AWS

SUMMIT

Security at Scale on AWS

Dave Walker – Specialist Solutions Architect, Security and Compliance

Chris Astley – Head of Cloud Ops, Tech Solutions KPMG UK

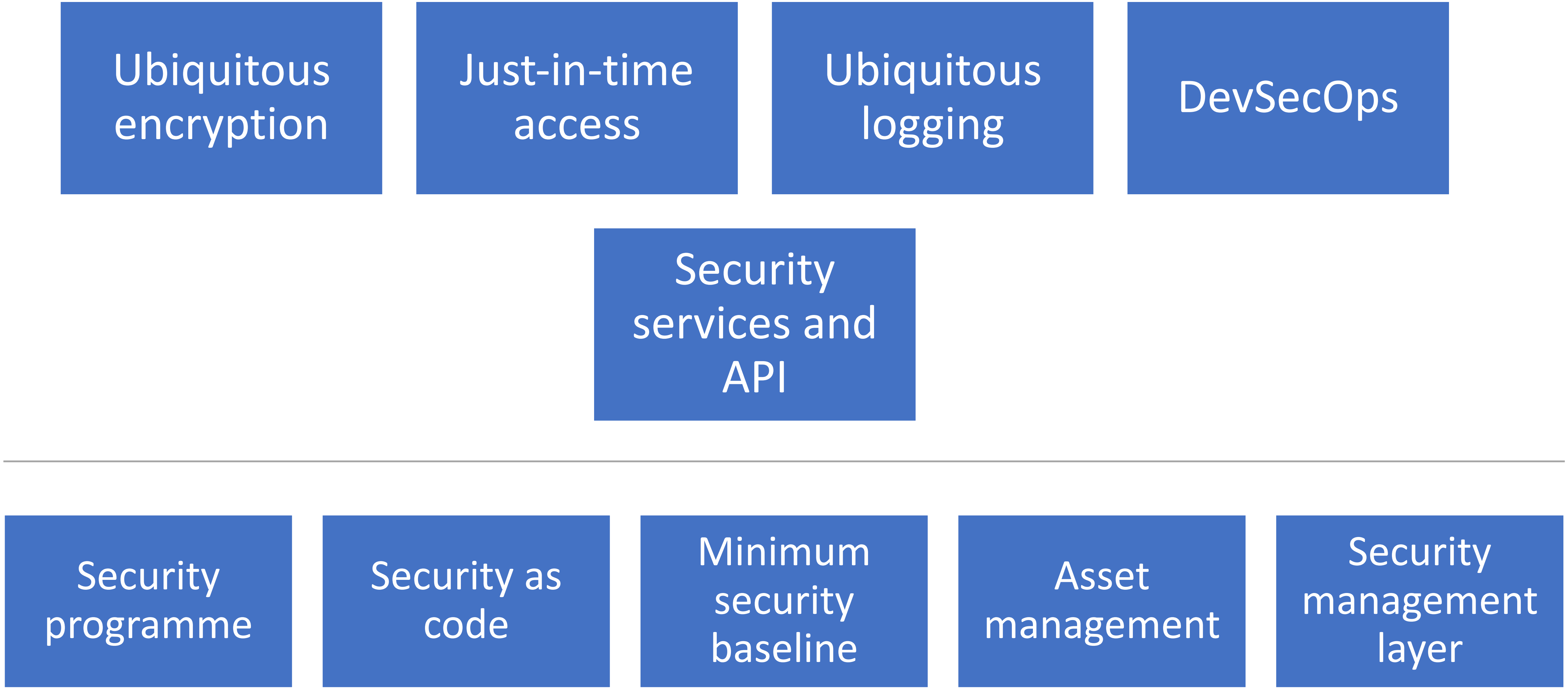
28/06/17

amazon web services

Agenda

- AWS, Approaches and Controls
- AWS and Human Factors
- How AWS Handles Security at Scale
- AWS controls that **<u>you</u>** don’t need to worry about
- Framework to help **<u>you</u>** adapt the cloud Faster
- AWS Services that **<u>you</u>** should be Using
- Reference Architectures that **<u>you</u>** can Use
- Chris @ KPMG!

Approaches Adopted by Successful Security Programmes



Ubiquitous encryption

Just-in-time access

Ubiquitous logging

DevSecOps

Security services and API

Security programme

Security as code

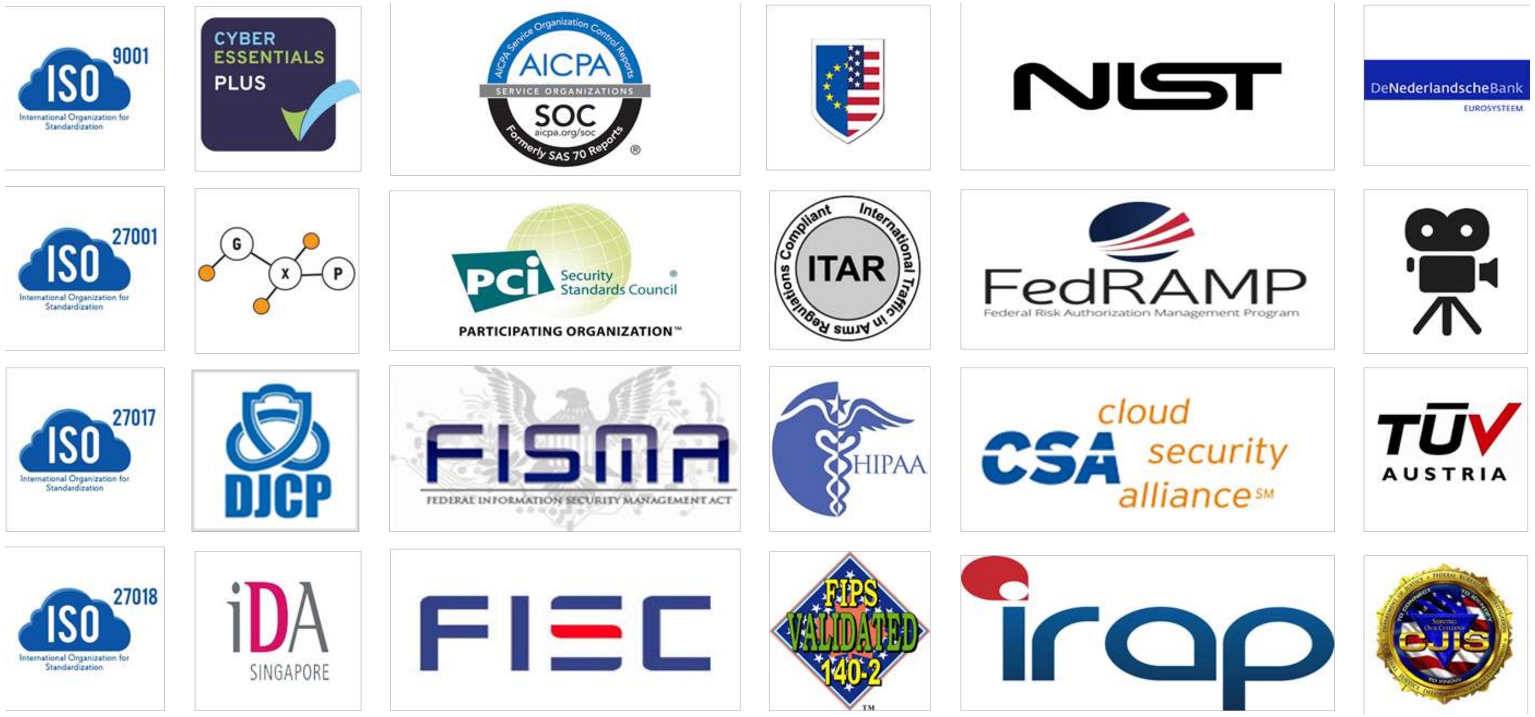
Minimum security baseline

Asset management

Security management layer

AWS Security Controls

70+ services

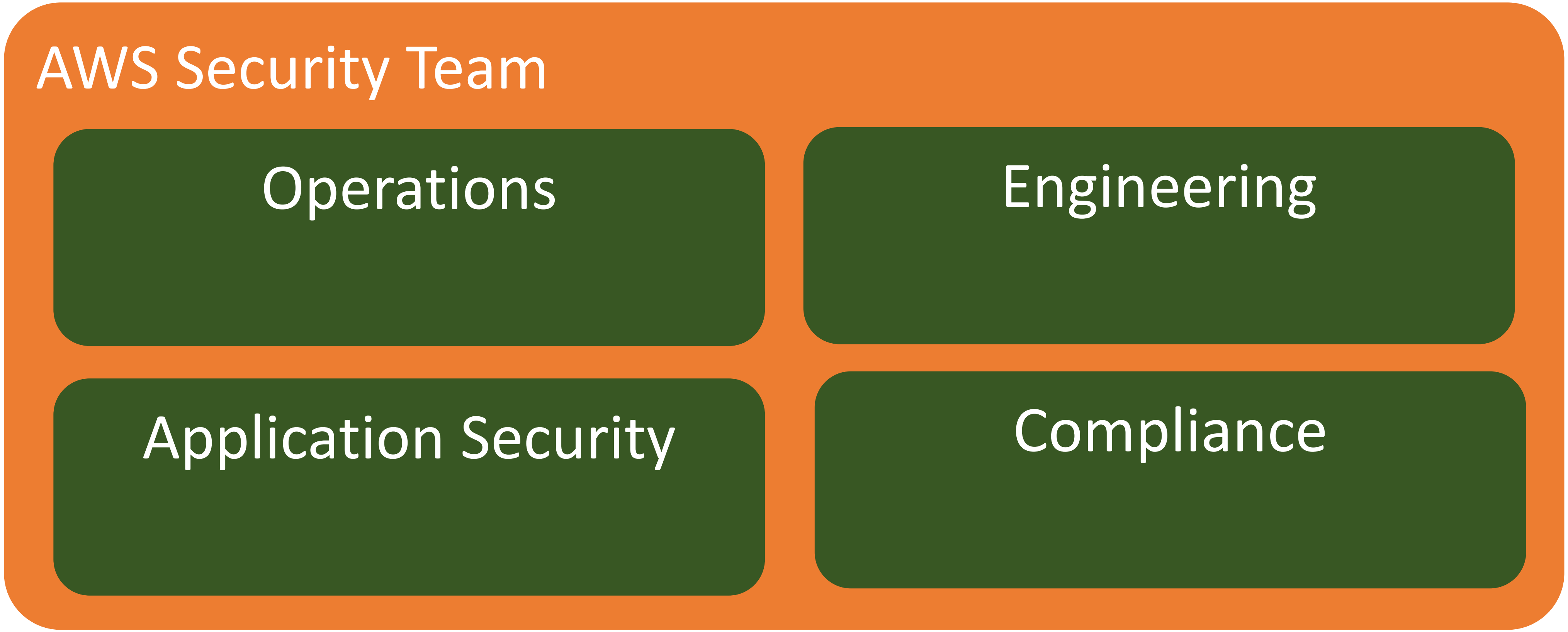

ISO 9001
CYBER ESSENTIALS PLUS
AICPA SERVICE ORGANIZATIONS SOC aicpa.org/soc Formerly SAS 70 Reports
NIST
DeNederlandscheBank EUROSYSTEEM
ISO 27001
G X P
PCI Security Standards Council PARTICIPATING ORGANIZATION
ITAR Compliant International Traffic in Arms Regulations
FedRAMP Federal Risk Authorization Management Program
ISO 27017
DJCP
FISMA FEDERAL INFORMATION SECURITY MANAGEMENT ACT
HIPAA
CSA cloud security alliance
TÜV AUSTRIA
ISO 27018
iDA SINGAPORE
FIEC
FIPS VALIDATED 140-2
irap
CJIS

2,670 Controls

3,030 Audit Requirements

7,710 Audit Artifacts

Human Factors



AWS Security Team

Operations

Engineering

Application Security

Compliance

Aligned for agility

Security Ownership as Part of DNA

Distributed

Embedded

Promotes culture of “everyone is an owner” for security

Makes security stakeholder in business success

Enables easier and smoother communication

Operating Principles

- Separation of duties
- Different personnel across service lines
- Least privilege

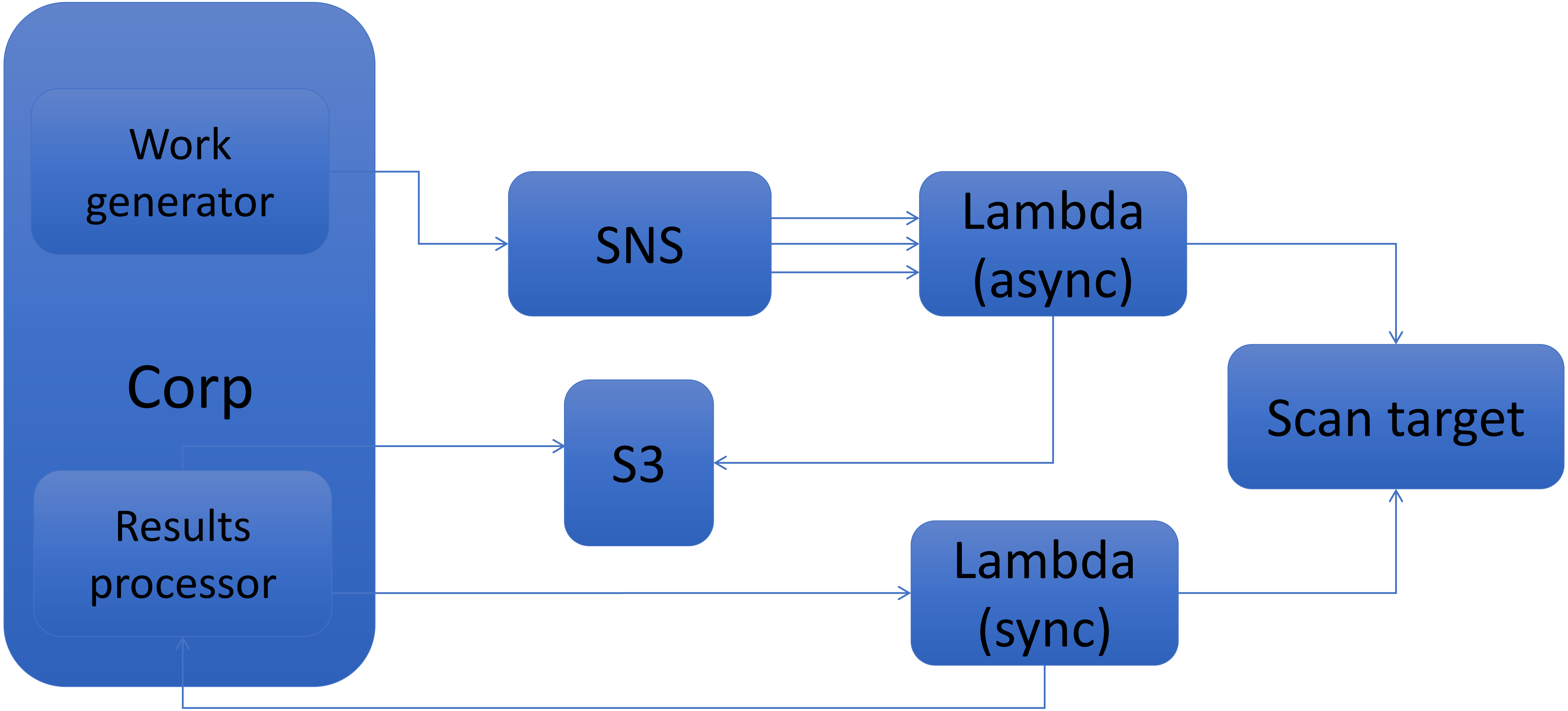
Technology to Automate Operational Principles

Visibility through log analytics

Shrinking the protection boundaries

Ubiquitous encryption

How AWS Handles Security at Scale



How Fast is the Analysis?

- Scan cadence: continual! (not batch)
- Mean time to detect & respond = ~7.5 minutes
    - ~5 min for CloudTrail log file to be produced
    - ~0 min for scan to begin (on order of seconds!)
    - ~0 min scan time (on order of milliseconds!)
    - ~2.5 min for results processor to ticket (runs every 5 min*)
- Worst case: ~10 minutes
- Best case: ~5 minutes

Autoticketing

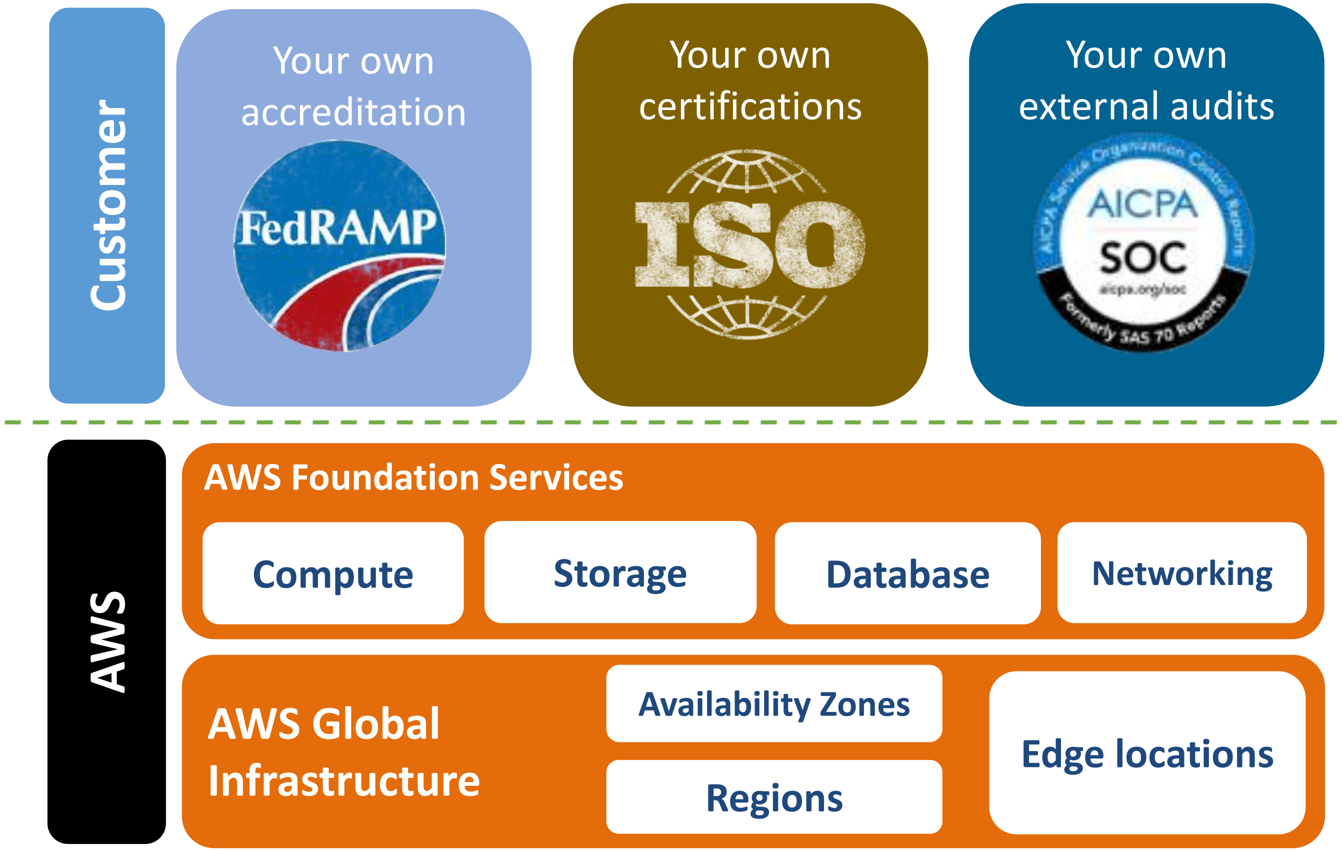
- Find and close gaps in security monitoring
- Be highly accurate and actionable
- Deliver results with low latency

How we make it even faster?

