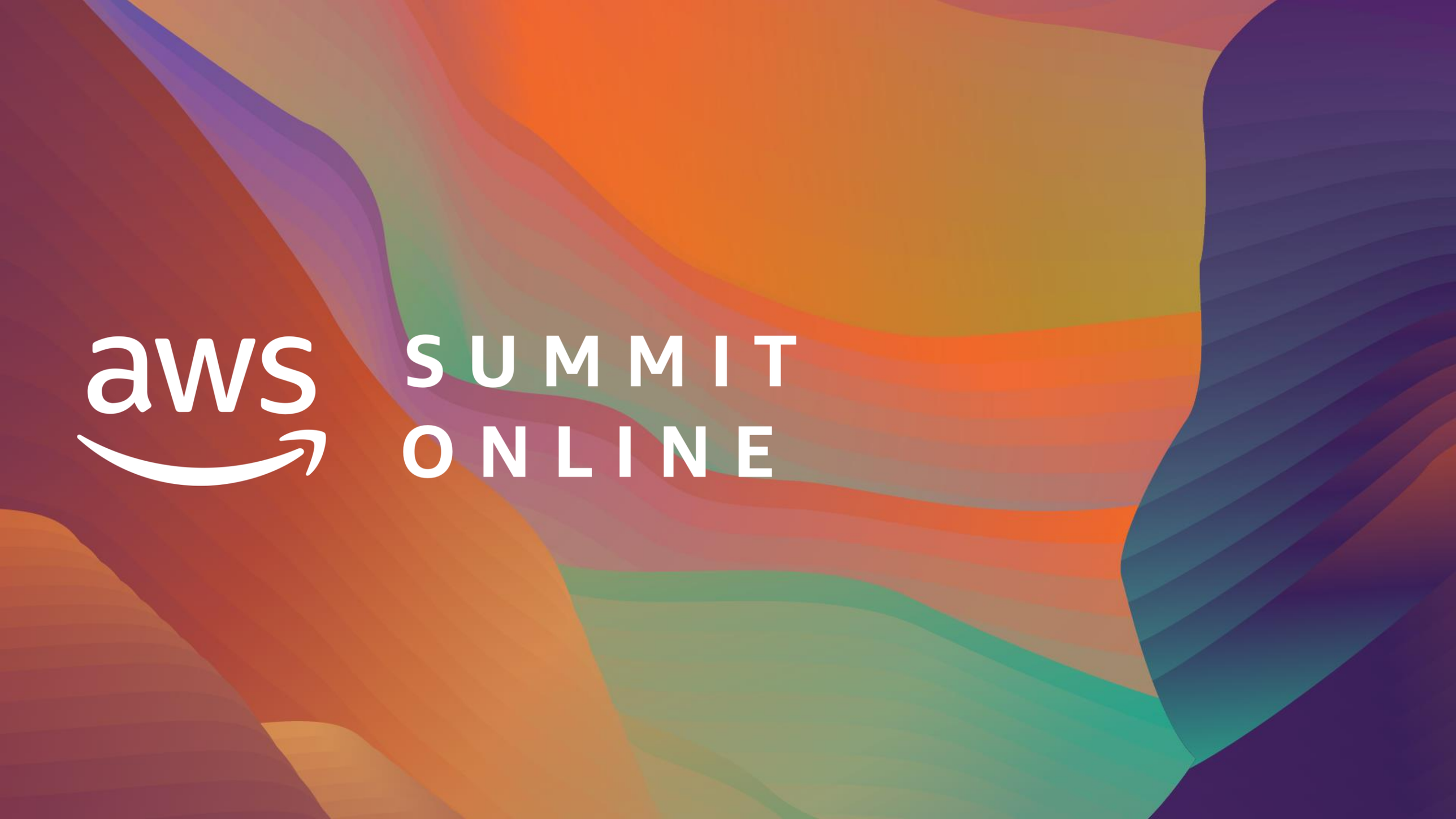

aws
SUMMIT
ONLINE

Security automation toolkit

Gaurav Jagavkar
Solution Architect, AISPL

aws SUMMIT ONLINE

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security Automation

If **THIS** happens, then do **THAT**

Behavior / Configuration / Findings

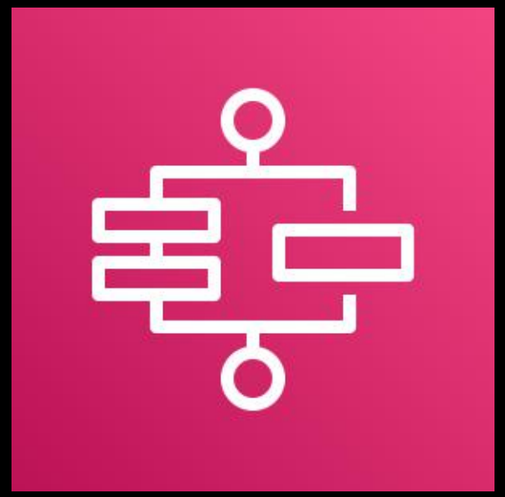
