Using Amazon CloudWatch for Incident Response

Mike Brown
SENIOR CLOUD INSTRUCTOR

@mgbleeds

Overview

Discuss event driven automation

Understand automated event management and healing

Work with CloudWatch event rules to invoke Step Functions

Course and module review

Understanding Event Driven Automation

Globomantics

Support teams receive daily updates on the status of their services

Security teams receive email alerts when a security event is reported

Time to detect and resolve issue is measured in hours

We have been asked to

- Improve Globomantics response time to performance, availability and security issues

Automation is the key to success

A Stepped Approach

Detect

CloudWatch events, event bridge and logs

Respond

Configure automation to respond to detected events

Report

Alert the relevant teams and log event and response

Events and Logging

CloudWatch events or EventBridge

AWS Config

S3 event notifications

Logs include

- CloudTrail
- VPC Flow Logs
- AWS WAF Logs
- And more.....

AWS Config rules

Amazon CloudWatch

AWS Inspector

Amazon GuardDuty

Amazon Macie

Amazon Detective

Visibility and Alerting

Automation

AWS Lambda

Serverless compute that can run code in response to events

AWS Step Functions

Easily coordinate a set of steps in response to an event

AWS Systems Manager

Visibility and control of your infrastructure

Our Goal

Better response

Improve out mean time to detect (MTTD) and our mean time to resolve (MTTR)

Innovate

Spend our time on the next big thing and improving what we have

What areas would you like to automate?

Globomantics

Support

Automate response to failures

Security

Detect and respond to security threats

Report

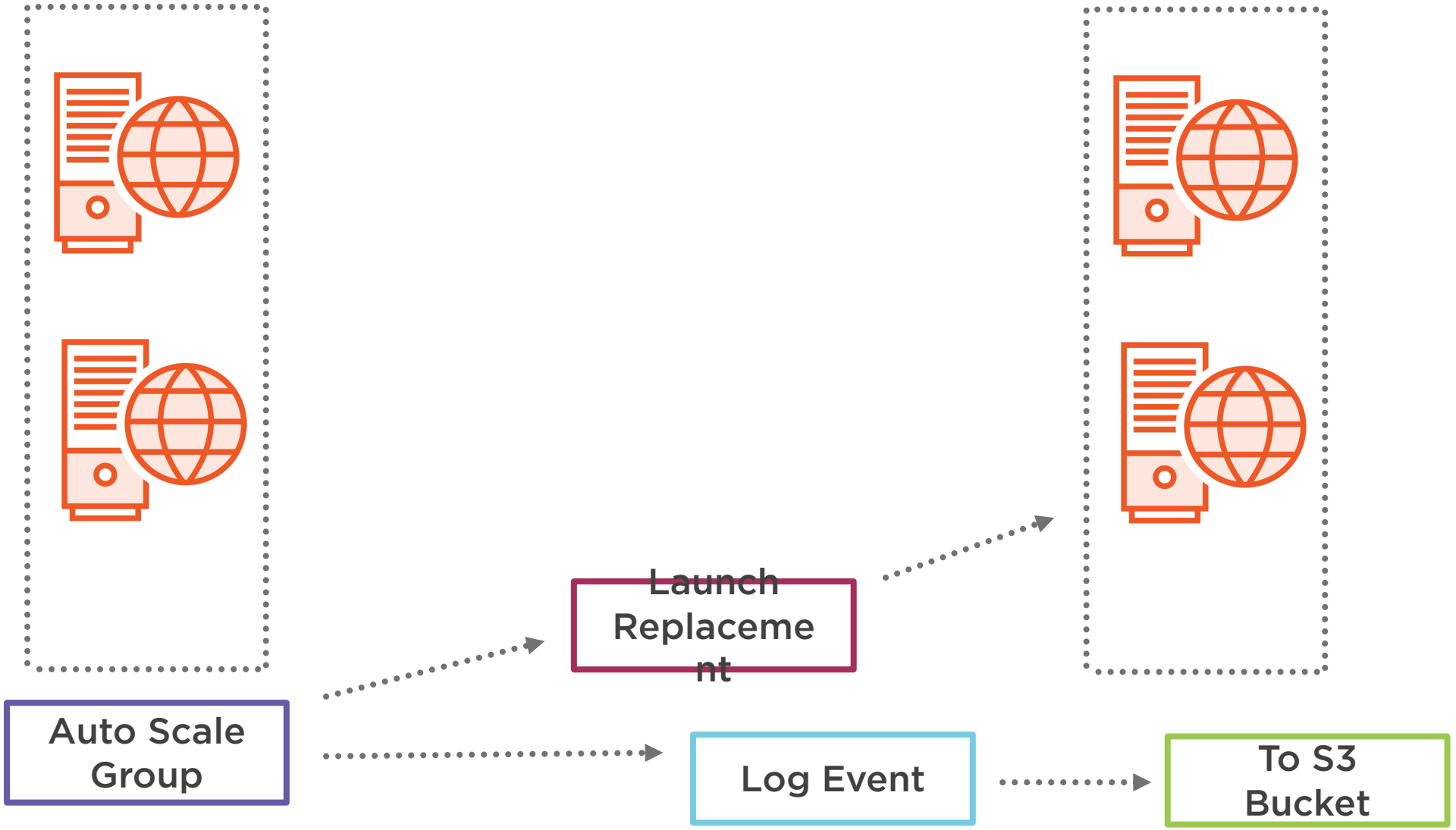
Log both the event and the automated response to the event