- Drink our own ale! CloudWatch Events
- Increase result processor run frequency
    - It takes < 1 minute per run on average
    - Change invocation to run every minute
    - New worst case = 1 minute
- MTTD ≤ 1 minute
- (For your own use: see eg https://github.com/capitalone/cloud-custodian)

I wish I was a Solid State Drive in someone else's Datacentre…

AWS Security Controls



Customer

Your own accreditation

Your own certifications

Your own external audits

AWS

AWS Foundation Services

Compute

Storage

Database

Networking

AWS Global Infrastructure

Availability Zones

Regions

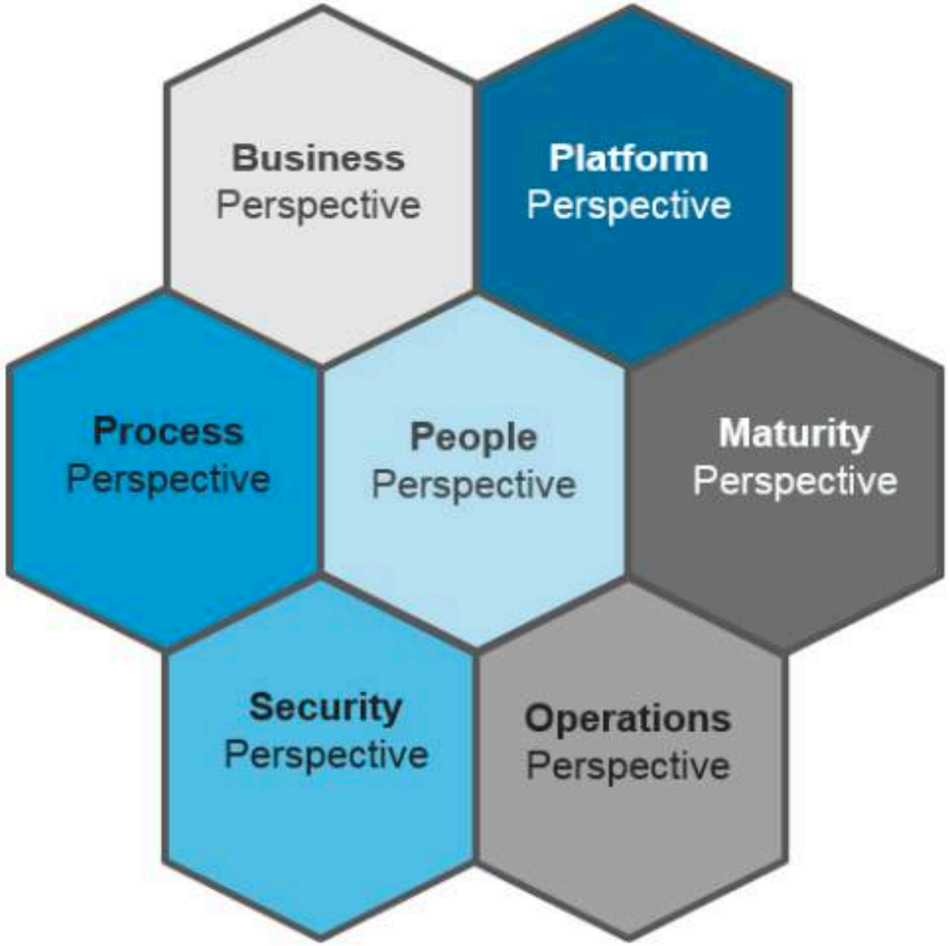
Edge locations

Customer scope and effort is reduced

Better results through focused efforts

Built on AWS consistent baseline controls

AWS Cloud Adoption Framework



- Each *Perspective* provides guidance for different parts of an organization

- Helps **YOU** adapt existing practices or introduce new practices for cloud computing

The Security Journey to the Cloud

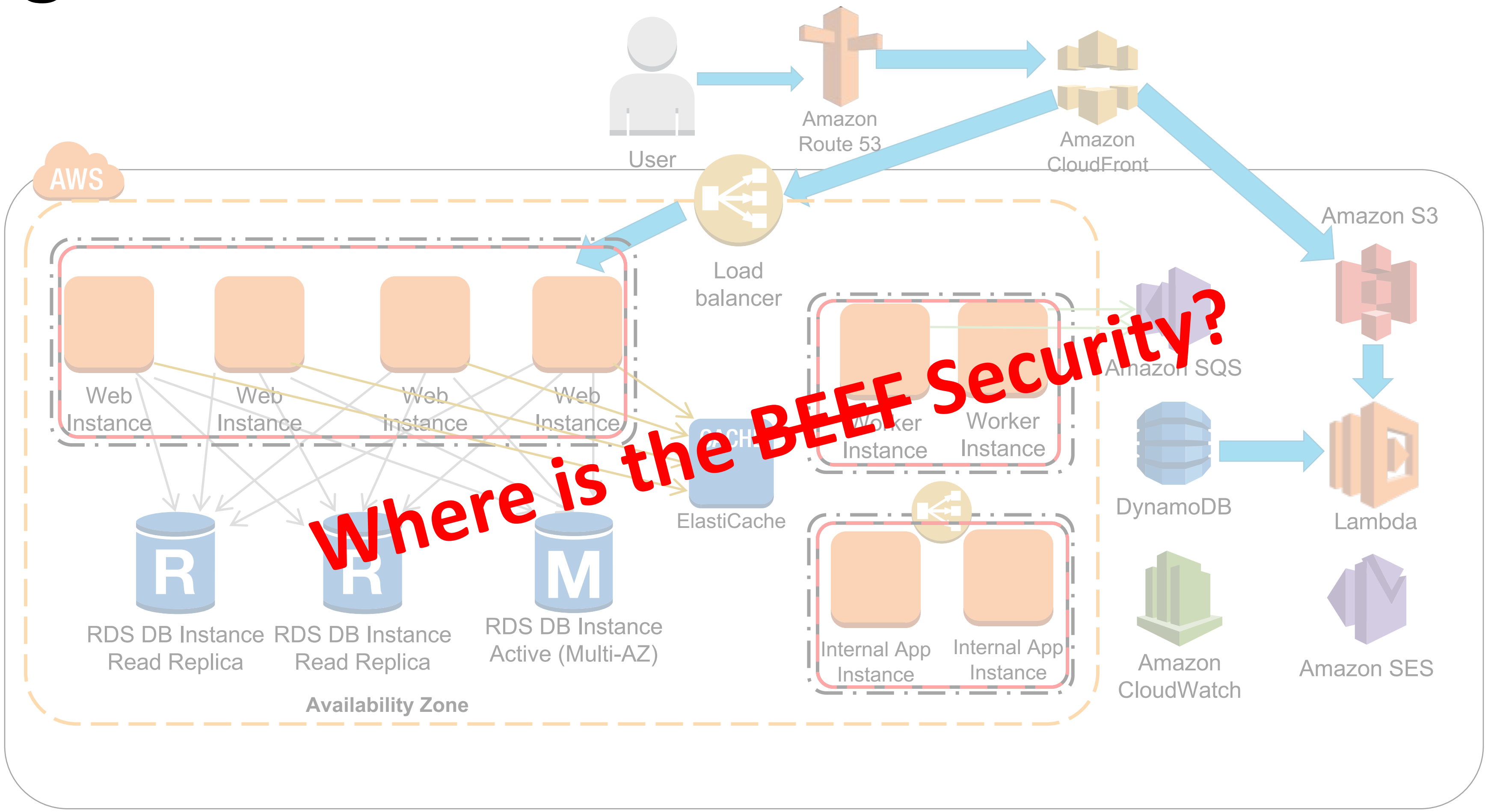
Security in the cloud is familiar.

The increase in agility and the ability to perform actions faster, at a larger scale and at a lower cost, does not invalidate well-established principles of information security.

The AWS CAF Security Perspective

5 Core Capabilities
Identity and Access Management
Detective controls
Infrastructure security
Data protection
Incident response

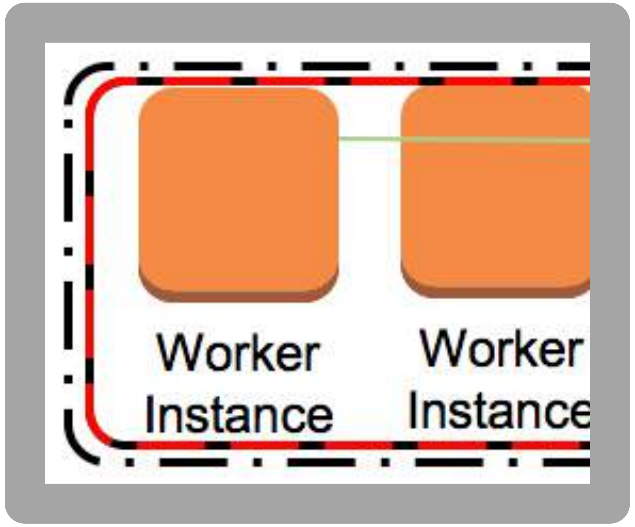
Scaling to >1 Million Users



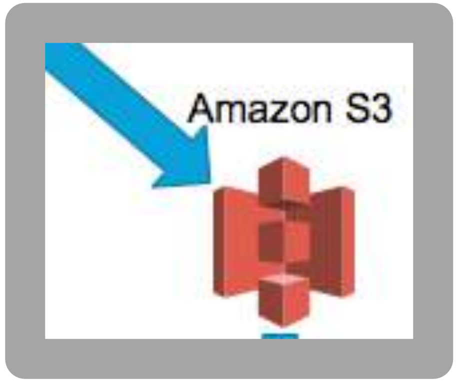
Where is the ~~BEEF~~ Security?

Security Already Built In…

Security groups are virtual firewalls that control the traffic for one or more resources



IAM securely controls access to AWS services and resources for your users.



Identity and Access Management

AWS Organizations

IAM

AWS Security Token Service

Detective Controls

Account

AWS CloudTrail

AWS Config

Resources

Amazon CloudWatch

Amazon Inspector

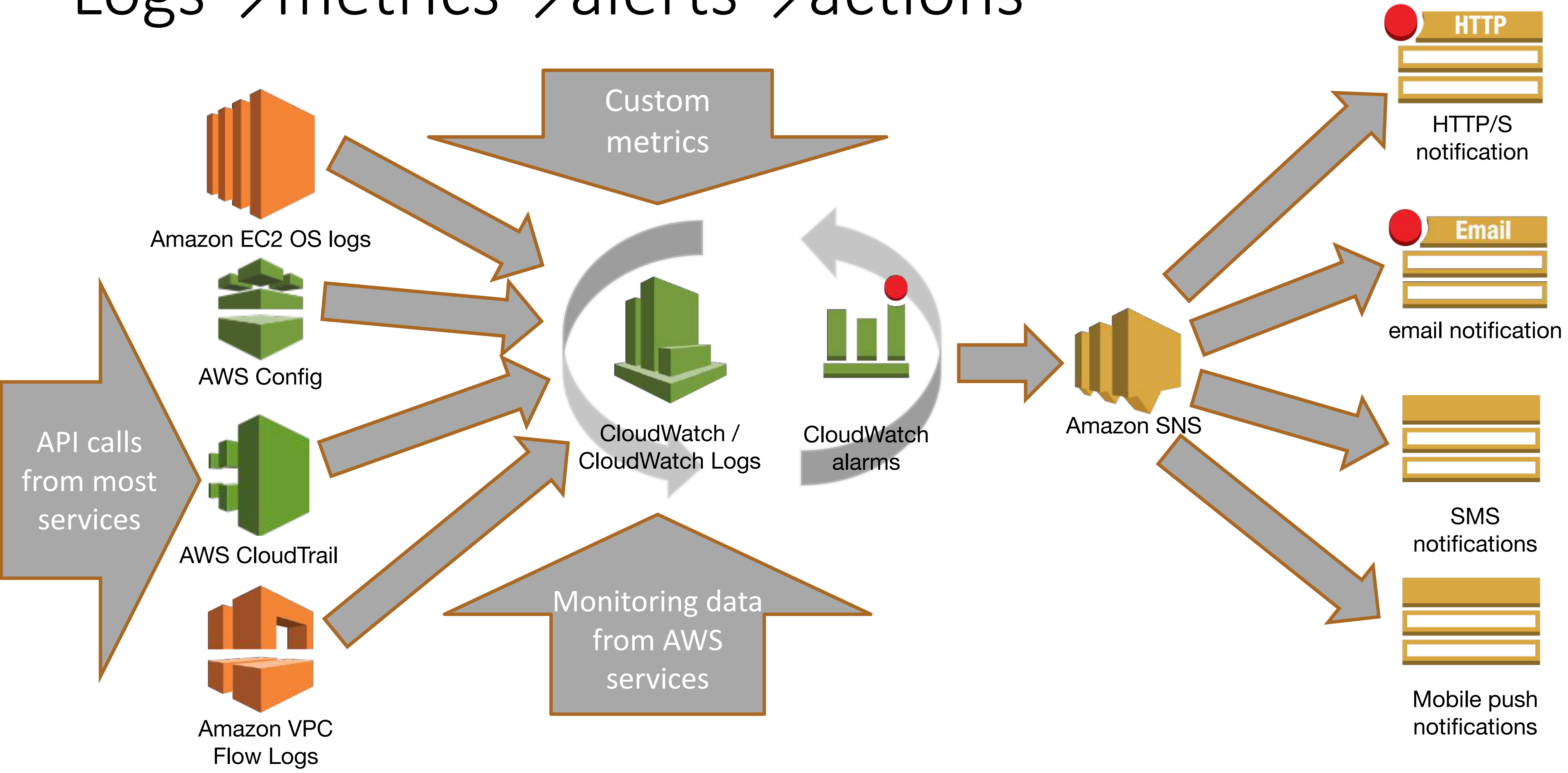
Network

VPC Flow Logs

If it moves…log it!

If it moves…log it!
(If it doesn’t move, watch it ‘til it moves – then log it!)

