AWS re:Invent

ENT312-R

# Automating performance optimization and risk management

**David Schliemann**
Senior Cloud Support Engineer
Amazon Web Services

AWS re:Invent

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws

# Agenda

Challenges of large-scale cloud architectures

Automating to reduce human effort

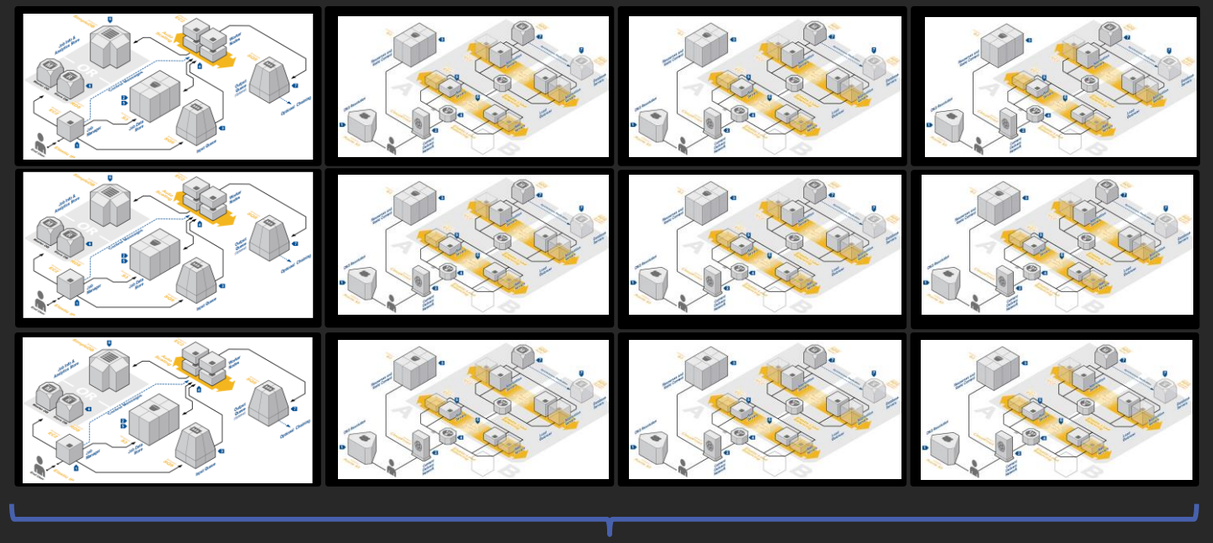
Introduction to monitoring and automation services

Learn how to automatically optimize your AWS environment based on AWS Trusted Advisor best practice recommendations

Learn how to reduce risk by automatically responding to AWS Health events

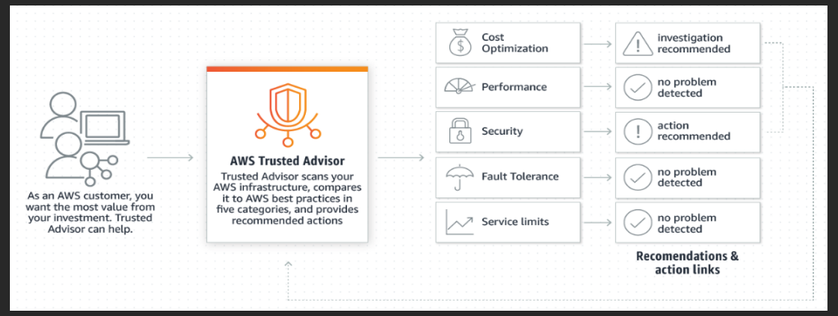
# Complexity Brings Challenges / Risks

- Unexpected bills and unused resources
- Service disruption, events and maintenance
- Lack of fault-tolerance
- Security vulnerabilities
- Performance gaps
- Lots of **heavy lifting for monitoring resources and implementing best practices**