AWS CloudTrail

Amazon CloudWatch

AWS GuardDuty

Notification / Respond / Remediate

Amazon Simple Notification Service



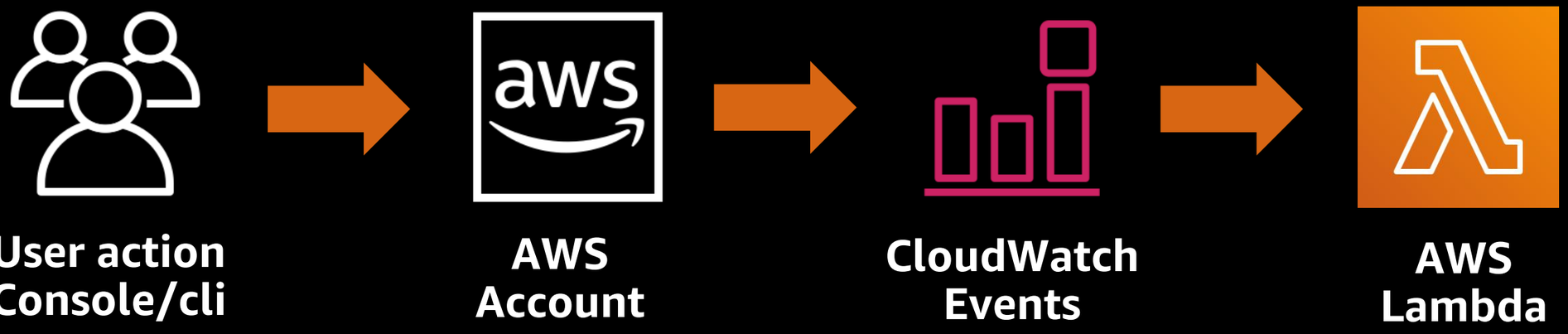
AWS Step Functions

AWS Lambda

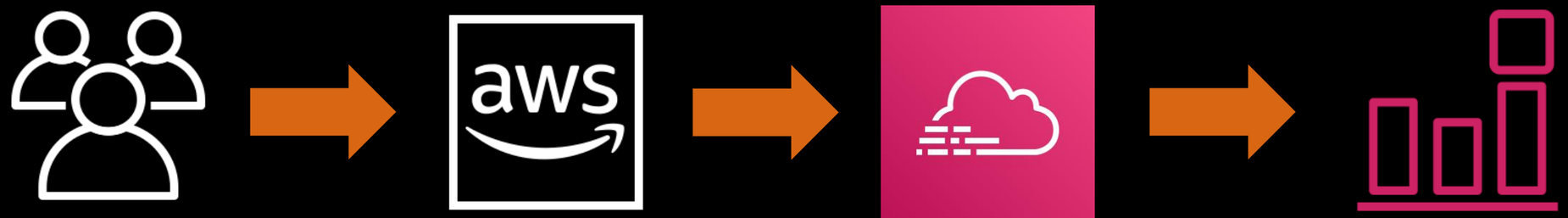
Use case:
“If some one turns OFF AWS CloudTrail, notify me and turn it back ON”