Logs→metrics→alerts→actions



Different log categories

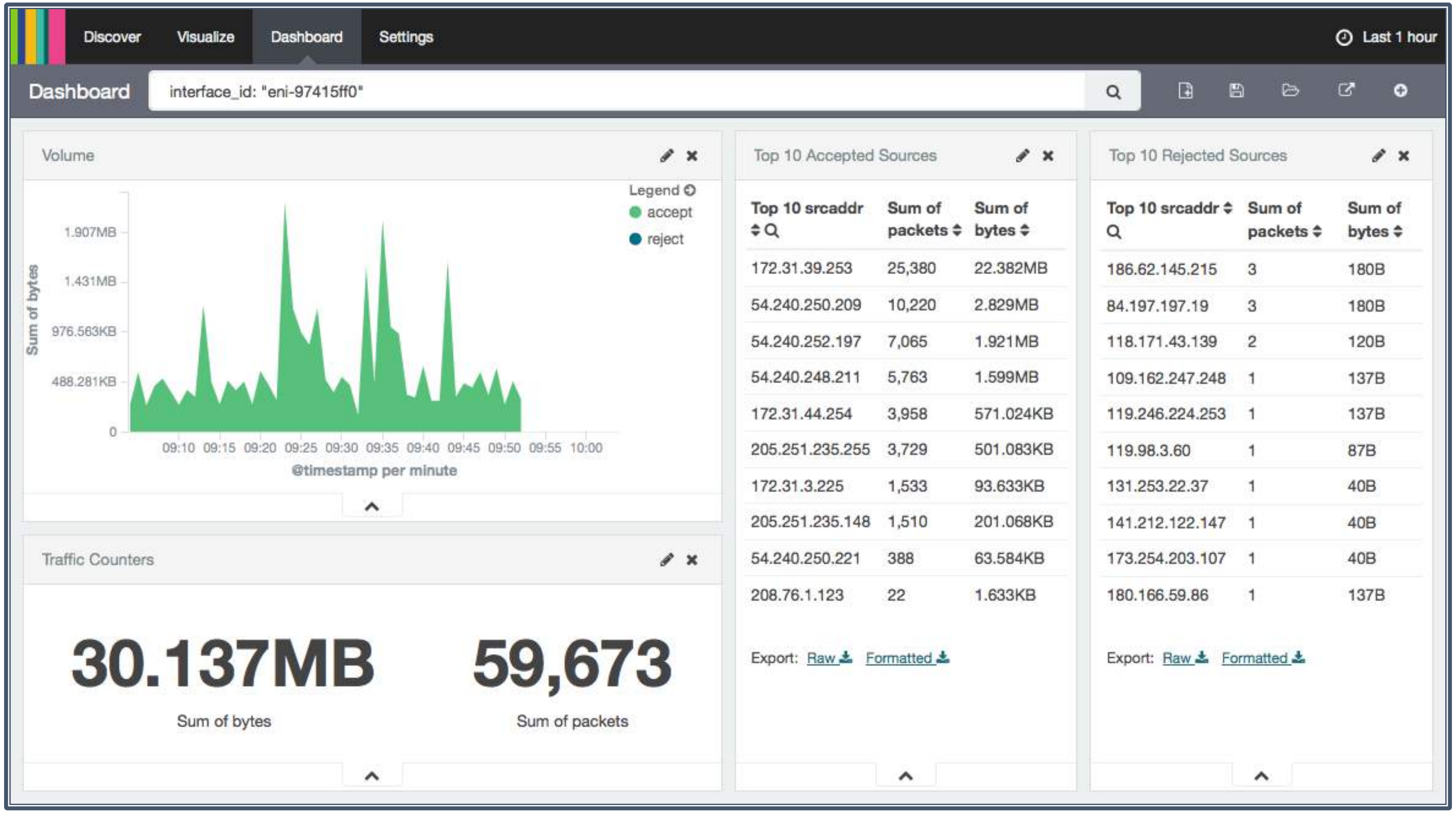
- **AWS infrastructure logs**
  - AWS CloudTrail
  - Amazon VPC Flow Logs

- **AWS service logs**
  - Amazon S3
  - Elastic Load Balancing
  - Amazon CloudFront
  - AWS Lambda (sometimes)
  - AWS Elastic Beanstalk
  - …

- **Host-based logs**
  - Messages
  - Security
  - NGINX/Apache/
  - Syslog etc
  - Performance Monitoring
  - …

Security-related events

Detective Controls - VPC Flow Logs



interface_id: "eni-97415ff0"

30.137MB

Sum of bytes

59,673

Sum of packets

Top 10 Accepted Sources

Top 10 srcaddr	Sum of packets	Sum of bytes
172.31.39.253	25,380	22.382MB
54.240.250.209	10,220	2.829MB
54.240.252.197	7,065	1.921MB
54.240.248.211	5,763	1.599MB
172.31.44.254	3,958	571.024KB
205.251.235.255	3,729	501.083KB
172.31.3.225	1,533	93.633KB
205.251.235.148	1,510	201.068KB
54.240.250.221	388	63.584KB
208.76.1.123	22	1.633KB

Export: Raw Formatted

Top 10 Rejected Sources

Top 10 srcaddr	Sum of packets	Sum of bytes
186.62.145.215	3	180B
84.197.197.19	3	180B
118.171.43.139	2	120B
109.162.247.248	1	137B
119.246.224.253	1	137B
119.98.3.60	1	87B
131.253.22.37	1	40B
141.212.122.147	1	40B
173.254.203.107	1	40B
180.166.59.86	1	137B

Export: Raw Formatted

Flow Log Record Structure

```
2 123456789 eni-31607853 172.16.0.10 172.16.0.172 80 41707 6 1 40 1440402534 1440402589
                                                                                 ACCEPT OK
```

Event-Version

Account Number

ENI-ID

Source-IP

Destination-IP

SourcePort

Destination-Port

Protocol Number

Number of Packets

Number of Bytes

Start-Time Window

End-Time Window

Action

State

Infrastructure Security

Resources

AWS Trusted Advisor

AWS Config Rules

AWS OpsWorks

Network

AWS Shield

AWS WAF

Infrastructure Security – AWS Config Rules

- Amazon CloudTrail is enabled…
  - *Is it?*
- All EBS volumes are encrypted…
  - *Are they?*
- All security groups in attached state should not have unrestricted access to port 22.
  - *Do they?*

Infrastructure Security – AWS Config Rules

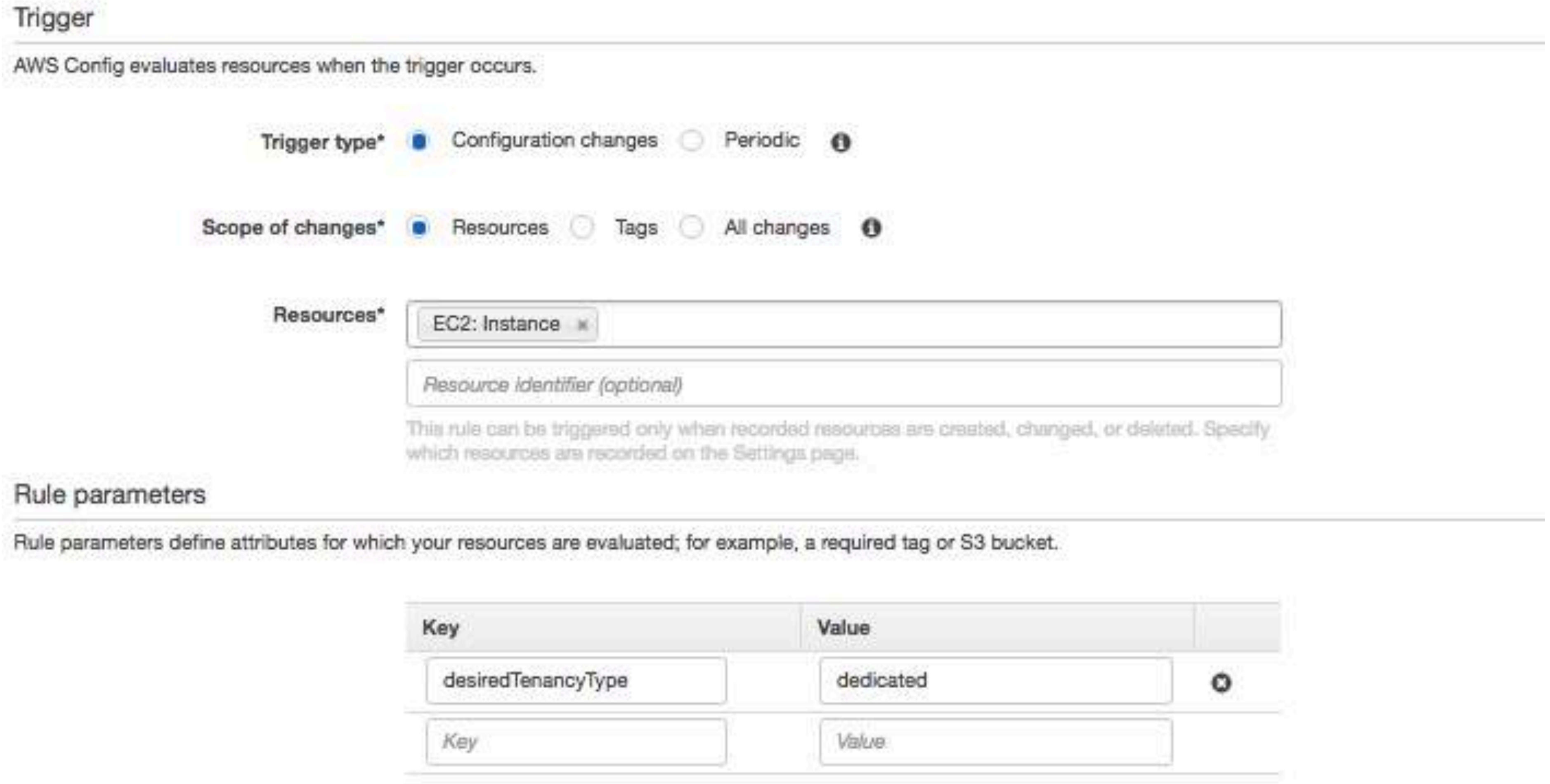
- Codify and Automate your own Practices
- Get started with Samples in AWS Lambda
- Implement guidelines for security best practices and compliance
- Use Rules from various AWS Partners
- View Compliance in one Dashboard

Infrastructure Security – AWS Config Rules

- Set your Policy, formulate your implementation plan:

Undesirable Event	Log Source	Action (Remedial or Alerting)	Function to Perform

Infrastructure Security – AWS Config Rules



Trigger

AWS Config evaluates resources when the trigger occurs.

Trigger type* ● Configuration changes ○ Periodic

Scope of changes* ● Resources ○ Tags ○ All changes

Resources* EC2: Instance

Resource identifier (optional)

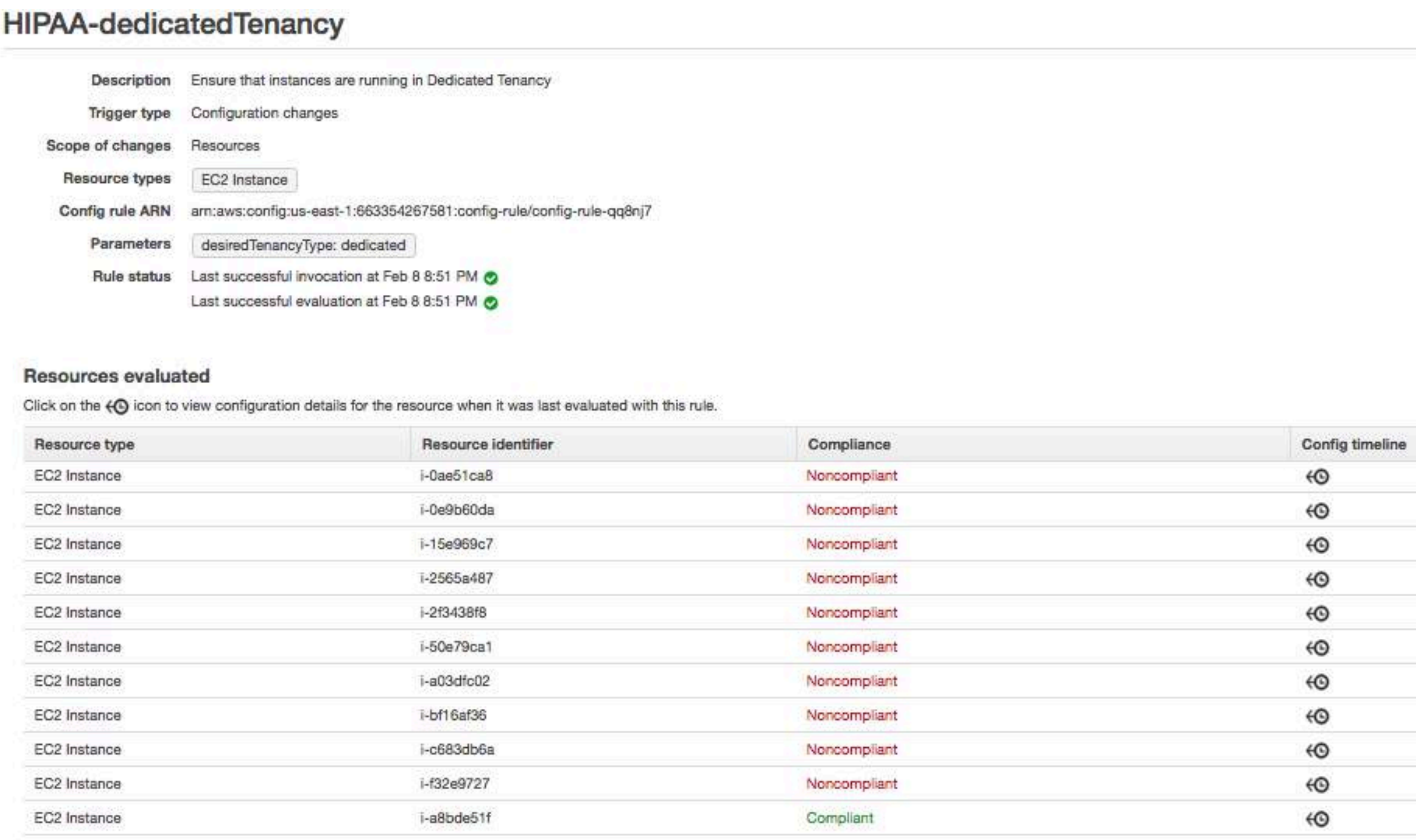
This rule can be triggered only when recorded resources are created, changed, or deleted. Specify which resources are recorded on the Settings page.

Rule parameters

Rule parameters define attributes for which your resources are evaluated; for example, a required tag or S3 bucket.

Key	Value
desiredTenancyType	dedicated
Key	*Value*

Infrastructure Security – AWS Config Rules



HIPAA-dedicatedTenancy

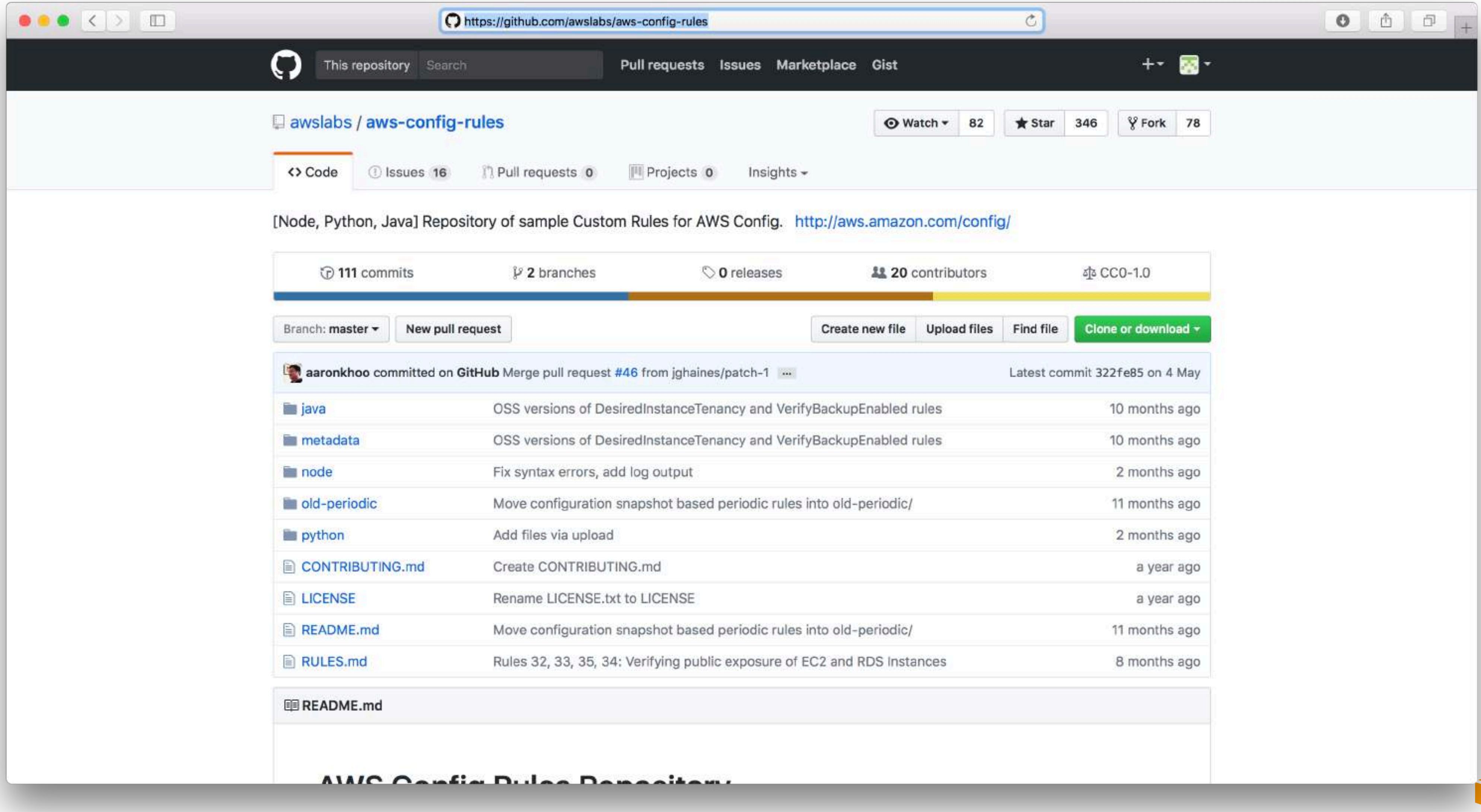
Description	Ensure that instances are running in Dedicated Tenancy
Trigger type	Configuration changes
Scope of changes	Resources
Resource types	EC2 Instance
Config rule ARN	arn:aws:config:us-east-1:663354267581:config-rule/config-rule-qq8nj7
Parameters	desiredTenancyType: dedicated
Rule status	Last successful invocation at Feb 8 8:51 PM ✓ Last successful evaluation at Feb 8 8:51 PM ✓

Resources evaluated

Click on the ⟲ icon to view configuration details for the resource when it was last evaluated with this rule.