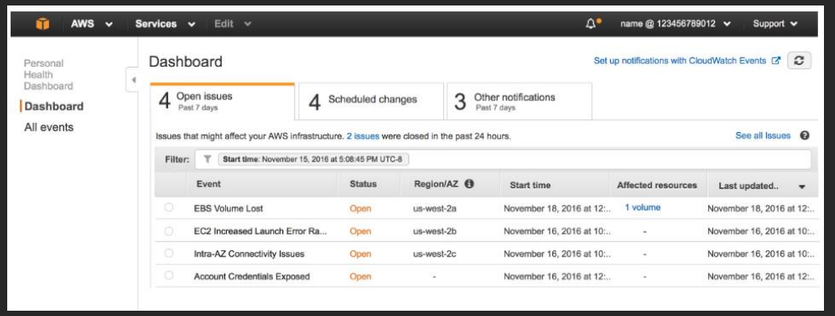


# How to automate your AWS environments?

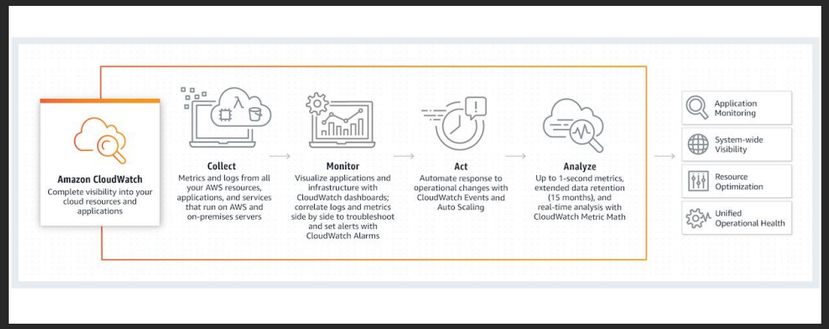
**AWS Trusted Advisor**




**AWS Personal Health Dashboard**




**Amazon CloudWatch**




Amazon EC2

AWS Systems Manager

AWS Batch

AWS Lambda

Amazon Kinesis

AWS CodePipeline

Amazon SQS

Amazon ECS

AWS Step Functions

Amazon SNS

AWS CodeBuild

# AWS Trusted Advisor

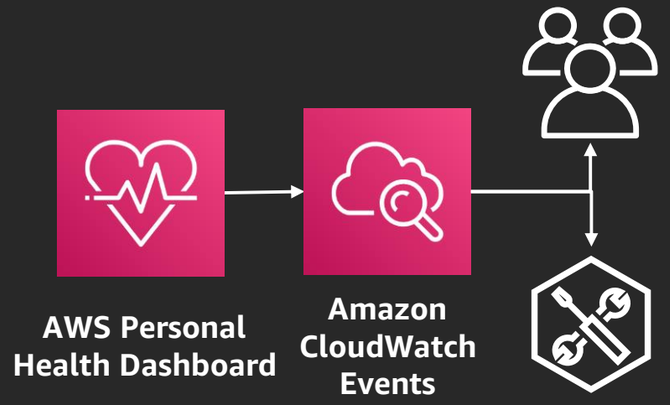
- Taking away the heavy lifting of monitoring best practices
- Trusted Advisor provides best practices (or checks)

Red (action recommended)
Yellow (investigation recommended)
Green (no problem detected)

# AWS Health and AWS Personal Health Dashboard

Visibility and transparency into your resources

Remediation guidance and knowledge articles




Custom notifications and automated actions

# Amazon CloudWatch Events

Amazon CloudWatch

- Near real-time stream of system event changes in Amazon Web Services resources
- Integration with multiple Amazon Web Services as source and targets

**rule**

```
{
  "source": [
    "aws.trustedadvisor"
  ],
  "detail-type": [
    "Trusted Advisor Check Item Refresh Notification"
  ],
  "detail": {
    "status": [
      "ERROR",
      "WARN"
    ]
  }
}
```