Understanding Automated Event Management and Healing

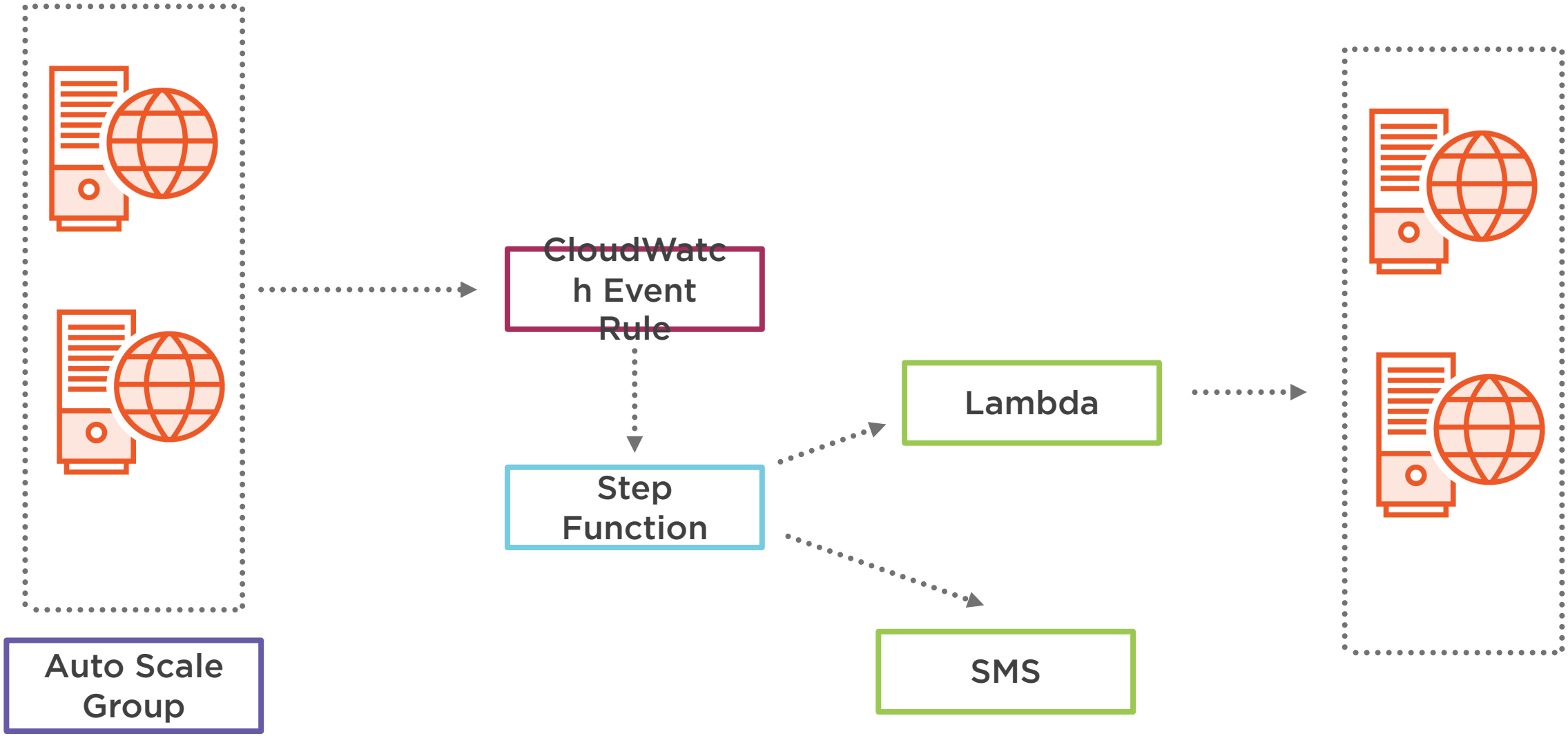
Where possible let the system heal itself and report the results to us