Resource type	Resource identifier	Compliance	Config timeline
EC2 Instance	i-0ae51ca8	Noncompliant	⟲
EC2 Instance	i-0e9b60da	Noncompliant	⟲
EC2 Instance	i-15e969c7	Noncompliant	⟲
EC2 Instance	i-2565a487	Noncompliant	⟲
EC2 Instance	i-2f3438f8	Noncompliant	⟲
EC2 Instance	i-50e79ca1	Noncompliant	⟲
EC2 Instance	i-a03dfc02	Noncompliant	⟲
EC2 Instance	i-bf16af36	Noncompliant	⟲
EC2 Instance	i-c683db6a	Noncompliant	⟲
EC2 Instance	i-f32e9727	Noncompliant	⟲
EC2 Instance	i-a8bde51f	Compliant	⟲

Infrastructure Security – AWS Config Rules



awslabs / aws-config-rules

[Node, Python, Java] Repository of sample Custom Rules for AWS Config. http://aws.amazon.com/config/

111 commits · 2 branches · 0 releases · 20 contributors · CC0-1.0

aaronkhoo committed on GitHub Merge pull request #46 from jghaines/patch-1 ... Latest commit 322fe85 on 4 May

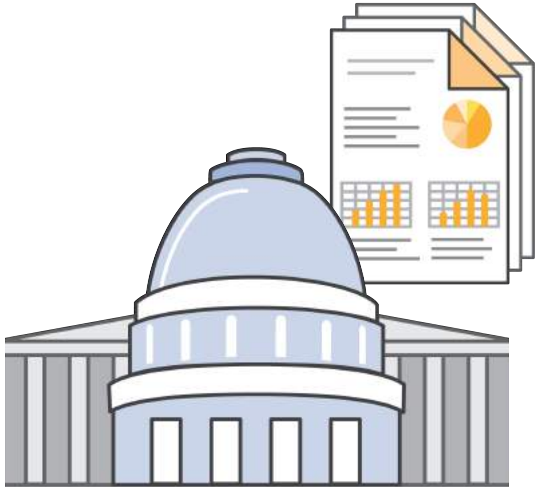
java	OSS versions of DesiredInstanceTenancy and VerifyBackupEnabled rules	10 months ago
metadata	OSS versions of DesiredInstanceTenancy and VerifyBackupEnabled rules	10 months ago
node	Fix syntax errors, add log output	2 months ago
old-periodic	Move configuration snapshot based periodic rules into old-periodic/	11 months ago
python	Add files via upload	2 months ago
CONTRIBUTING.md	Create CONTRIBUTING.md	a year ago
LICENSE	Rename LICENSE.txt to LICENSE	a year ago
README.md	Move configuration snapshot based periodic rules into old-periodic/	11 months ago
RULES.md	Rules 32, 33, 35, 34: Verifying public exposure of EC2 and RDS Instances	8 months ago

README.md

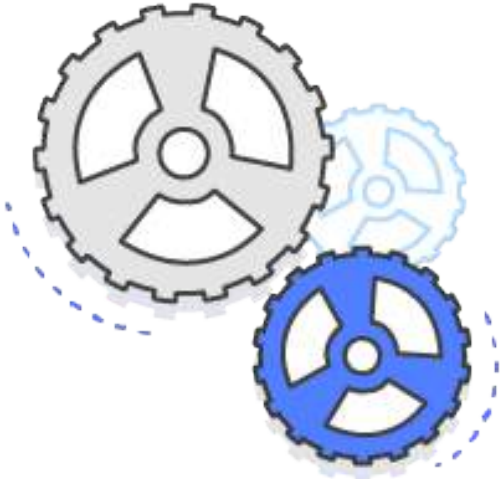
AWS Config Rules Repository

Introducing AWS Organizations

Policy-based management for multiple AWS accounts.



Control AWS service use across accounts



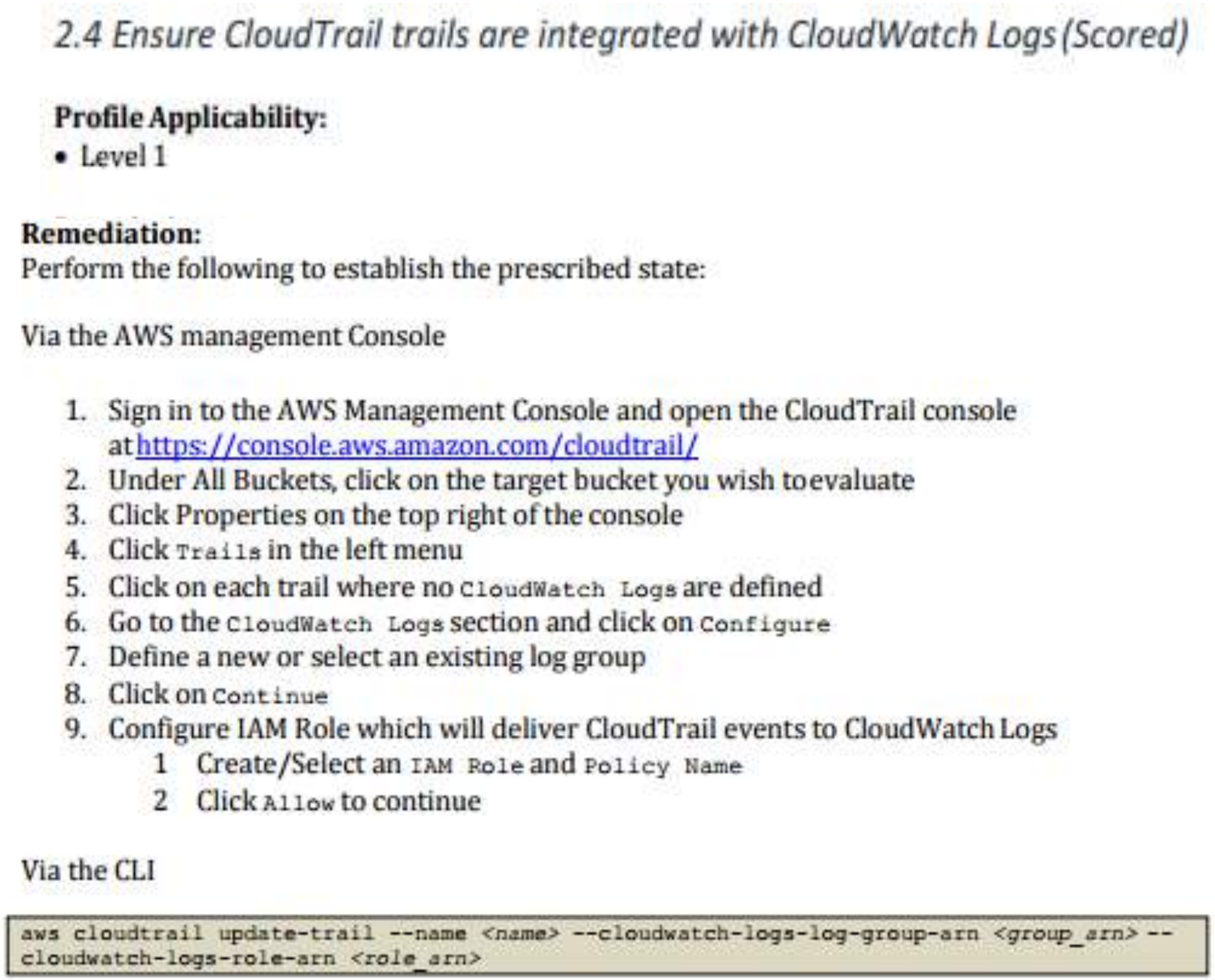
Automate AWS account creation

Consolidate billing

Industry Best Practices for
Securing AWS Resources

Center for Internet Security®

- Architecture agnostic set of security configuration best practices
- provides set-by-step implementation and assessment procedures



2.4 Ensure CloudTrail trails are integrated with CloudWatch Logs (Scored)

Profile Applicability:

- Level 1

Remediation:
Perform the following to establish the prescribed state:

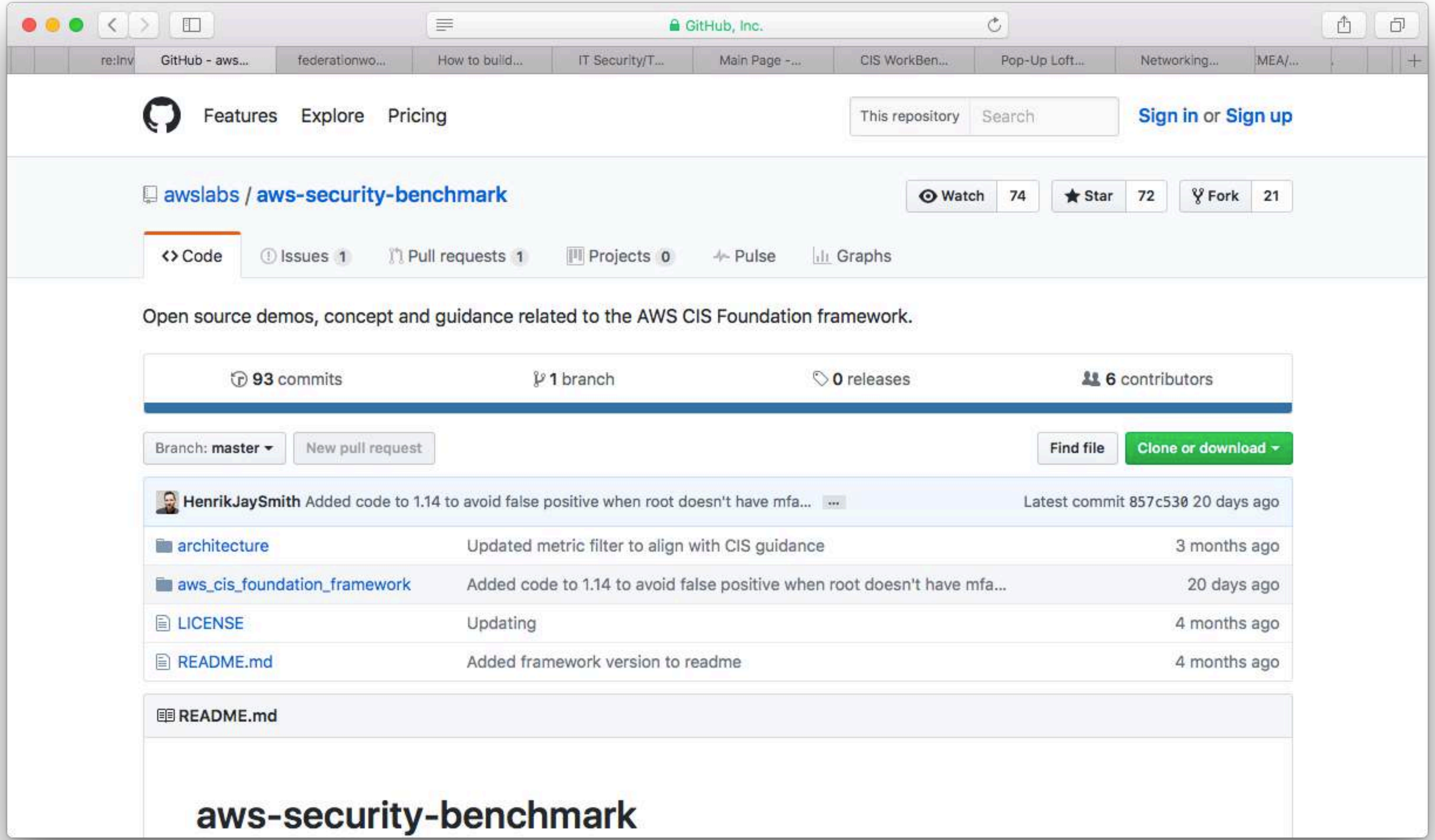
Via the AWS management Console

1. Sign in to the AWS Management Console and open the CloudTrail console at https://console.aws.amazon.com/cloudtrail/
2. Under All Buckets, click on the target bucket you wish to evaluate
3. Click Properties on the top right of the console
4. Click `Trails` in the left menu
5. Click on each trail where no `CloudWatch Logs` are defined
6. Go to the `CloudWatch Logs` section and click on `Configure`
7. Define a new or select an existing log group
8. Click on `Continue`
9. Configure IAM Role which will deliver CloudTrail events to CloudWatch Logs
   1 Create/Select an `IAM Role` and `Policy Name`
   2 Click `Allow` to continue

Via the CLI

```
aws cloudtrail update-trail --name <name> --cloudwatch-logs-log-group-arn <group_arn> --
cloudwatch-logs-role-arn <role_arn>
```

Automating New Account Security Baselining…



awslabs / aws-security-benchmark

Open source demos, concept and guidance related to the AWS CIS Foundation framework.

93 commits | 1 branch | 0 releases | 6 contributors

HenrikJaySmith Added code to 1.14 to avoid false positive when root doesn't have mfa… … Latest commit 857c530 20 days ago

architecture	Updated metric filter to align with CIS guidance	3 months ago
aws_cis_foundation_framework	Added code to 1.14 to avoid false positive when root doesn't have mfa…	20 days ago
LICENSE	Updating	4 months ago
README.md	Added framework version to readme	4 months ago

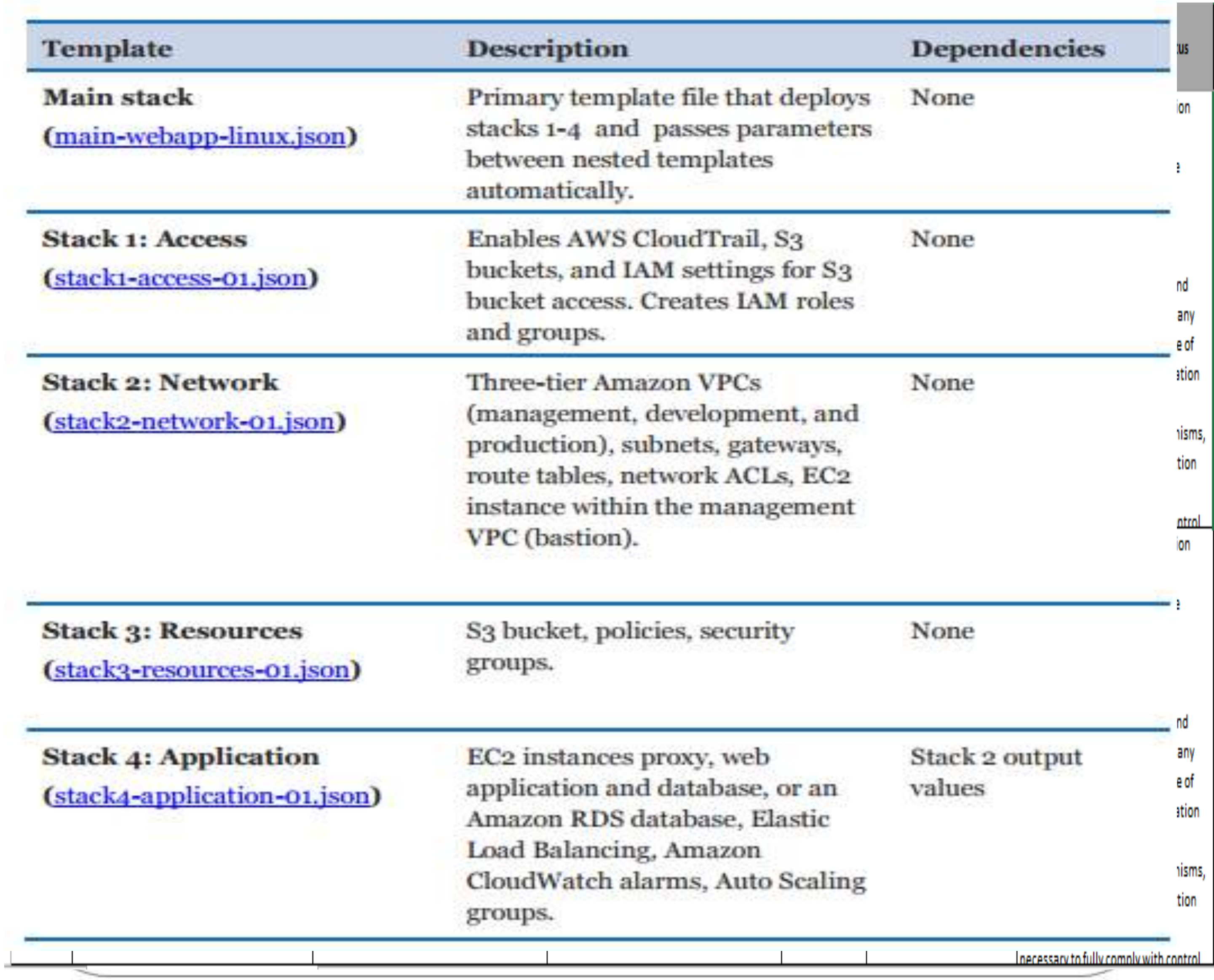
README.md

aws-security-benchmark

AWS Enterprise Accelerator:

Compliance Architectures

- Sample Architecture –
- Security Controls Matrix
- Cloudformation Templates
  - 5 x templates
- User Guide



Template	Description	Dependencies
Main stack (main-webapp-linux.json)	Primary template file that deploys stacks 1-4 and passes parameters between nested templates automatically.	None
Stack 1: Access (stack1-access-01.json)	Enables AWS CloudTrail, S3 buckets, and IAM settings for S3 bucket access. Creates IAM roles and groups.	None
Stack 2: Network (stack2-network-01.json)	Three-tier Amazon VPCs (management, development, and production), subnets, gateways, route tables, network ACLs, EC2 instance within the management VPC (bastion).	None
Stack 3: Resources (stack3-resources-01.json)	S3 bucket, policies, security groups.	None
Stack 4: Application (stack4-application-01.json)	EC2 instances proxy, web application and database, or an Amazon RDS database, Elastic Load Balancing, Amazon CloudWatch alarms, Auto Scaling groups.	Stack 2 output values

Infrastructure Security – Organizations SCPs

- Enables you to control which AWS service APIs are accessible
  - Define the list of APIs that are allowed – *whitelisting*
  - Define the list of APIs that must be blocked – *blacklisting*
- Cannot be overridden by local administrator
- Resultant permission on IAM user/role is the intersection between the SCP and assigned IAM permissions
- Necessary but not sufficient
- IAM policy simulator is SCP aware

Blacklisting example

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": "redshift:*",
      "Resource": "*"
    }
  ]
}
```

Whitelisting example

```
{
 "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
             "ec2:RunInstances",
             "ec2:DescribeInstances",
             "ec2:DescribeImages",
             "ec2:DescribeKeyPairs",
             "ec2:DescribeVpcs",
             "ec2:DescribeSubnets",