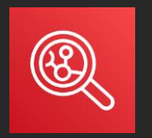
Amazon Kinesis Data Firehose

AWS Step Functions

Amazon SQS

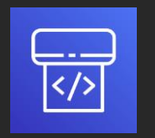
Amazon EC2

AWS Lambda

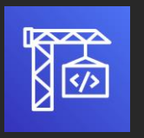


Amazon Inspector

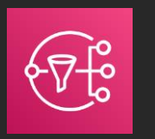
AWS Systems Manager



AWS CodePipeline



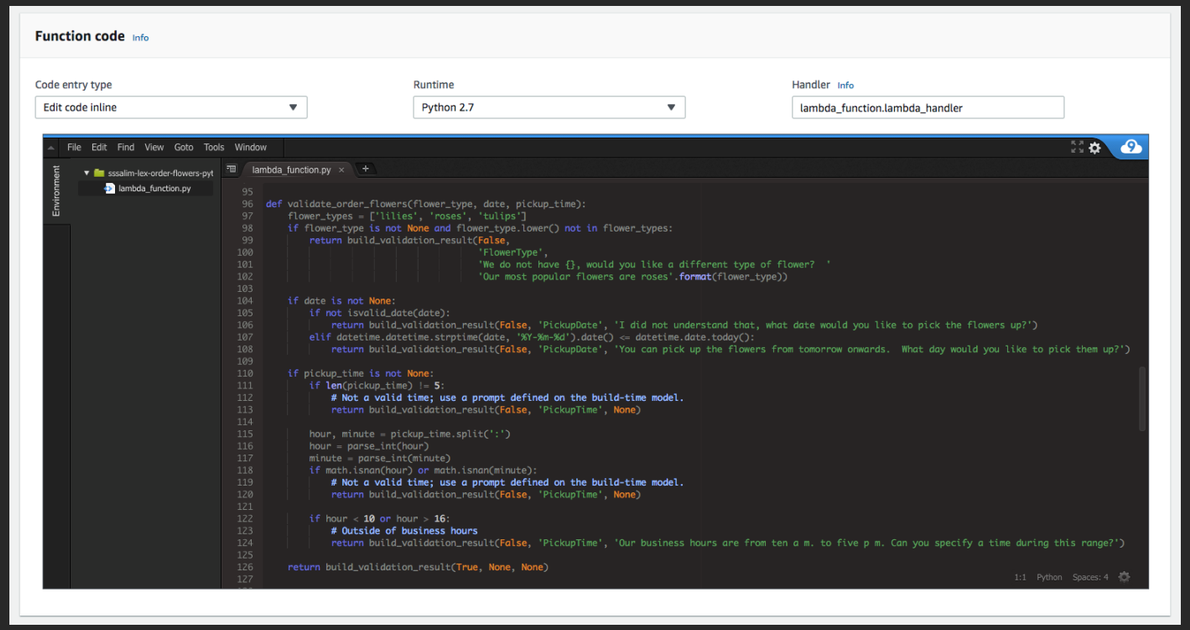
AWS CodeBuild



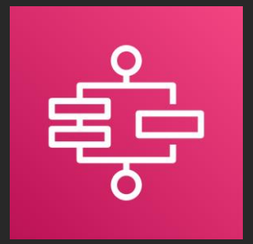
Amazon Simple Notification Service

# AWS Lambda

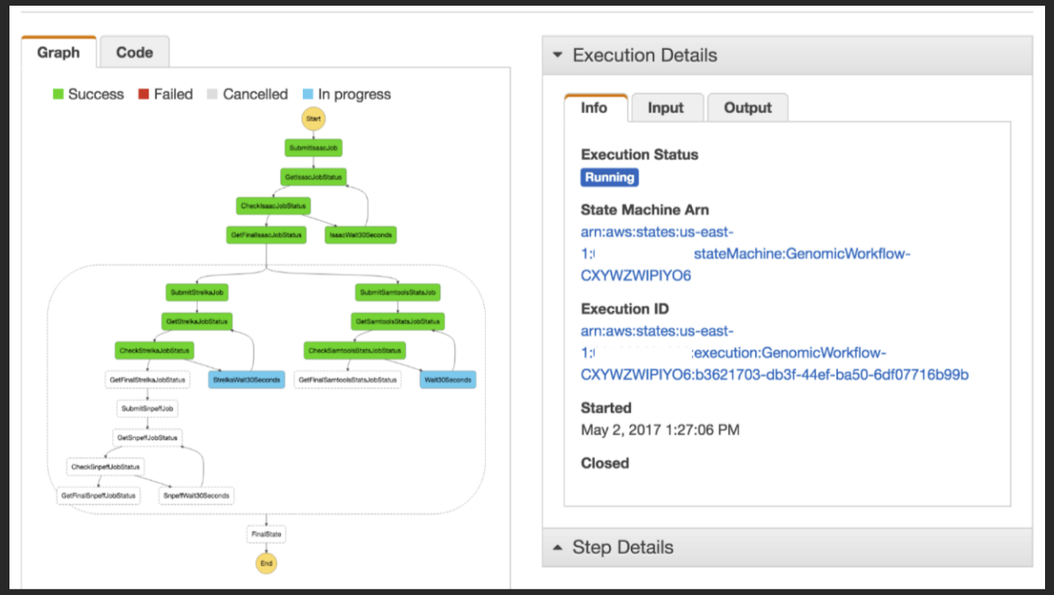
- Allows you to run code without provisioning or managing servers
- Pay per execution of the code rather than the lifetime of the server hosting it
- Supports multiple languages: Java, Python, Go, C#, PowerShell



# AWS Step Functions



- Workflow configuration and abstraction
- Coordination of distributed components
- Component reuse
- State management
- AWS service integrations