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

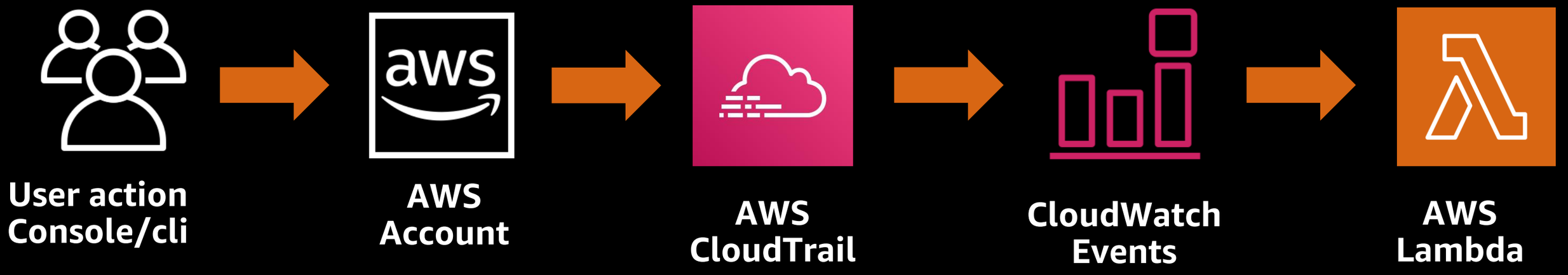
High level play book #1




```
Cloudtrail:StopLogging
```




```
{
    "source": ["aws.cloudtrail"
    ],
    "detail-type": ["AWS API Call via CloudTrail"
    ],
    "detail": {
       "eventSource": ["cloudtrail.amazonaws.com"
       ],
       "eventName": ["StopLogging"
     ]
    }
}
```




```
cloudtrail:start_logging
```

Demo: AWS CloudTrail

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Demo: AWS CloudTrail

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use case:
“Monitor AWS S3 bucket of production data compliance, prohibit public read/write, if it FAILS this compliance check, remediate by updating the bucket ACL”

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

User action
Console/cli

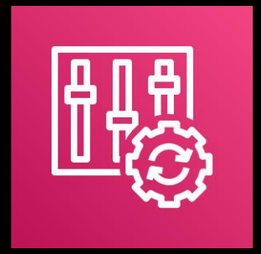
AWS
Account

AWS Config


```
"evaluations": [
 {
     "annotation": "The S3 bucket ACL allows public read access.",
     "orderingTimestamp": "May 7, 2019 7:17:31 AM",
     "complianceResourceType": "AWS::S3::Bucket",
     "complianceResourceId": "customer-data-bucket",
     "complianceType": "NON_COMPLIANT"
 }
]
```

User action
Console/cli

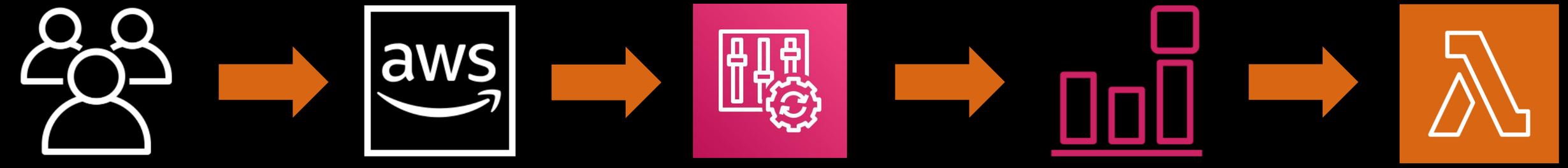
AWS
Account



AWS Config

CloudWatch
Events


```
"complianceResourceId": [
        "customer-data-bucket"
      ],
      "complianceType": [
       "NON_COMPLIANT"
      ]
"additionalEventData": {
     "managedRuleIdentifier": [
      "S3_BUCKET_PUBLIC_READ_PROHIBITED”
     ]
  {
```




```
resource = list(event['detail']['requestParameters']['evaluations'])[0]
    bucketName = resource['complianceResourceId']

s3.put_bucket_acl(Bucket = bucketName, ACL = 'private')
```

Demo: AWS S3 bucket policy change

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use case:
“Monitor firewall ports for compliance. On failure, reset to default and notify.”