      "ec2:DescribeSecurityGroups"
      ],
      "Resource": "*"
    }]}
```

More on SCPs

But:

- you don't have to apply an SCP before you populate your account with assets...
- this lends the idea of "immutable infrastructure" to other services, from the point of view of the child accounts
- (including Serverless)
- eg:
  - S3 websites which can't have their contents changed
  - Lambda functions which are invoke-only "black boxes"
  - ACM cert / key pairs which can't be deleted
  - Prevent CloudTrail, Config ever being turned off
  - ...

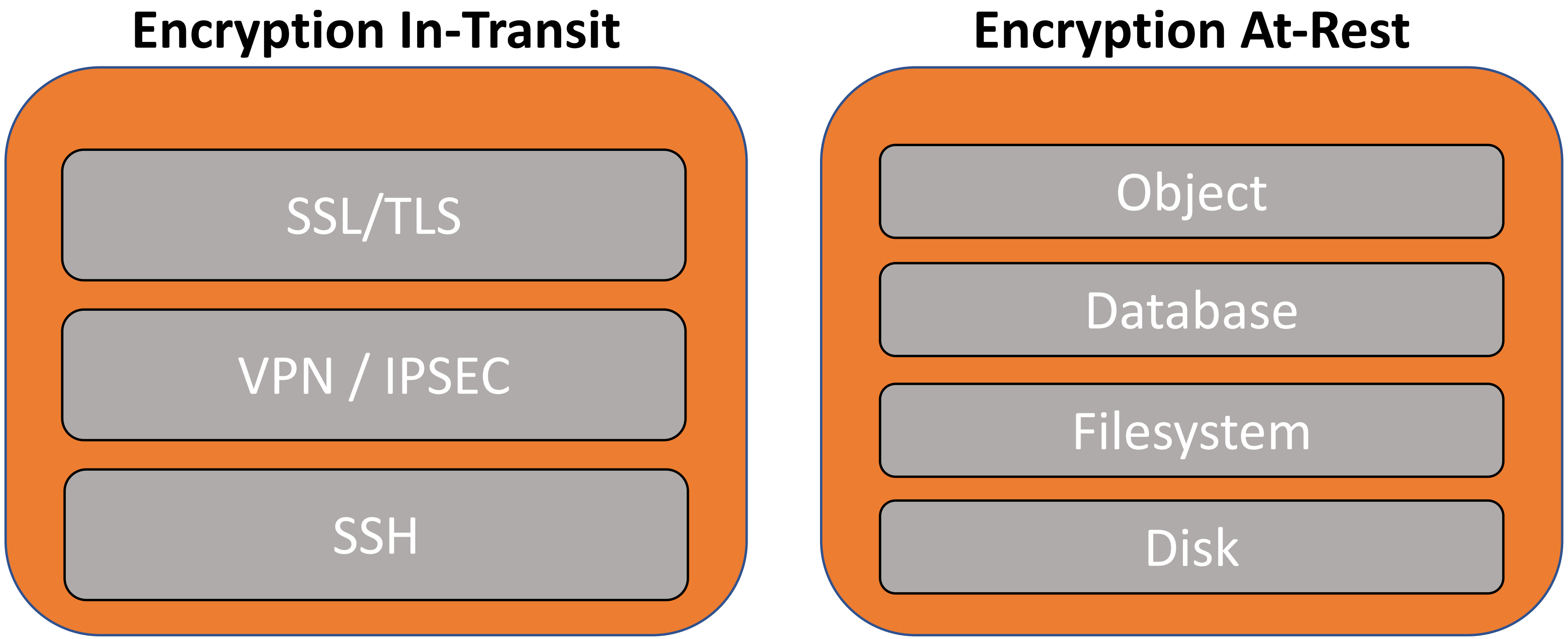
Data Protection

AWS CloudHSM

AWS Key Management Service

AWS Certificate Manager

Data Protection - Encryption



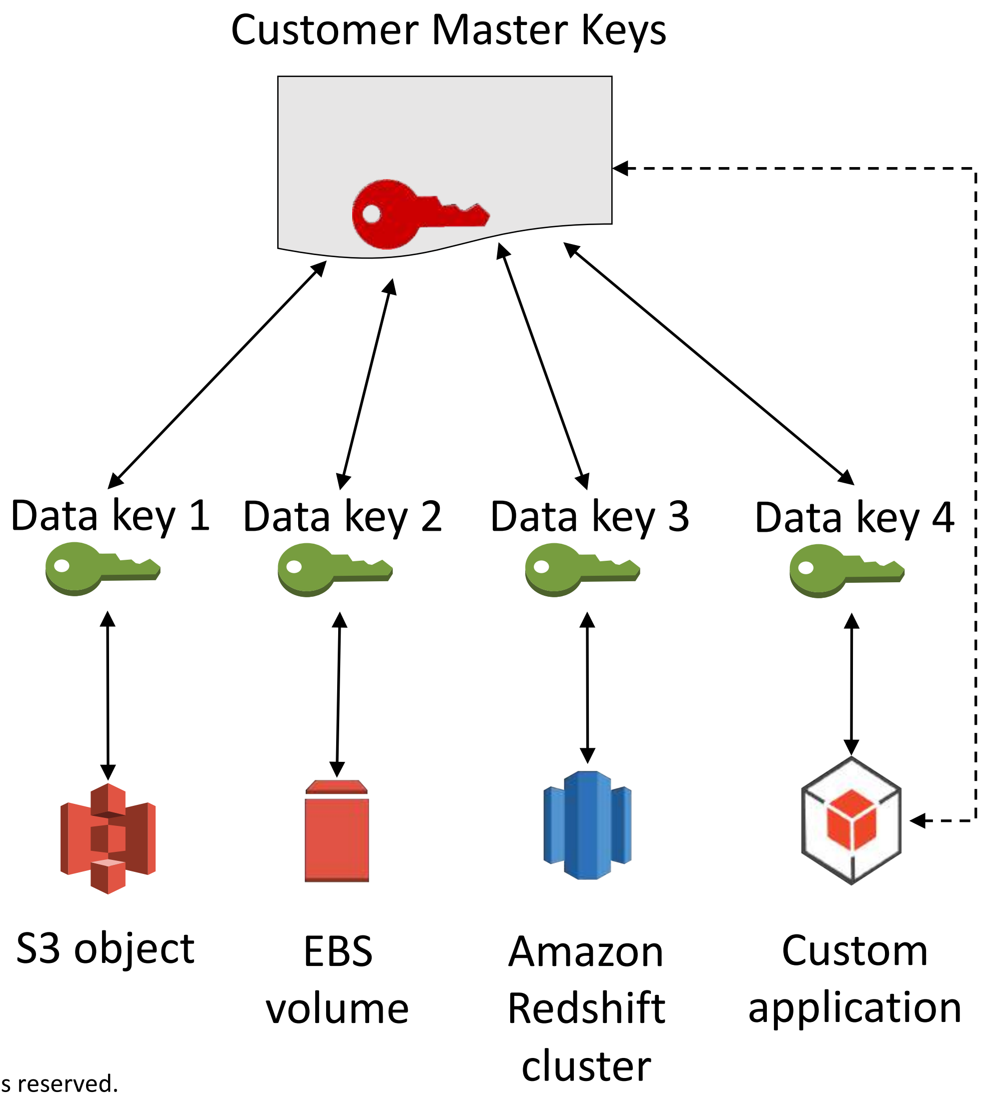
Encryption In-Transit

- SSL/TLS
- VPN / IPSEC
- SSH

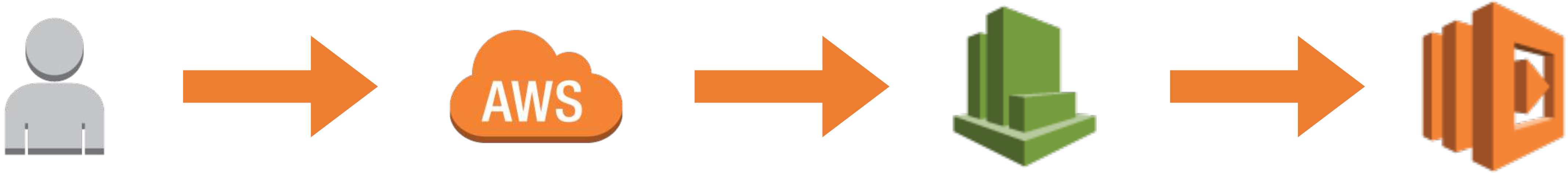
Encryption At-Rest

- Object
- Database
- Filesystem
- Disk

Data Protection – AWS KMS



Responding to Issues: the Automation Playbook…



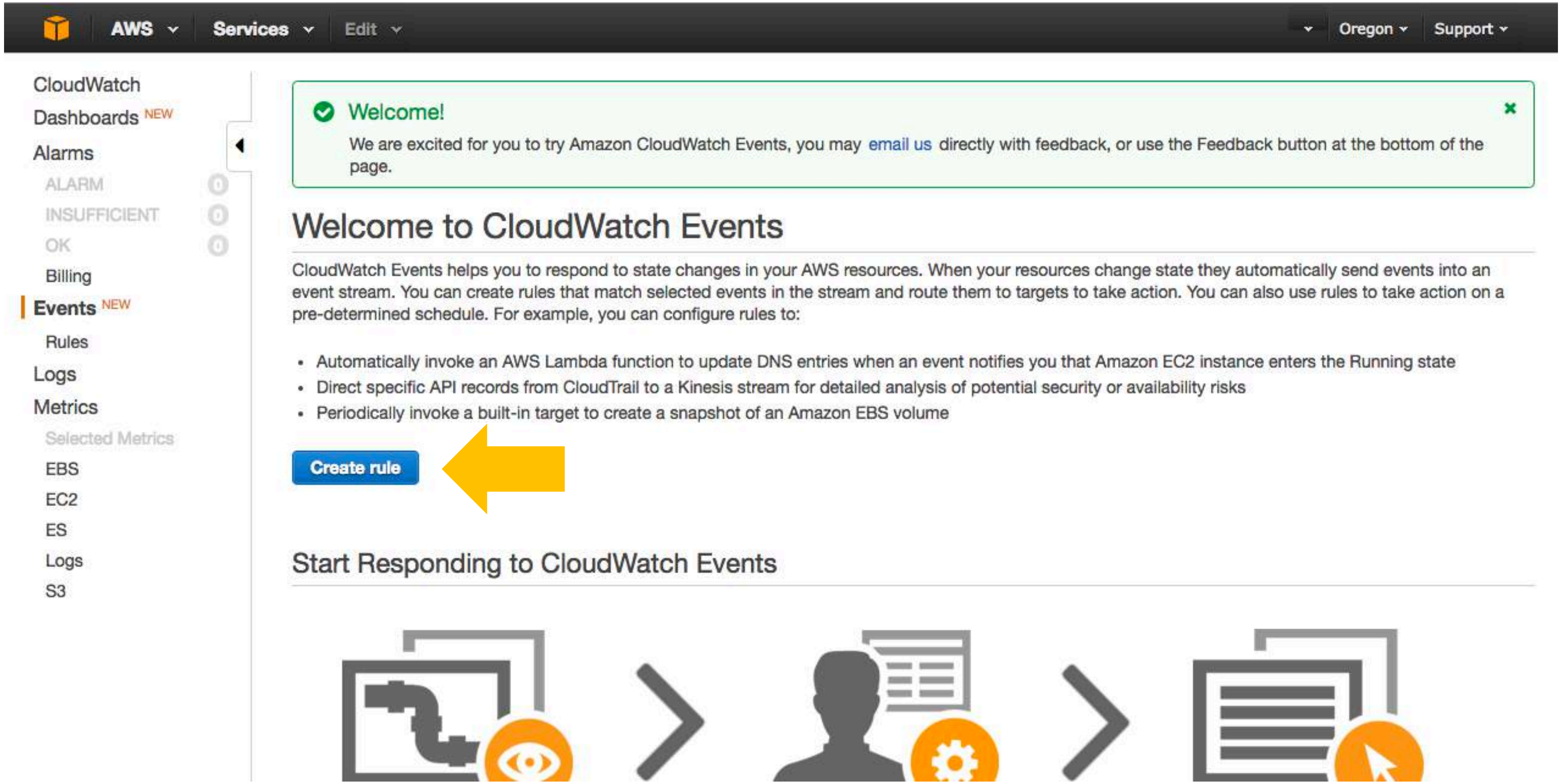
Adversary
(or Intern)

Your environment

CloudWatch
Events event

Responder

Incident Response – AWS CloudWatch Events



Welcome!

We are excited for you to try Amazon CloudWatch Events, you may email us directly with feedback, or use the Feedback button at the bottom of the page.

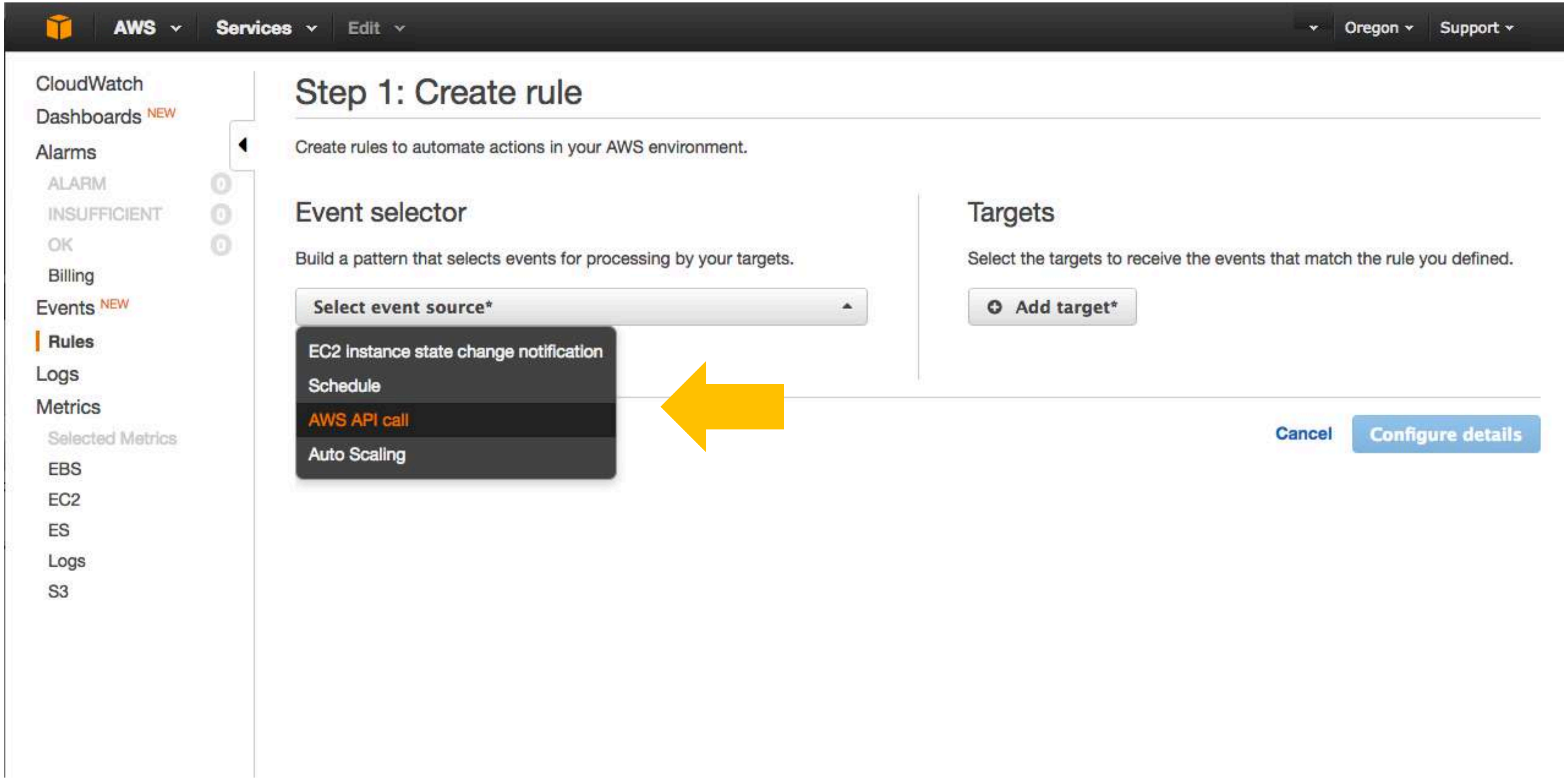
Welcome to CloudWatch Events

CloudWatch Events helps you to respond to state changes in your AWS resources. When your resources change state they automatically send events into an event stream. You can create rules that match selected events in the stream and route them to targets to take action. You can also use rules to take action on a pre-determined schedule. For example, you can configure rules to:

- Automatically invoke an AWS Lambda function to update DNS entries when an event notifies you that Amazon EC2 instance enters the Running state
- Direct specific API records from CloudTrail to a Kinesis stream for detailed analysis of potential security or availability risks
- Periodically invoke a built-in target to create a snapshot of an Amazon EBS volume

Start Responding to CloudWatch Events

Incident Response – AWS CloudWatch Events



Step 1: Create rule

Create rules to automate actions in your AWS environment.

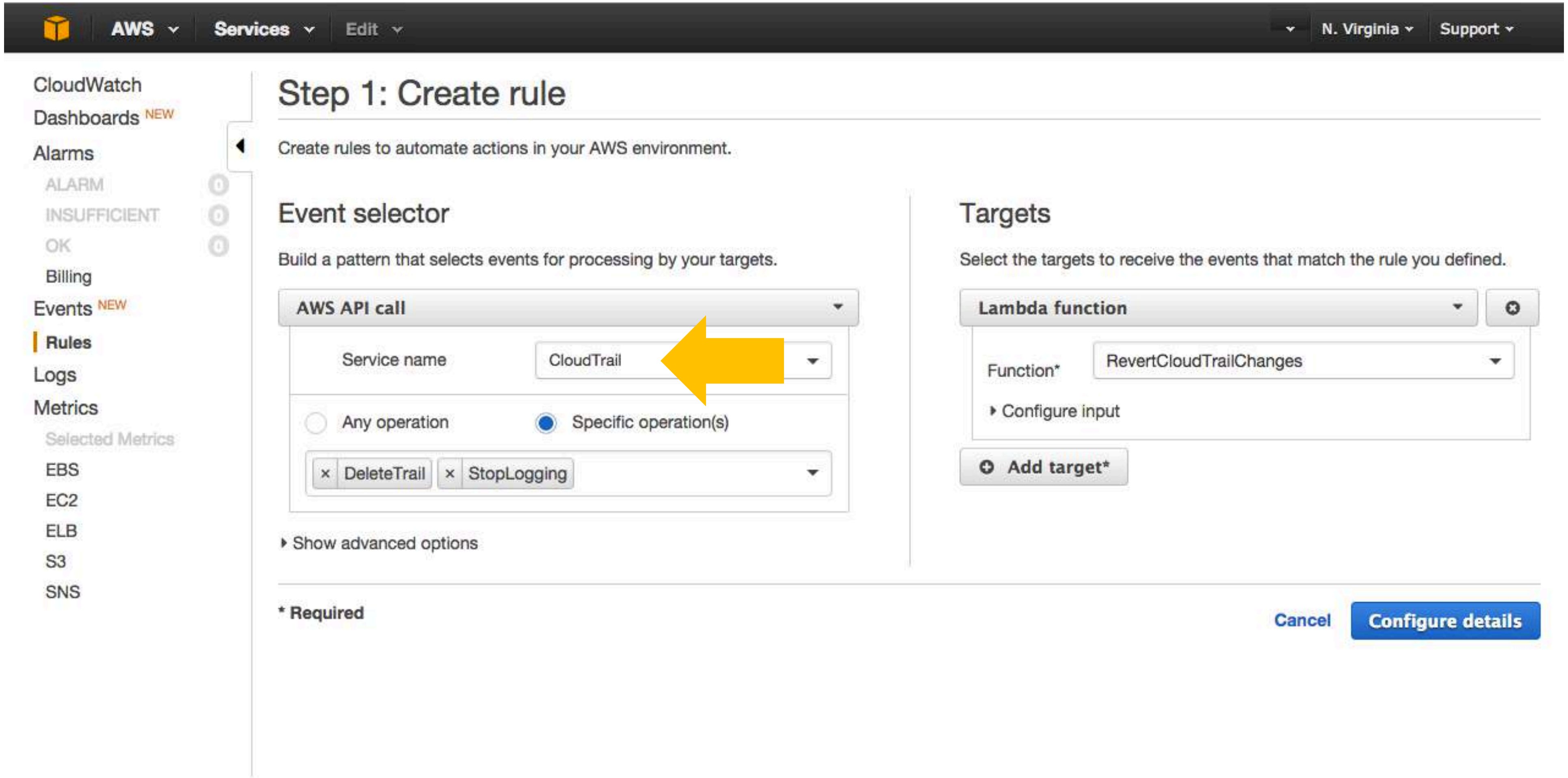
Event selector