# Automation best practices

Define context

Reference resource using tagging / naming convention / AWS CloudFormation

Principal of least privilege

Allow access to necessary API for automation

Think event driven

Detect change leveraging existing service AWS Config / Amazon CloudWatch Event

Think serverless

Use serverless

# Scenario 1: High-utilization Amazon EC2 instances

## https://github.com/aws/aws-health-tools



© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EC2 instances overutilized

Performance

**High-utilization Amazon EC2 instances:**

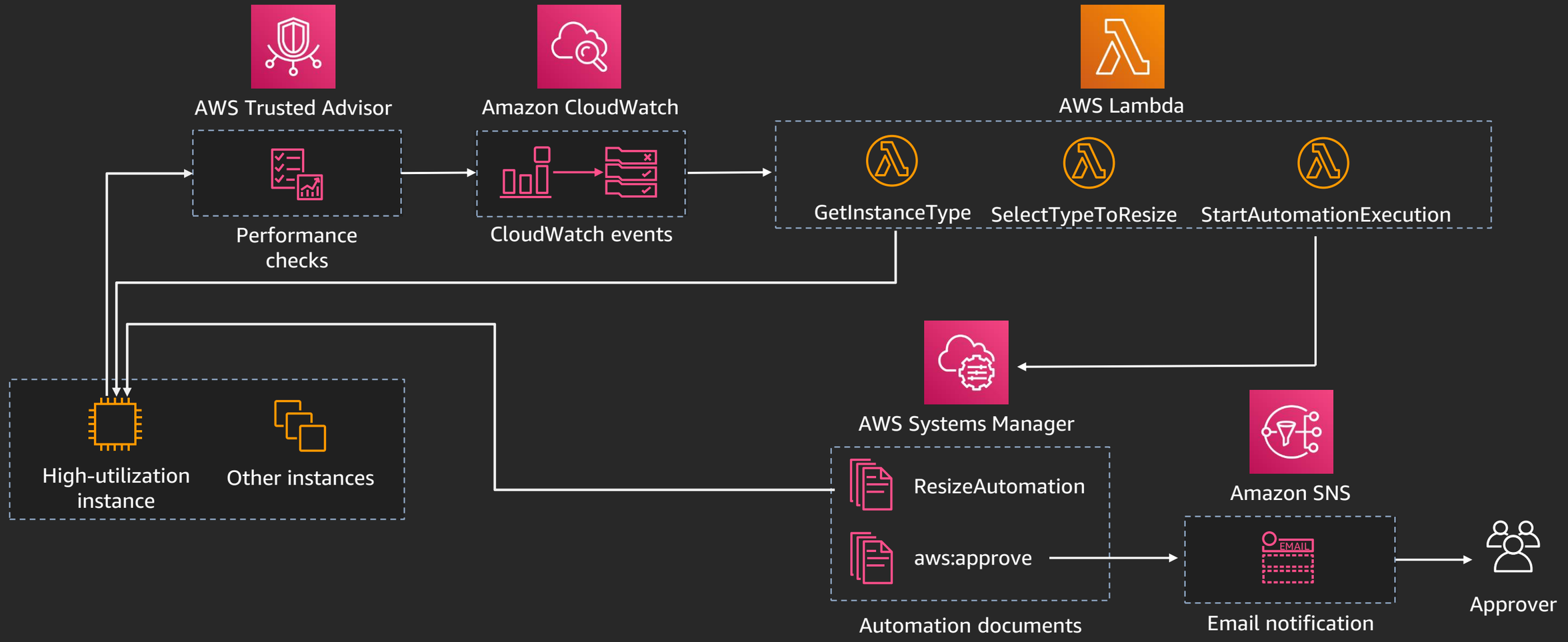
- Checks Amazon EC2 instances that were running at any time during the last 14 days and alerts if the daily CPU utilization was more than 90% on four or more days

**Why:**

- Consistent high utilization may indicate application does not have enough resources
- This may lead to a regression in application performance