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

User action
Console/cli

Security
Group

AWS Config

Edit -securitygroup-remediation

AWS Config evaluates your AWS resources against this rule when it is triggered.

Name* securitygroup-remediation

Description Remediation Security Group

AWS Lambda function ARN* arn:aws:lambda:ap-south-1[redacted]:function:securitygroup-remediation-responder

Edit AWS Lambda function

AWS Config will gain permission to invoke the function by updating the function's access policy.

Trigger

AWS Config evaluates resources when the trigger occurs.

AWS Config now triggers rules periodically without delivering a configuration snapshot. You can access configuration details captured by AWS Config in your rule. Learn more.

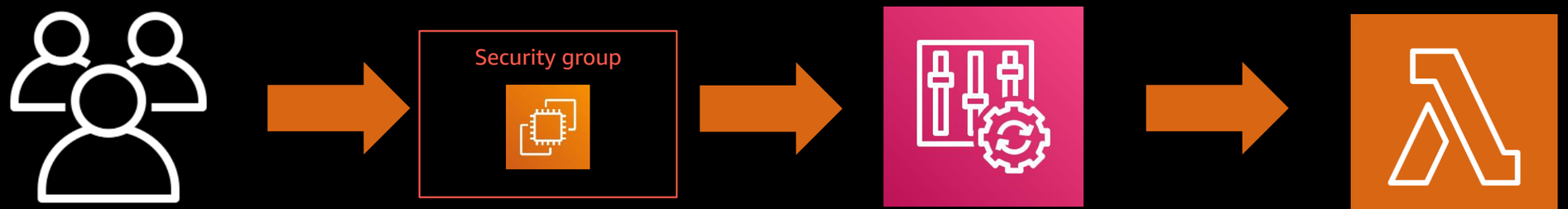
Trigger type* ☑ Configuration changes ☐ Periodic

Scope of changes* ◉ Resources ○ Tags ○ All changes

Resources* EC2: SecurityGroup ×

sg-[redacted]

This rule can be triggered only when recorded resources are created, changed, or deleted. Specify which resources are recorded on the Settings page.




```
ip_permissions = response["SecurityGroups"][0]["IpPermissions"]
authorize_permissions = [item for item in REQUIRED_PERMISSIONS if item not in ip_permissions]
revoke_permissions = [item for item in ip_permissions if item not in REQUIRED_PERMISSIONS]


if authorize_permissions:
   client.authorize_security_group_ingress(GroupId=group_id,
IpPermissions=authorize_permissions)
```

Demo: Security Group inbound rule change

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Code Resources

AWS Config rules

https://github.com/awslabs/aws-config-rules

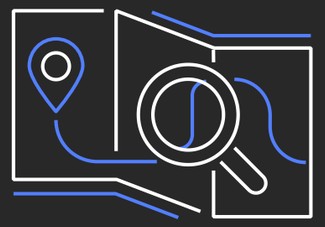
AWS Security automation

https://github.com/awslabs/aws-security-automation

Amazon GuardDuty Hands on

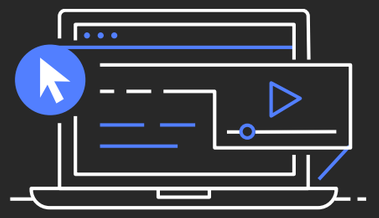
https://github.com/aws-samples/amazon-guardduty-hands-on

AWS Training and Certification



Training for the Whole Team

Explore tailored learning paths for customers and partners



Flexibility to Learn Your Way

Build cloud skills with 550+ free digital training courses, or dive deep with classroom training

Validate Skills with AWS Certification

Demonstrate expertise with an industry-recognized credential

Education Programs

Find entry-level cloud talent with AWS Academy and AWS re/Start

aws.amazon.com/training

Thank you!

aws SUMMIT ONLINE

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.