Build a pattern that selects events for processing by your targets.

Targets

Select the targets to receive the events that match the rule you defined.

Incident Response – AWS CloudWatch Events



Step 1: Create rule

Create rules to automate actions in your AWS environment.

Event selector

Build a pattern that selects events for processing by your targets.

AWS API call

Service name: CloudTrail

○ Any operation ● Specific operation(s)

× DeleteTrail × StopLogging

Show advanced options

Targets

Select the targets to receive the events that match the rule you defined.

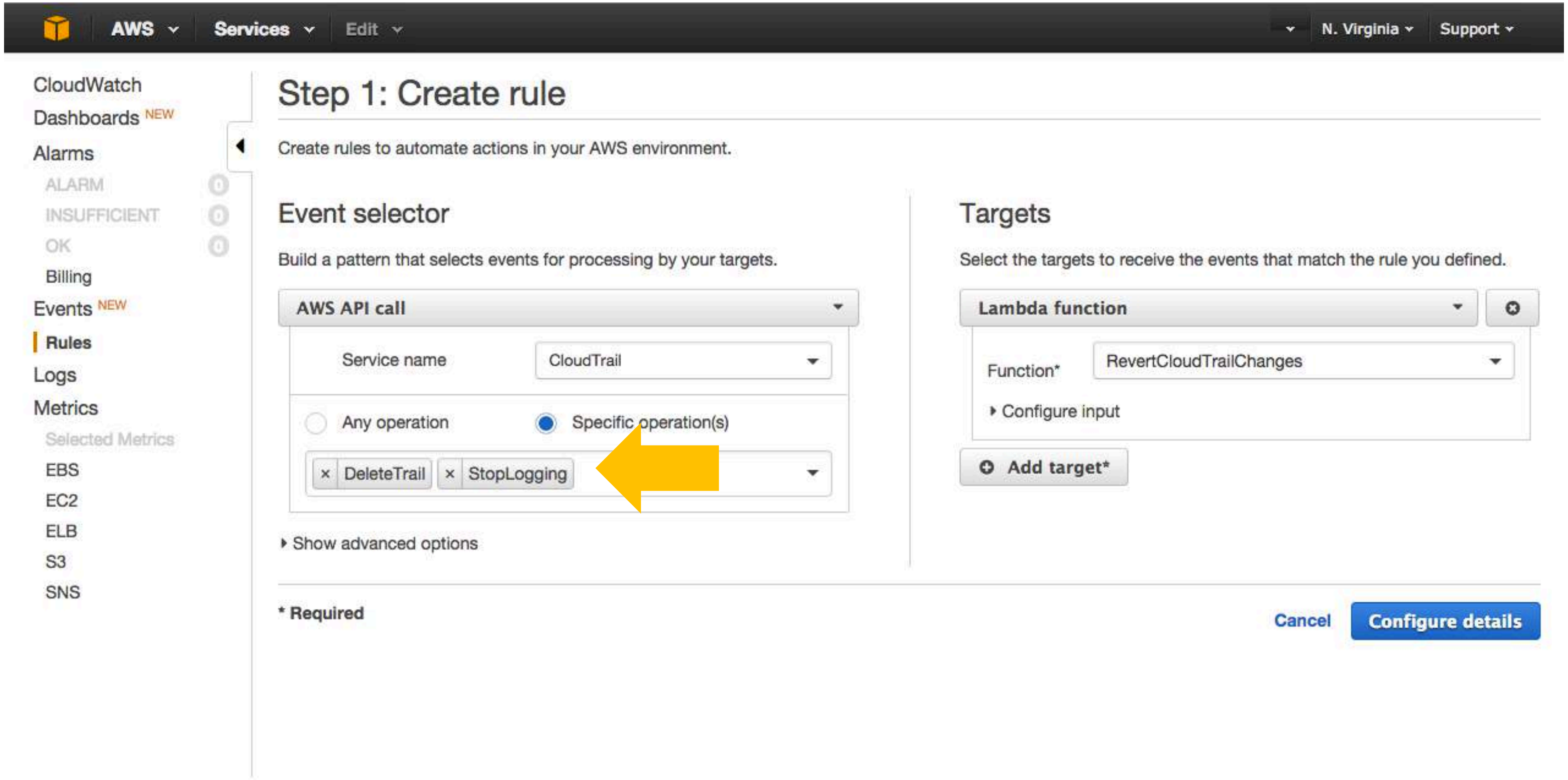
Lambda function

Function*: RevertCloudTrailChanges

Configure input

* Required

Incident Response – AWS CloudWatch Events



Step 1: Create rule

Create rules to automate actions in your AWS environment.

Event selector

Build a pattern that selects events for processing by your targets.

AWS API call

Service name: CloudTrail

○ Any operation ● Specific operation(s)

× DeleteTrail × StopLogging

▸ Show advanced options

Targets

Select the targets to receive the events that match the rule you defined.

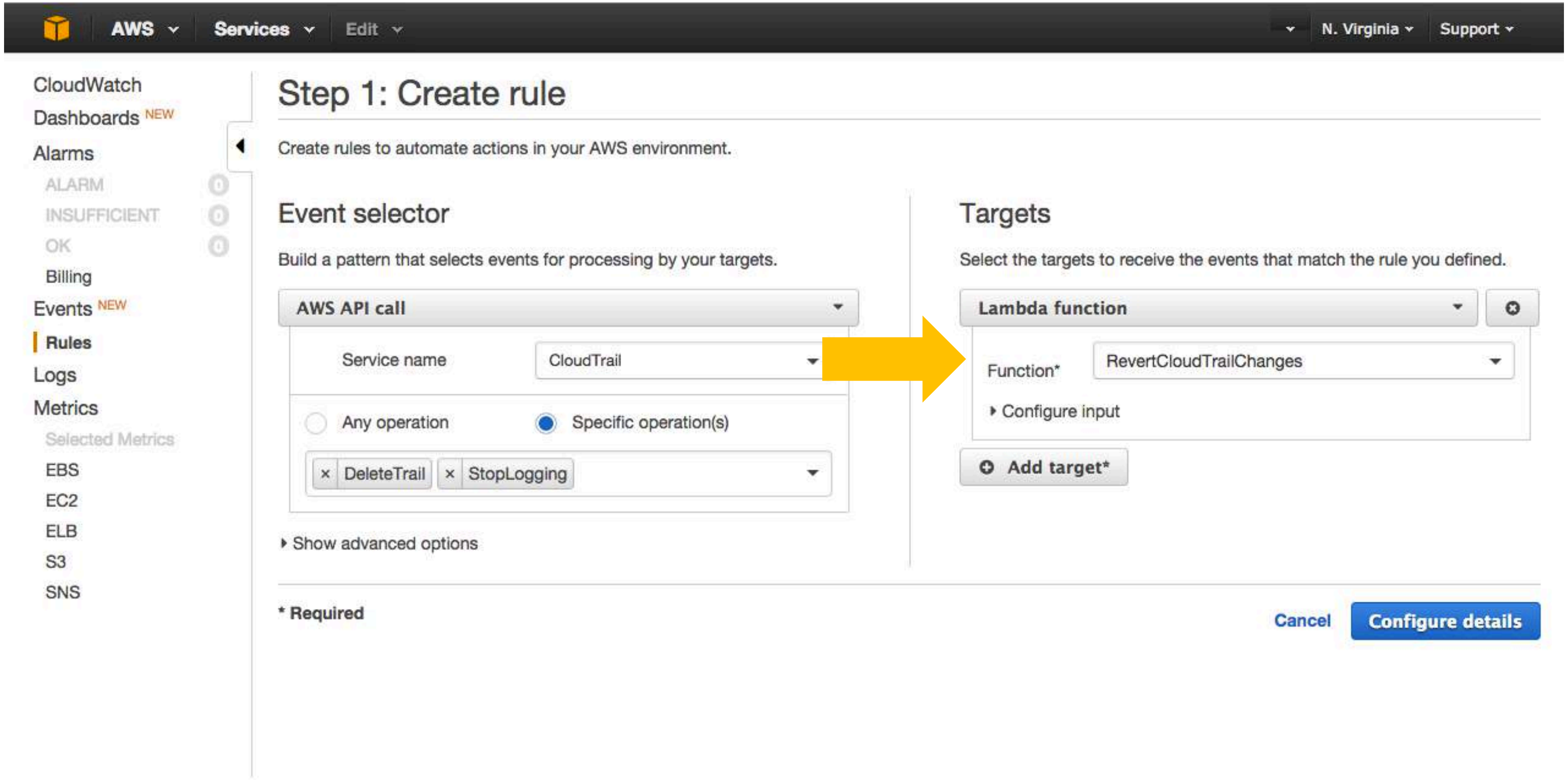
Lambda function

Function*: RevertCloudTrailChanges

▸ Configure input

* Required

Incident Response – AWS CloudWatch Events



Step 1: Create rule

Create rules to automate actions in your AWS environment.

Event selector

Build a pattern that selects events for processing by your targets.

AWS API call

Service name: CloudTrail

○ Any operation ● Specific operation(s)

× DeleteTrail × StopLogging

‣ Show advanced options

Targets

Select the targets to receive the events that match the rule you defined.

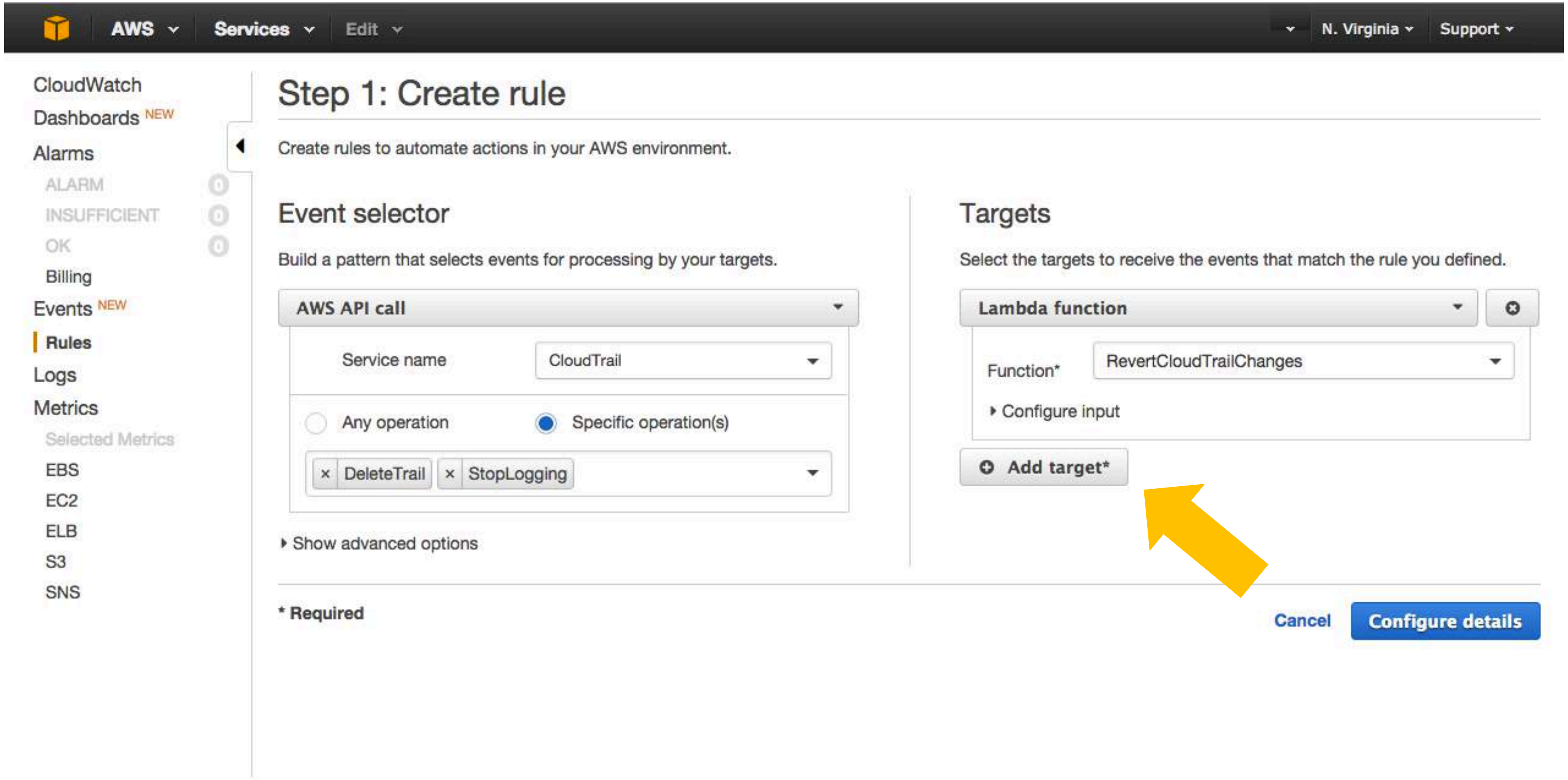
Lambda function

Function*: RevertCloudTrailChanges

‣ Configure input

* Required

Incident Response – AWS CloudWatch Events



Step 1: Create rule

Create rules to automate actions in your AWS environment.

Event selector

Build a pattern that selects events for processing by your targets.

AWS API call

Service name: CloudTrail

○ Any operation ● Specific operation(s)

× DeleteTrail × StopLogging

▸ Show advanced options

Targets

Select the targets to receive the events that match the rule you defined.

Lambda function

Function*: RevertCloudTrailChanges

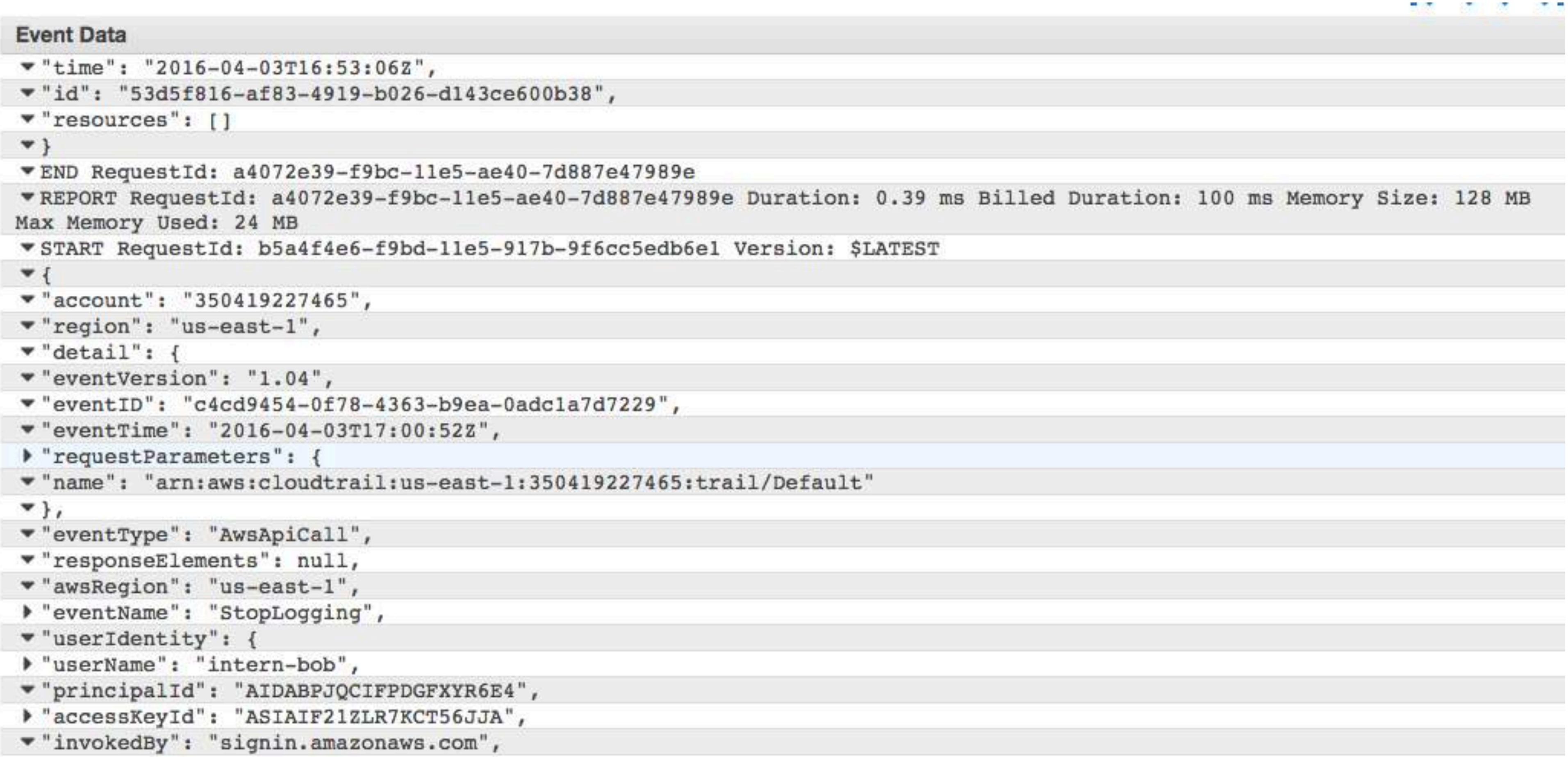
▸ Configure input

* Required

Incident Response – Lambda Log