Amazon EC2

# Resize high CPU EC2 instance type (with approval)



# Scenario 2: AWS Health DoS abuse report

## https://github.com/aws/aws-health-tools

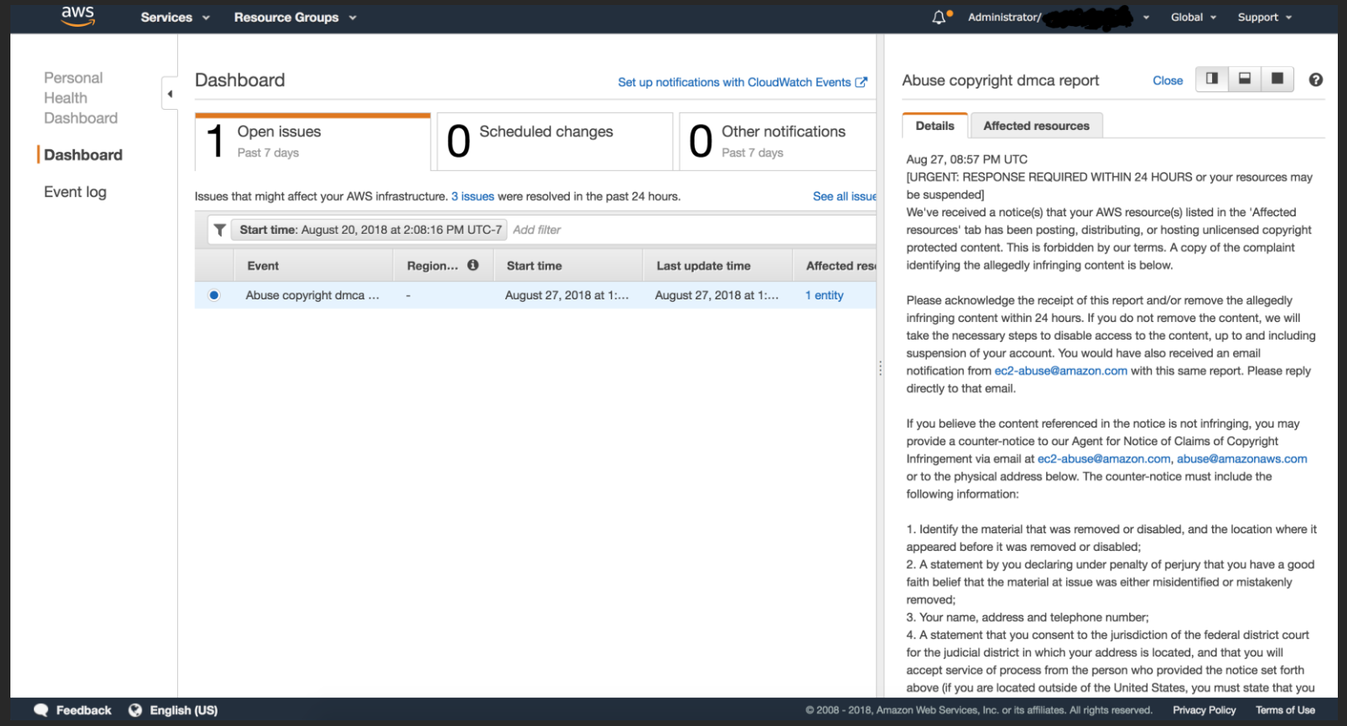


© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS Health abuse events

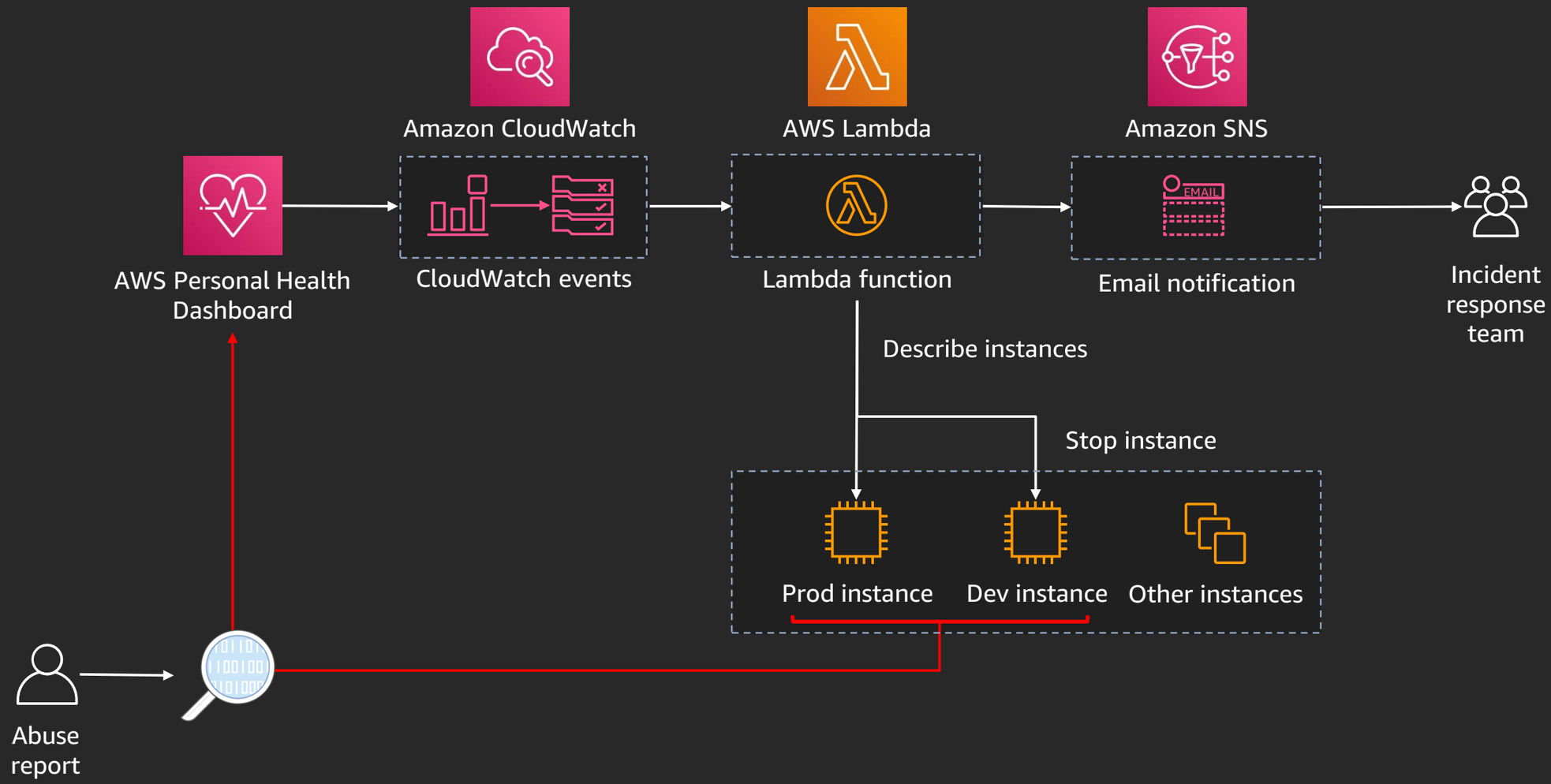
## Programmatically capture abuse events to notify relevant parties and take automation action in AWS Health for the following:

- Sending email spam
- Spamming online forums or other websites
- Hosting a site advertised in spam
- Excessive web crawling
- Intrusion attempts (e.g., SSH or FTP)
- Exploit attacks (e.g., SQL injections)
- Hosting unlicensed copyright-protected material
- Phishing website
- Website hosting viruses / malware
- Credit card fraud
- Open proxy
- Port scanning




https://aws.amazon.com/blogs/mt/automating-processes-for-handling-and-remediating-aws-abuse-alerts/

# AWS Health DoS abuse report automation



# Pro tips

- Stopping the offending instances
  - Safest approach
  - Instances disabled until operations can inspect
- Disabling network access via firewall
  - AWS Systems Manager Run Command
  - Permits real-time inspection while abuse is ongoing
- Lock down security groups and network ACLs
  - Dangerous as other resources may be using them

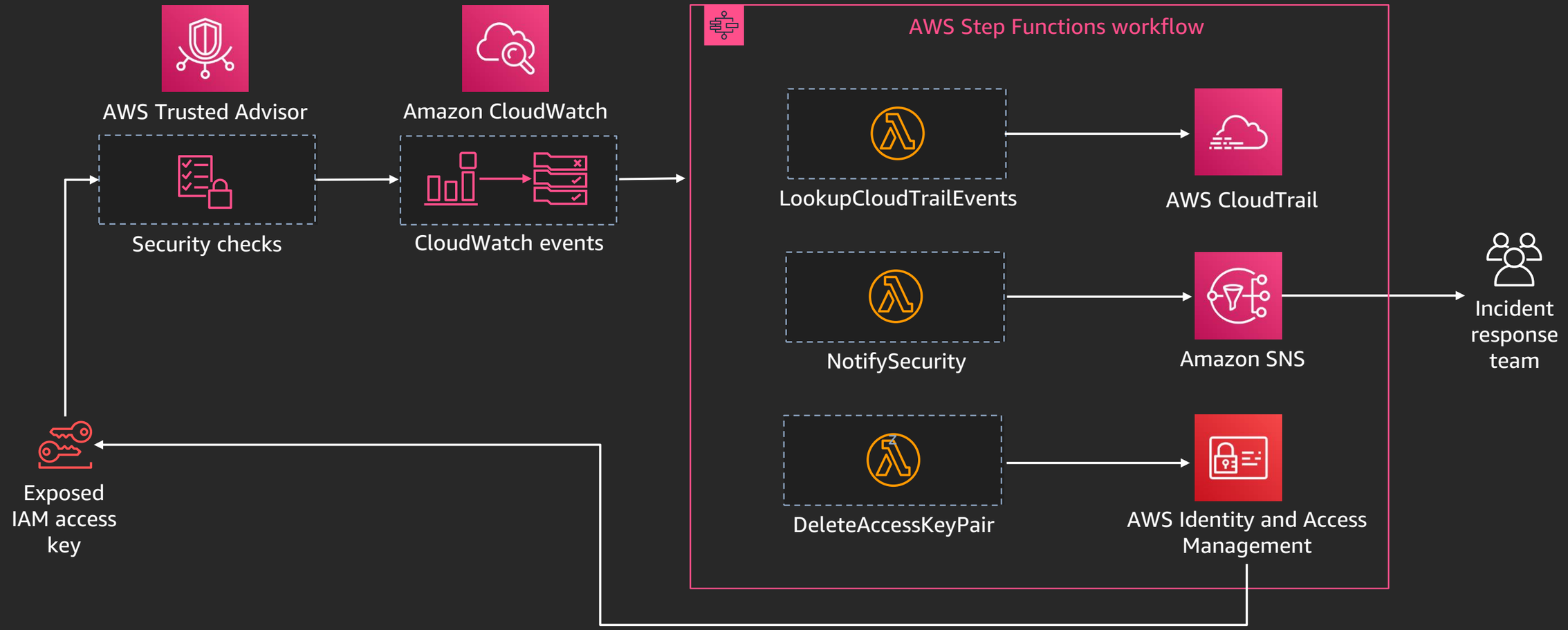
# Bonus scenario: Key deletion for exposed AWS IAM keys

## https://github.com/aws/Trusted-Advisor-Tools



© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Key deletion of exposed IAM keys



# Pro tips

- Deleting credentials
  - Blunt hammer, but effective
- Extend workflow to rotate key
  - Create a second access key
  - Update applications to use the new access key
  - Validate the applications are working
  - Change the state of the previous access key to inactive
  - Validate that your applications are still working
  - Delete the inactive access key
- (Optional) Add approval step
  - Allows teams to identify dependencies on compromised credentials
  - Risk vs. potential downtime

"Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job."