Scenario 1: Automate the deployment of new infrastructure if there is a failure

Scenario 1: Possible Solution 1

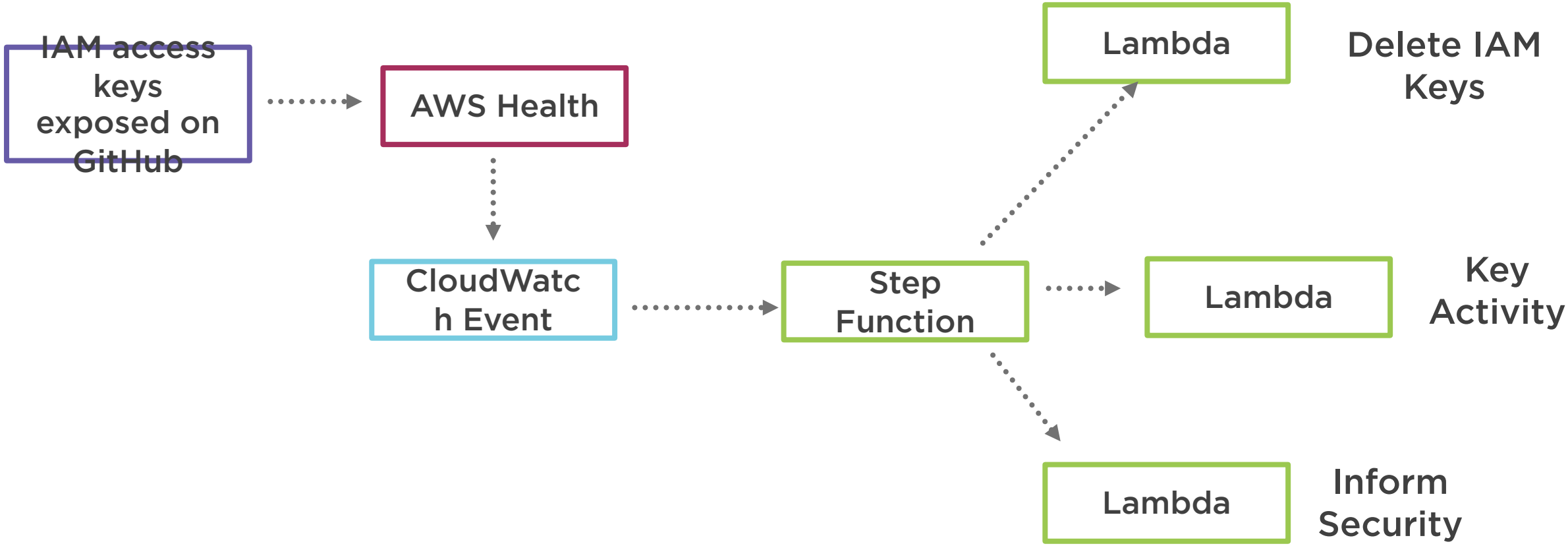


Scenario 1: Possible Solution 2



Scenario 2: IAM access keys publicly exposed

Scenario 2: Possible Solution



How could your organization benefit from automated healing?

Automation, Visibility and Control

Use CloudFormation to automate deployments

Consider tools like Elastic Beanstalk

Consider containers and using the Elastic Kubernetes Service (EKS)

Use Systems Manager for operational insights and control of your infrastructure

Demo

Work with a CloudWatch event rule to invoke a Step Function

Working with

- AWS Console

To follow along you will need an AWS Account

Course and Module Review

Metrics

Dashboards

Alarms

Events

Logs

Log insights

CloudWatch

Event Response

CloudWatch events

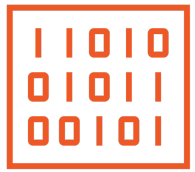
EventBridge

Automation for event response

- Infrastructure
- Security
- Application deployment

CloudTrail

Management events



Data events

Insight events

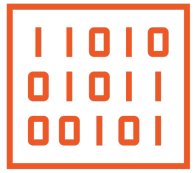
AWS Tags

- Cost allocation
- Grouping resources
- Software deployments
- Access control

Metadata

Used to provide instance details to our EC2 deployed applications

Used to provide role information to our EC2 deployed applications



Used to provide user data to EC instances

Automation is the key to success

Summary

Learned the power of event driven automation

Discussed automated healing

Course review