```
from __future__ import print_function
import json

def lambda_handler(event, context):
    print(json.dumps(event, indent=2))
```

Incident Response – AWS CloudWatch Events



Event Data

```
"time": "2016-04-03T16:53:06Z",
"id": "53d5f816-af83-4919-b026-d143ce600b38",
"resources": []
}
END RequestId: a4072e39-f9bc-11e5-ae40-7d887e47989e
REPORT RequestId: a4072e39-f9bc-11e5-ae40-7d887e47989e Duration: 0.39 ms Billed Duration: 100 ms Memory Size: 128 MB
Max Memory Used: 24 MB
START RequestId: b5a4f4e6-f9bd-11e5-917b-9f6cc5edb6e1 Version: $LATEST
{
"account": "350419227465",
"region": "us-east-1",
"detail": {
"eventVersion": "1.04",
"eventID": "c4cd9454-0f78-4363-b9ea-0adc1a7d7229",
"eventTime": "2016-04-03T17:00:52Z",
"requestParameters": {
"name": "arn:aws:cloudtrail:us-east-1:350419227465:trail/Default"
},
"eventType": "AwsApiCall",
"responseElements": null,
"awsRegion": "us-east-1",
"eventName": "StopLogging",
"userIdentity": {
"userName": "intern-bob",
"principalId": "AIDABPJQCIFPDGFXYR6E4",
"accessKeyId": "ASIAIF21ZLR7KCT56JJA",
"invokedBy": "signin.amazonaws.com",
```

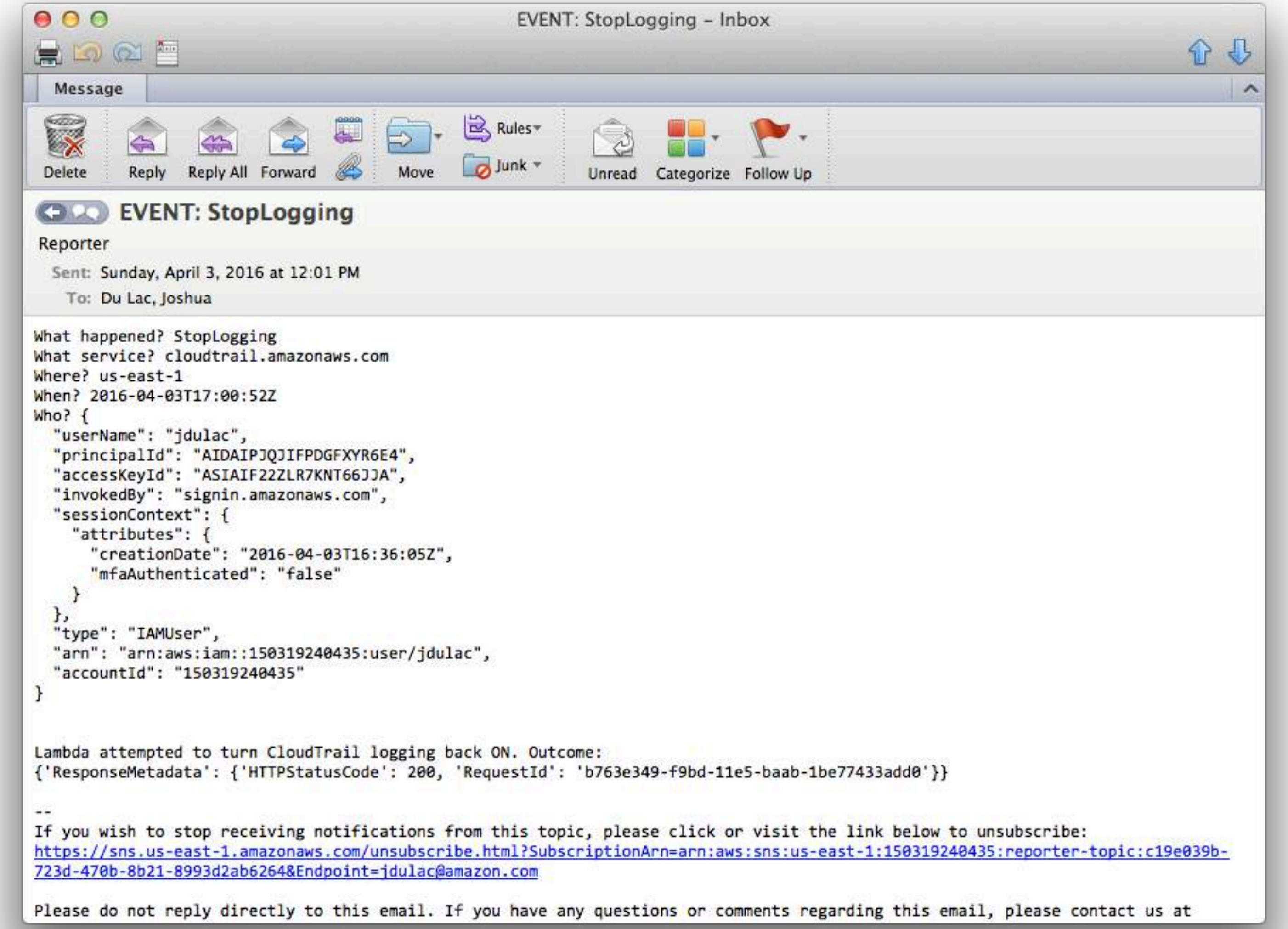
Incident Response – Lambda Respond

```
cloudtrail = boto3.client('cloudtrail')
trail_arn =
event["detail"]["requestParameters"]["name
"]

ct_response = cloudtrail.start_logging(
    Name = trail_arn
)
```

Incident Response – Lambda Notify

```
sns_topic = "arn:aws:sns:us-east-1:123459227412:reporter-topic"

subject = 'EVENT: ' + event["detail"]["eventName"]
message = "What happened? " + event["detail"]["eventName"] + "\n" \
"What service? " + event["detail"]["eventSource"] + "\n" \
"Where? " + event["detail"]["awsRegion"] + "\n" \
"When? " + event["detail"]["eventTime"] + "\n" \
"Who? " + str(json.dumps(event["detail"]["userIdentity"], indent=2))

sns = boto3.client('sns')
sns_response = sns.publish(
    TopicArn = sns_topic,
    Message = message,
    Subject = subject,
    MessageStructure = 'string'
)
```

Incident Response – Amazon SNS Notification



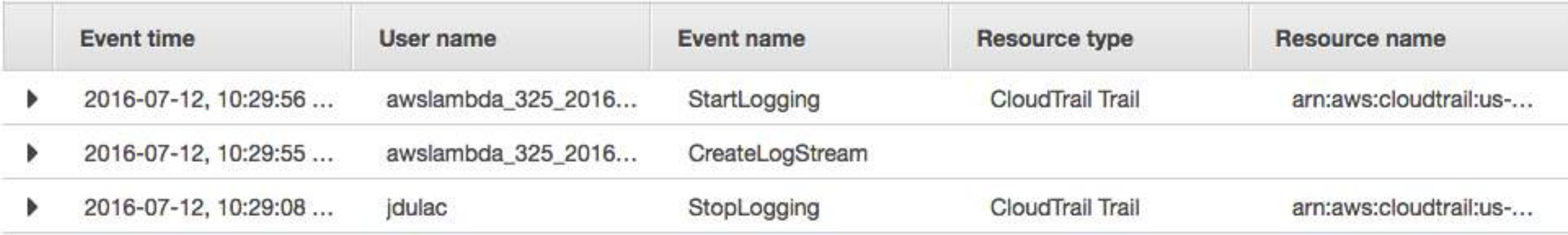
EVENT: StopLogging

Reporter

Sent: Sunday, April 3, 2016 at 12:01 PM
To: Du Lac, Joshua

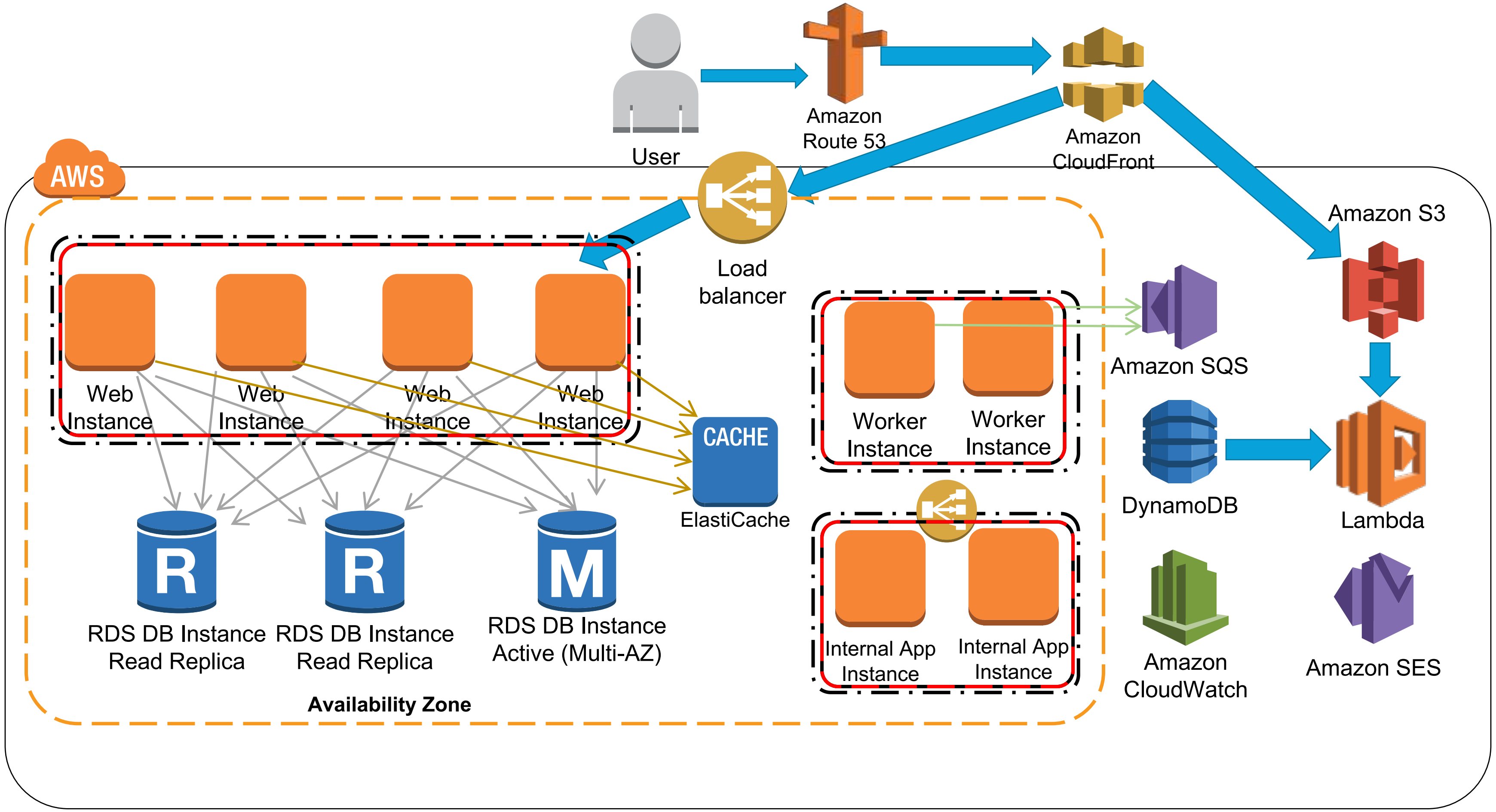
```
What happened? StopLogging
What service? cloudtrail.amazonaws.com
Where? us-east-1
When? 2016-04-03T17:00:52Z
Who? {
  "userName": "jdulac",
  "principalId": "AIDAIPJQJIFPDGFXYR6E4",
  "accessKeyId": "ASIAIF22ZLR7KNT66JJA",
  "invokedBy": "signin.amazonaws.com",
  "sessionContext": {
    "attributes": {
      "creationDate": "2016-04-03T16:36:05Z",
      "mfaAuthenticated": "false"
    }
  },
  "type": "IAMUser",
  "arn": "arn:aws:iam::150319240435:user/jdulac",
  "accountId": "150319240435"
}


Lambda attempted to turn CloudTrail logging back ON. Outcome:
{'ResponseMetadata': {'HTTPStatusCode': 200, 'RequestId': 'b763e349-f9bd-11e5-baab-1be77433add0'}}

--
If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:
https://sns.us-east-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-east-1:150319240435:reporter-topic:c19e039b-
723d-470b-8b21-8993d2ab6264&Endpoint=jdulac@amazon.com