**Jerome Saltzer**

Communications of the ACM



© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

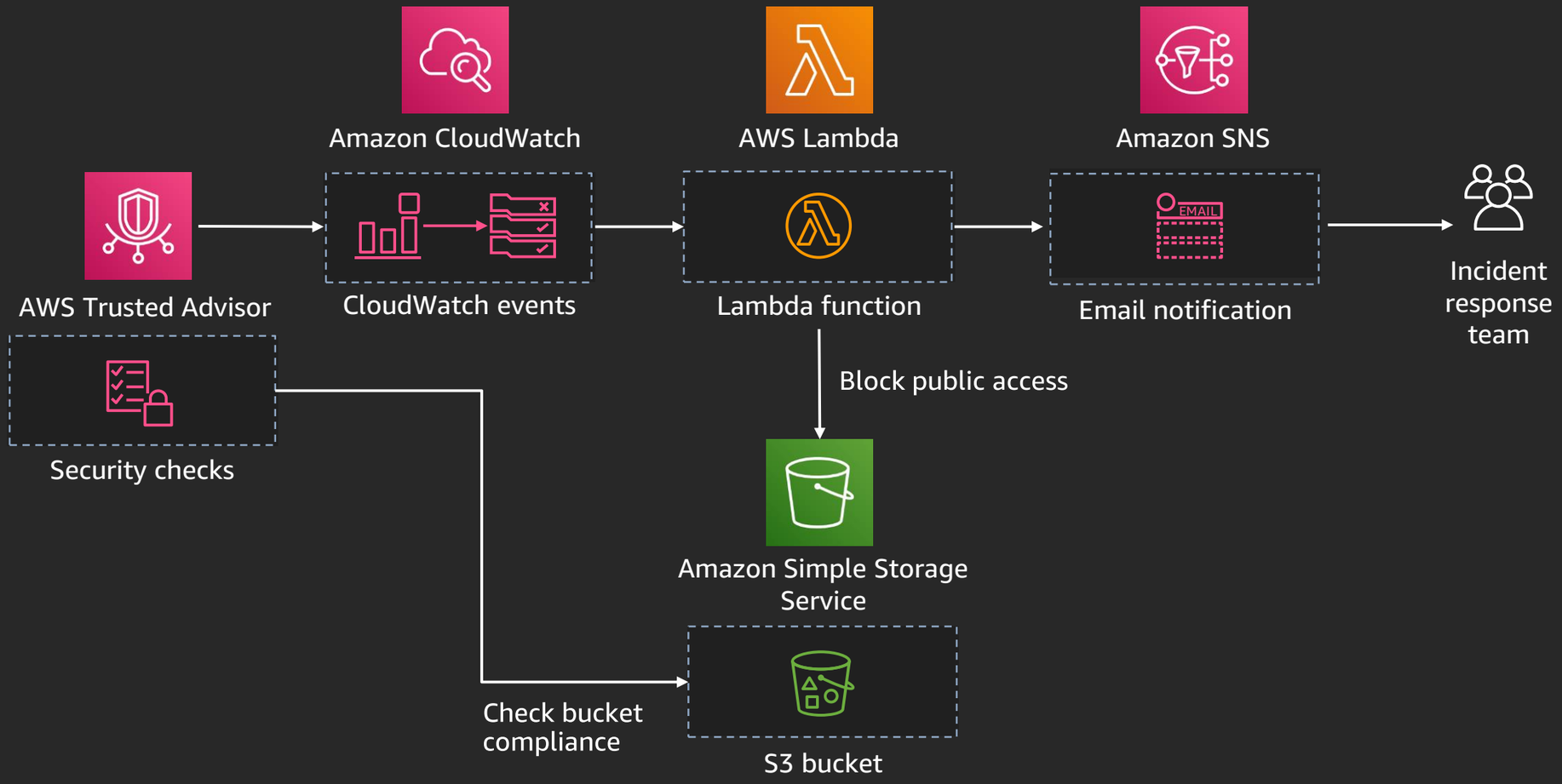
# Bonus scenario 2: Amazon S3 bucket privatizer

