AWS CloudTrail

@2018 CHAITANYA GAAJULA - ALL RIGHTS RESERVED

Agenda

- What is Cloud Trail ?
- Benefits
- How it Works ?
- Integration with Lambda and CloudWatch
- Demo & Lab

@2018 CHAITANYA GAAJULA - ALL RIGHTS RESERVED

What is CloudTrail?

- AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account.
- With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure.
- CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.
- Event history simplifies security analysis, resource change tracking, and troubleshooting.

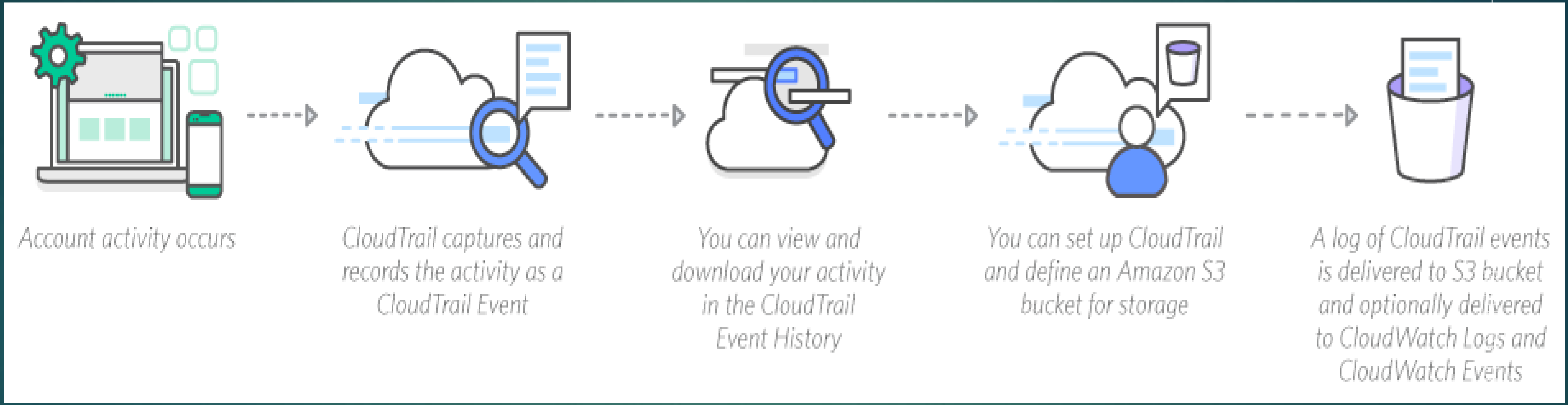
@2018 CHAITANYA GAAJULA - ALL RIGHTS RESERVED

Benefits

- Simplified Compliance
- Visibility into User and Resource Activity
- Security Analysis
- Security Automation

@2018 CHAITANYA GAAJULA - ALL RIGHTS RESERVED

How It Works



Account activity occurs

CloudTrail captures and records the activity as a CloudTrail Event

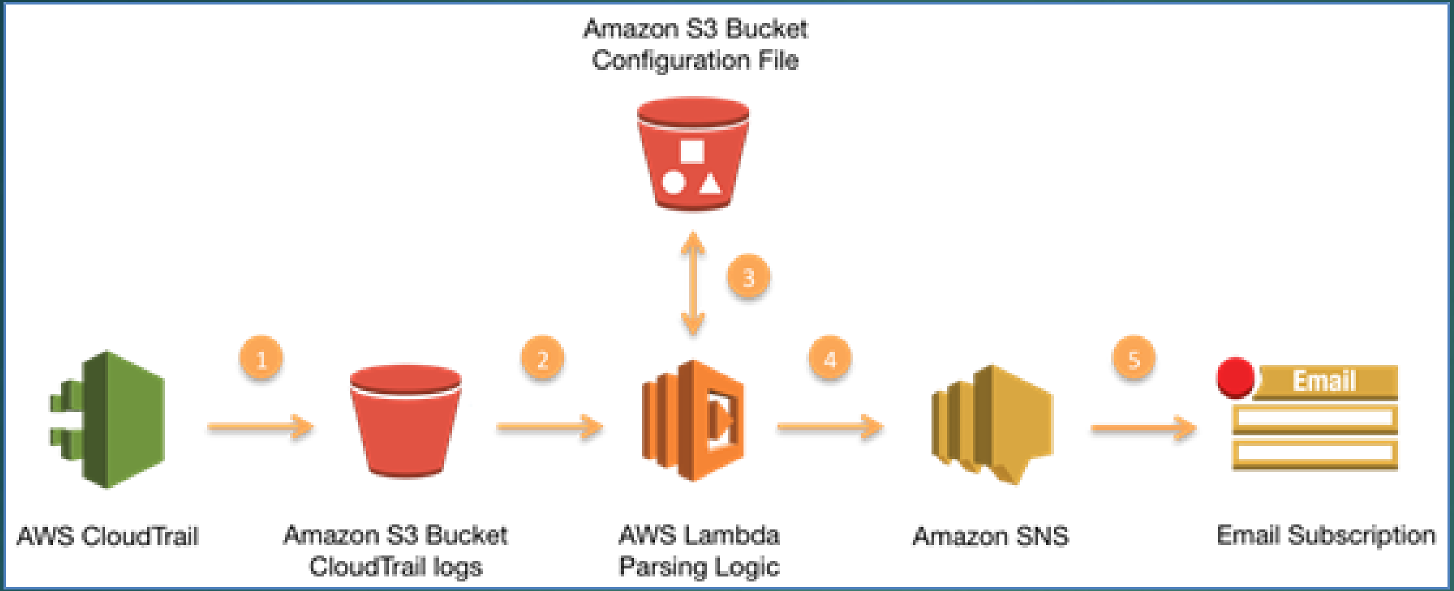
You can view and download your activity in the CloudTrail Event History

You can set up CloudTrail and define an Amazon S3 bucket for storage

A log of CloudTrail events is delivered to S3 bucket and optionally delivered to CloudWatch Logs and CloudWatch Events

@2018 CH
ED

Using CloudTrail and Lambda together



- CloudTrail generates a log entry for every API call made on your account. CloudTrail aggregates the log entries in JSON text files, zips the files, and copies them to the Amazon S3 bucket configured to receive CloudTrail log files.

- The log parsing logic is deployed as a Lambda function. The Lambda function is triggered when CloudTrail copies a new file to your S3 bucket.

- The Lambda function uses a configuration file that contains a list of specific API keywords that, when detected, will trigger a notification. The configuration file is stored in an S3 bucket.

- Whenever relevant keywords are detected in the CloudTrail logs, the Lambda function posts a notification to an SNS topic.

- SNS dispatches the notification to every topic subscriber via email, Amazon SQS, SMS, HTTP call, or mobile push.

@2018 CHAITANYA GAAJULA - ALL RIGHTS RESERVED

Using CloudWatch and CloudTrail together

https://aws.amazon.com/blogs/security/how-to-receive-notifications-when-your-aws-accounts-root-access-keys-are-used/

@2018 CHAITANYA GAAJULA - ALL RIGHTS RESERVED

DEMO & LAB

@2018 CHAITANYA GAAJULA - ALL RIGHTS RESERVED

THANK YOU

@2018 CHAITANYA GAAJULA - ALL RIGHTS RESERVED