AWS re:Invent

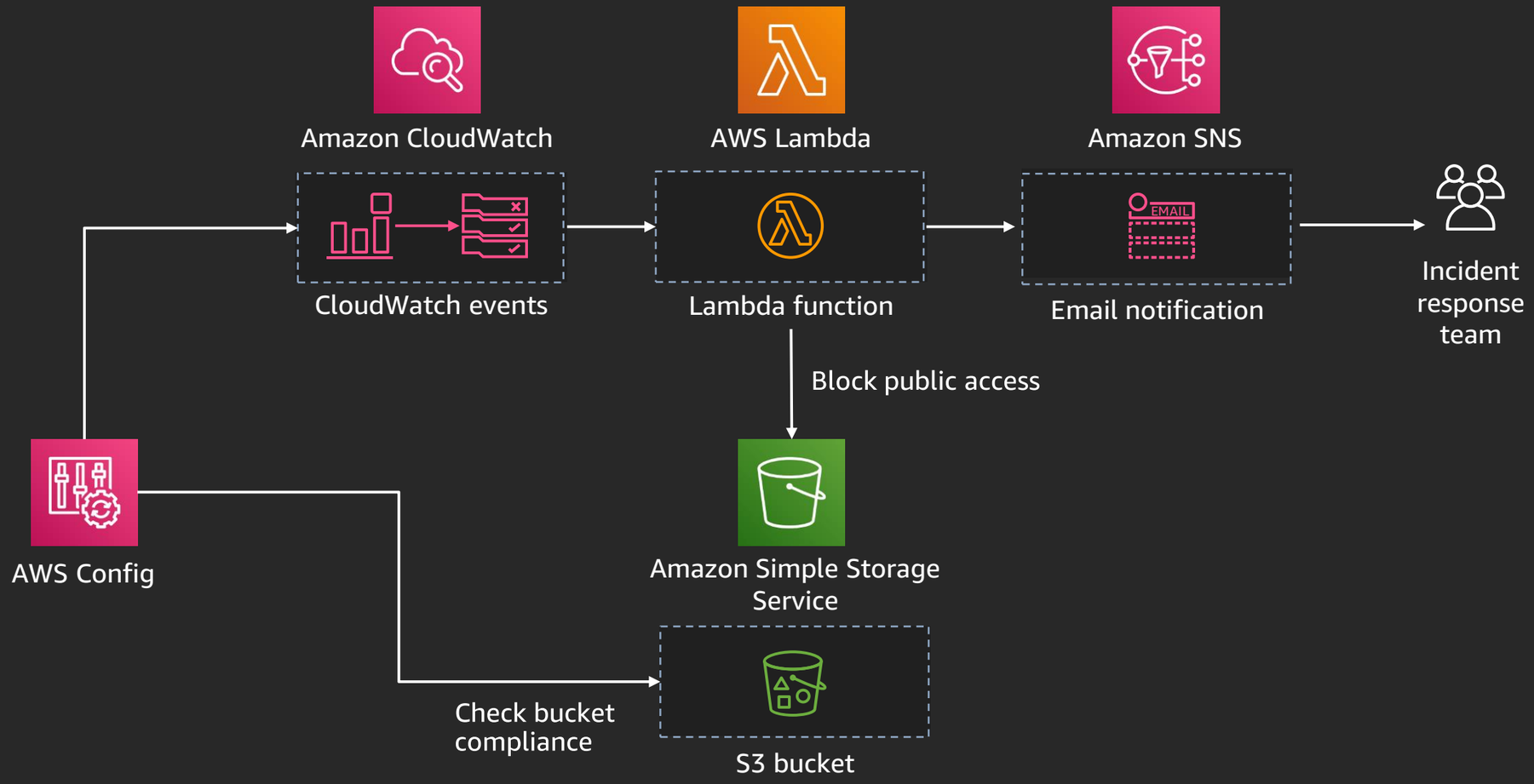
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws

# S3 bucket privatizer



# S3 bucket privatizer (with AWS Config)



# Conclusion

By leveraging Trusted Advisor and AWS Health, you can build automated workflows that adhere to best practices and promote operational health

For step-by-step guides and more automation ideas, please see the samples in the following open-source repositories:

https://github.com/aws/Trusted-Advisor-Tools/

https://github.com/aws/aws-health-tools

# AWS Training and Certification for the enterprise

## Resources to help your organization build cloud skills and achieve business objectives

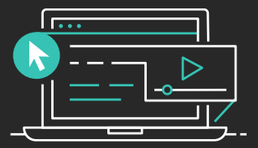
Cost savings (TCO)

Staff productivity

Operational resilience

Business agility

### Comprehensive skill development plan for broad cloud fluency



Digital training

Classroom training

AWS Certification

Enterprise resources

Talent pipeline

Visit aws.amazon.com/training/enterprise

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws training and certification

# AWS customer enablement

## Migrate and build faster in the cloud

**AWS Professional Services**
Accelerate your business outcomes

**AWS Support**
Break-fix, issue resolution, and proactive guidance

**AWS Managed Services**
Operate your AWS infrastructure on your behalf

**AWS IQ**
On-demand help from AWS certified third-party experts

**AWS Training and Certification**
Build skills and validate expertise

**APN Partners**
A global network with deep AWS expertise

# Thank you!

**David Schliemann**

schliema@amazon.com

AWS re:Invent

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws

# Please complete the session survey in the mobile app.



© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.