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at
```

Incident Response – Complete

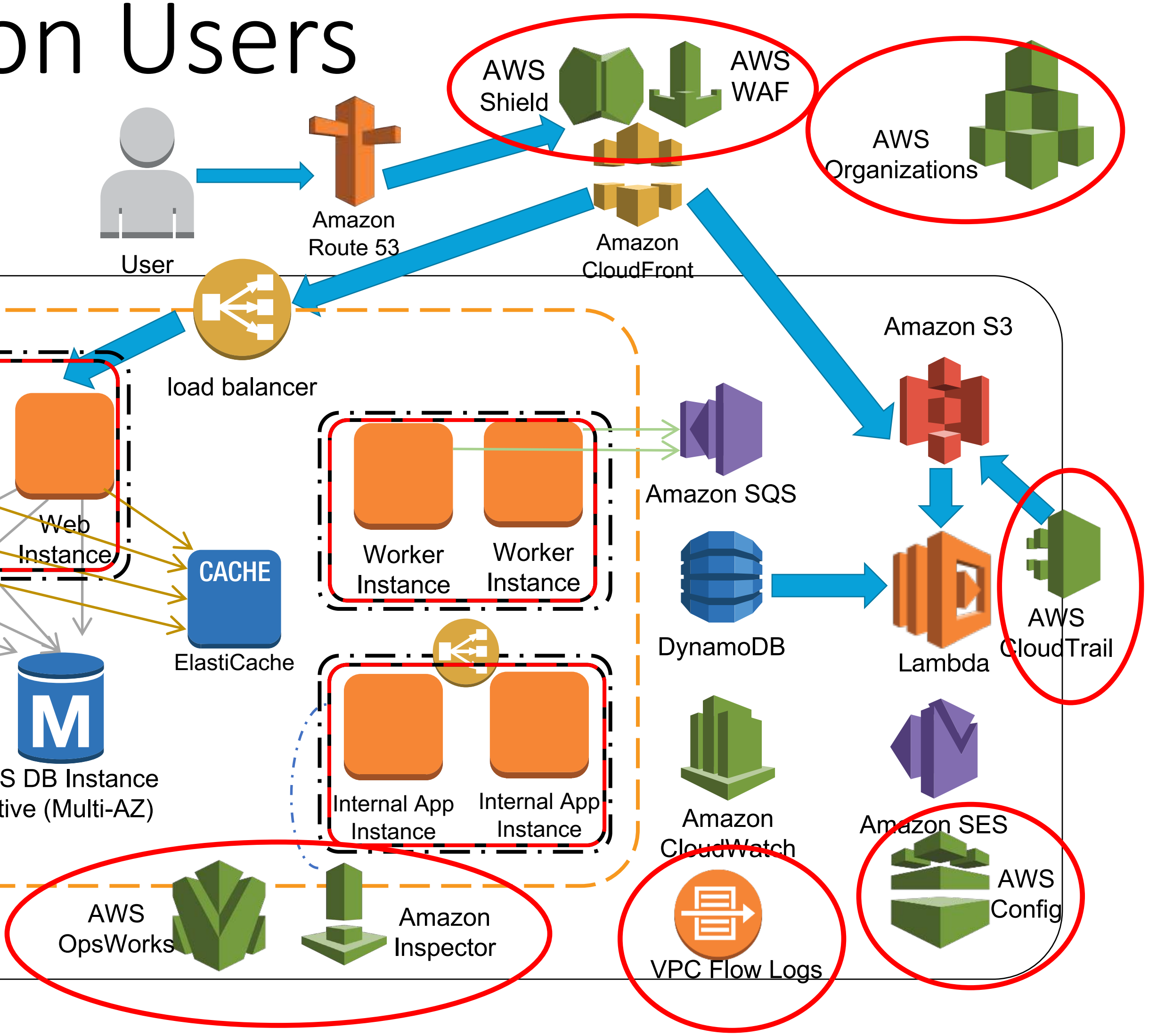


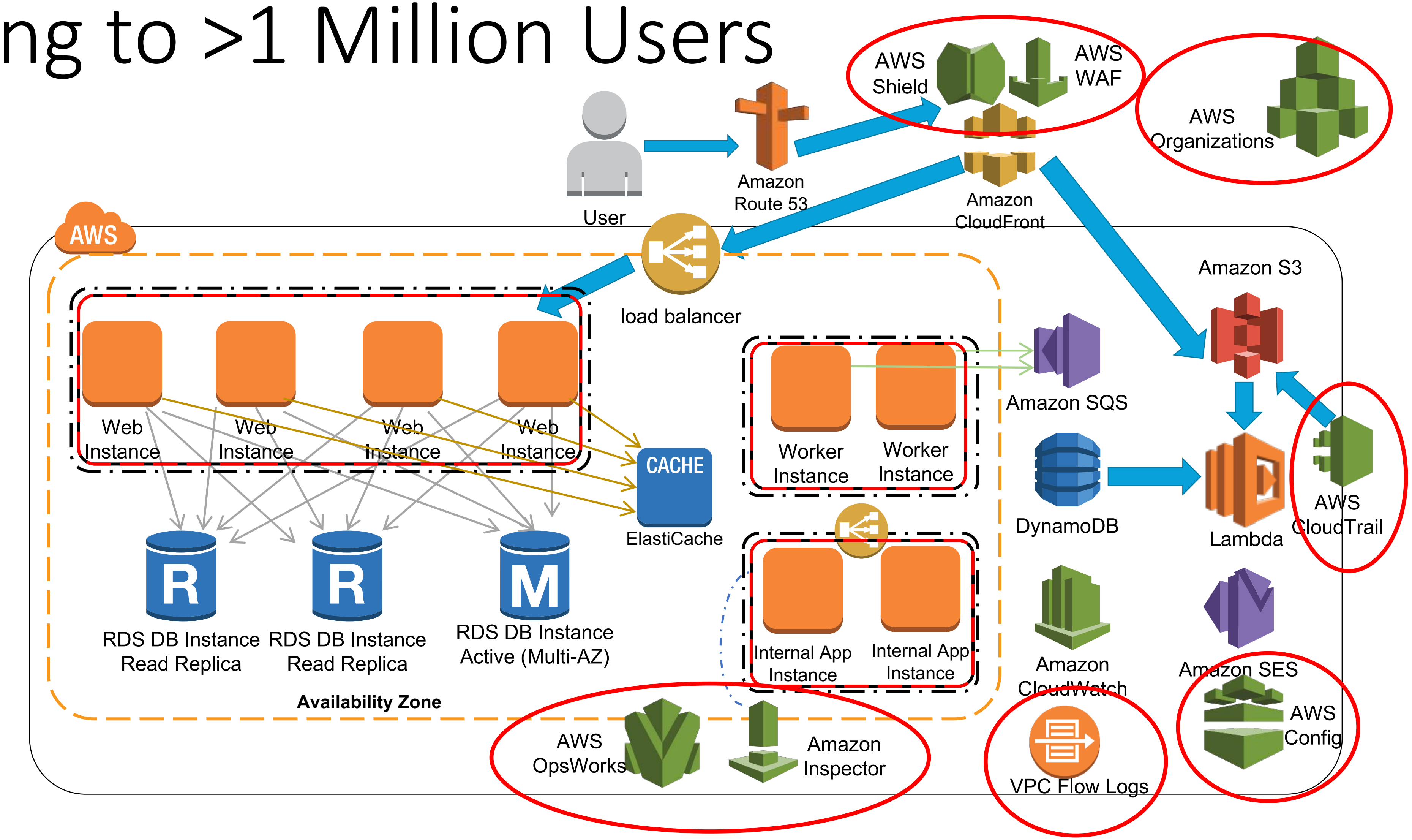
	Event time	User name	Event name	Resource type	Resource name
▶	2016-07-12, 10:29:56 ...	awslambda_325_2016...	StartLogging	CloudTrail Trail	arn:aws:cloudtrail:us-...
▶	2016-07-12, 10:29:55 ...	awslambda_325_2016...	CreateLogStream		
▶	2016-07-12, 10:29:08 ...	jdulac	StopLogging	CloudTrail Trail	arn:aws:cloudtrail:us-...

Scaling to >1 Million Users



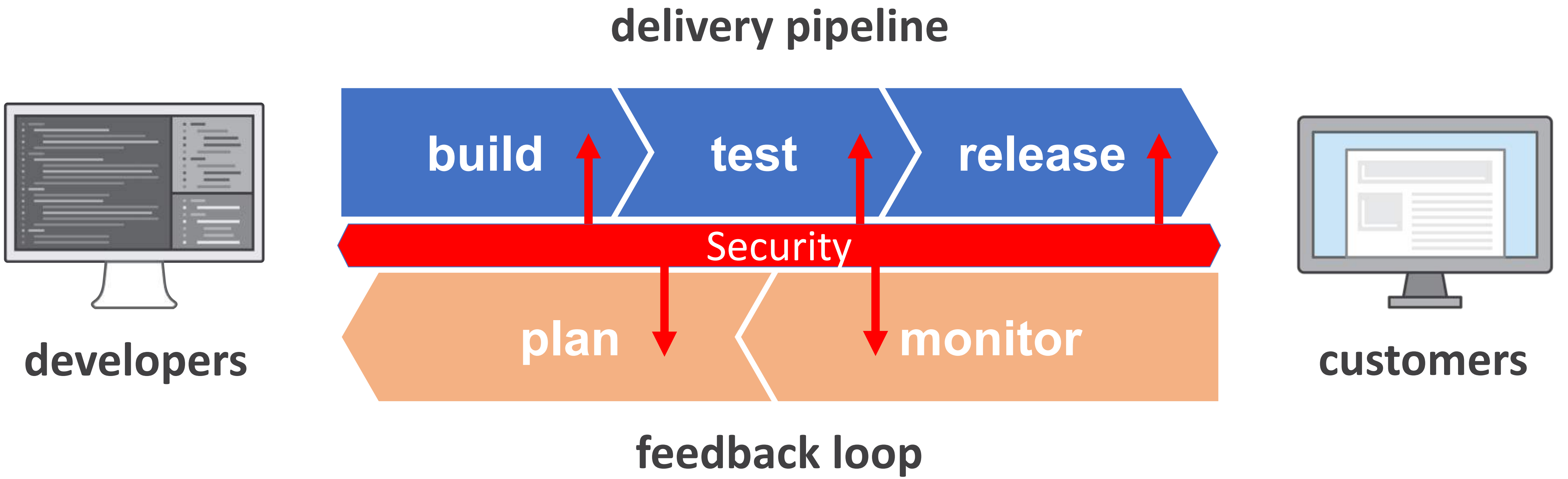
Scaling to >1 Million Users





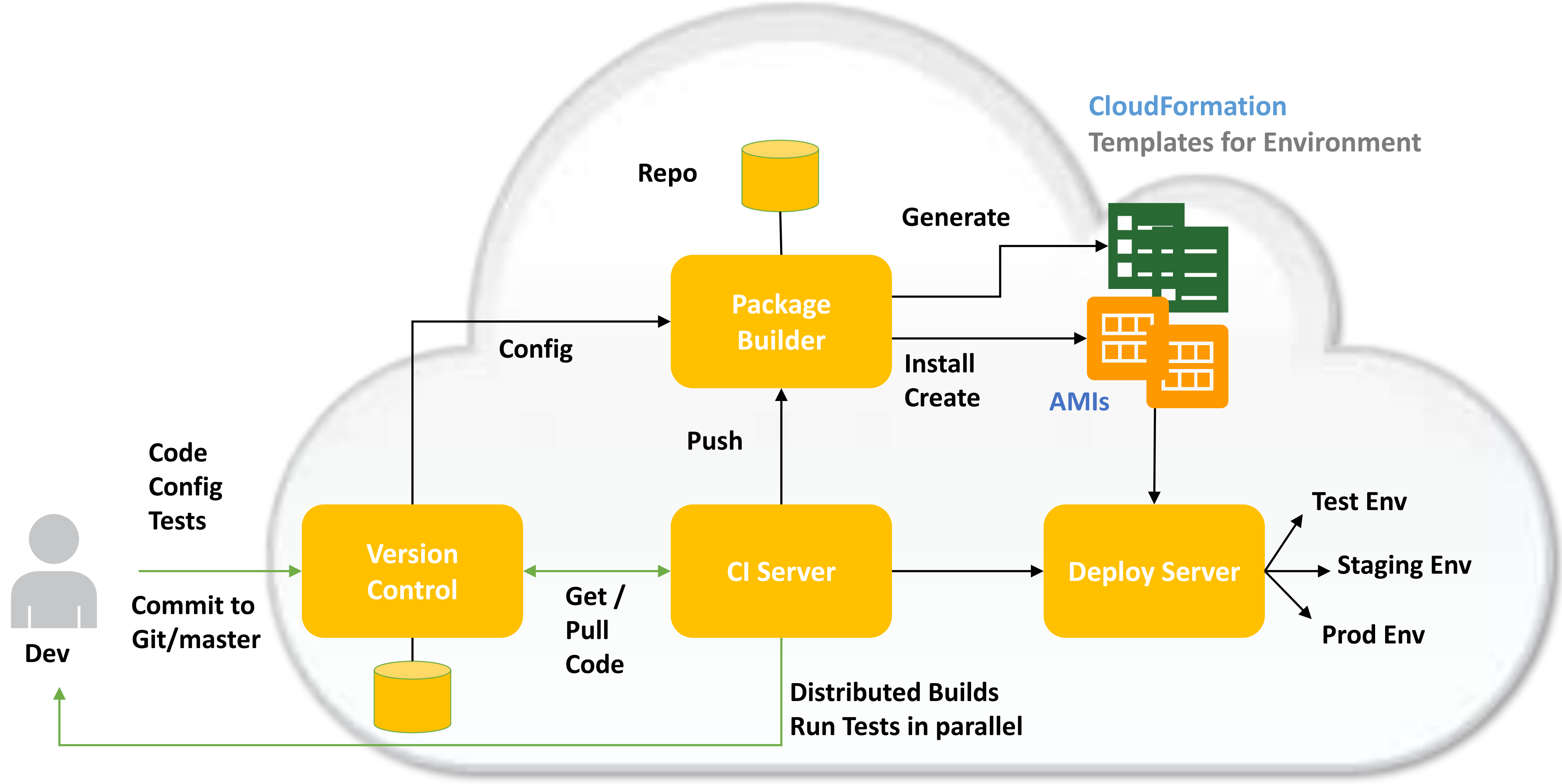
Security + DevOps = DevSecOps

Software development lifecycle



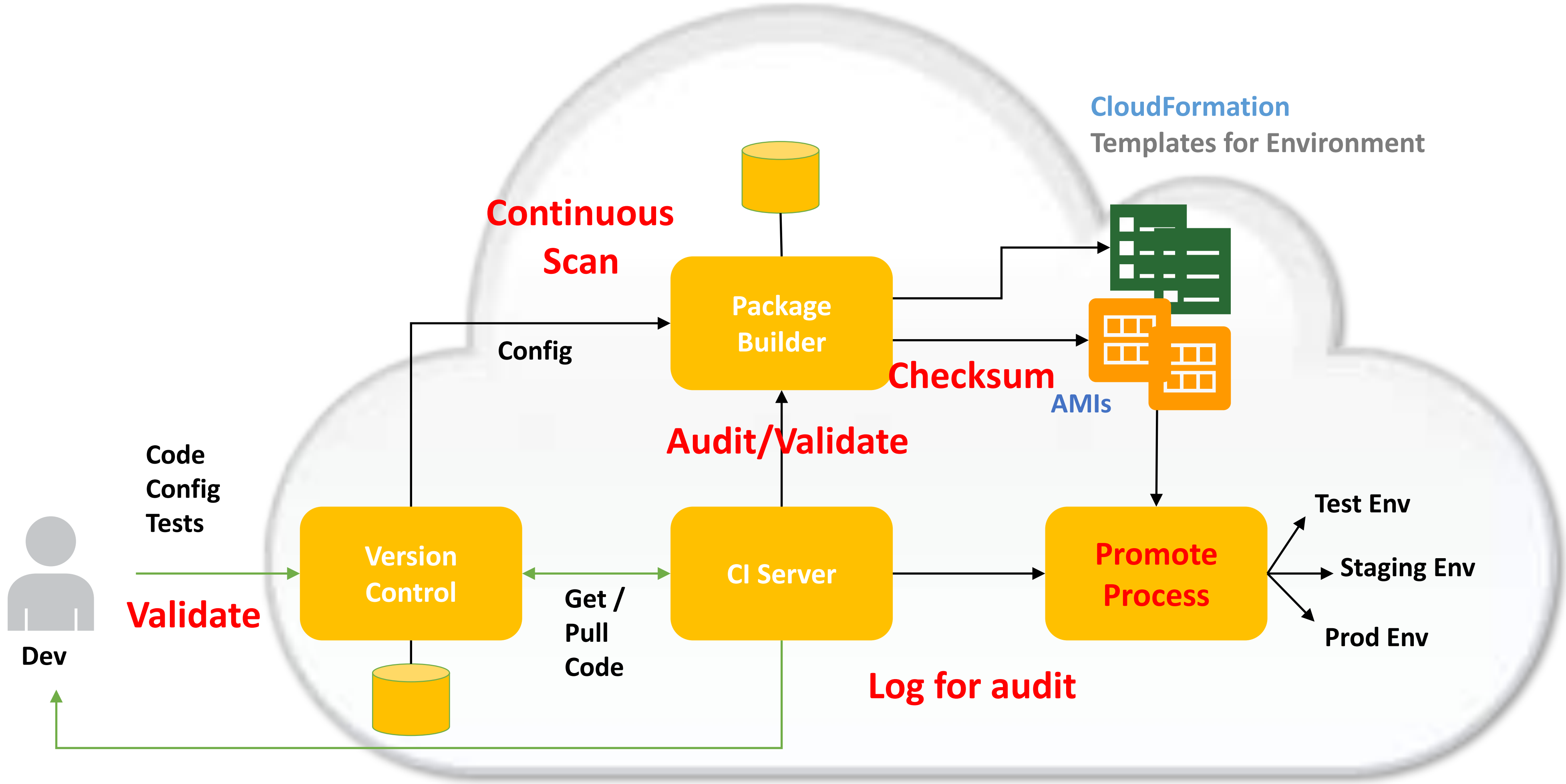
DevOps = **Efficiencies that speed up this lifecycle**
DevSecOps = **Validate building blocks without slowing lifecycle**

CI/CD for DevOps



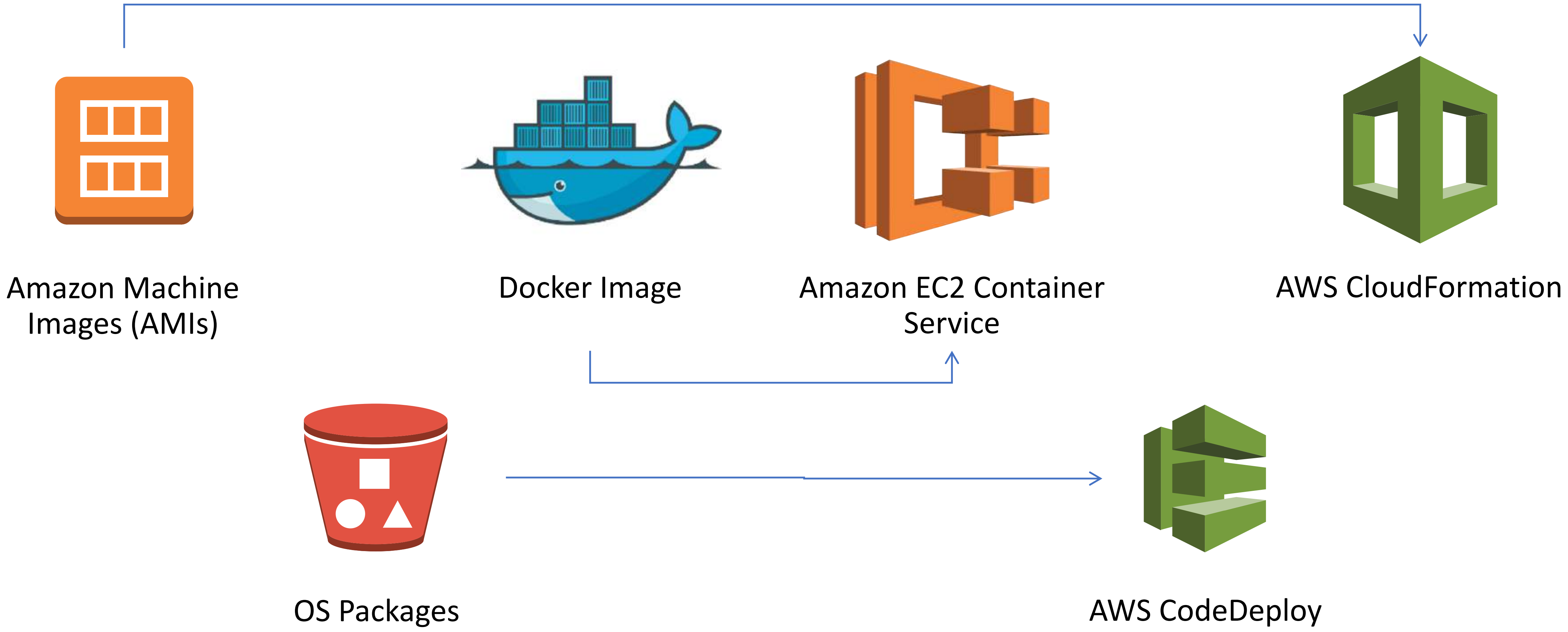
Send Build Report to Dev
Stop everything if build failed

CI/CD for DevSecOps



Send Build Report to Security
Stop everything if audit/validation failed

Deployment Mechanisms for Software Artifacts



Amazon Machine Images (AMIs)

Docker Image

Amazon EC2 Container Service

AWS CloudFormation

OS Packages

AWS CodeDeploy

Deployment Mechanisms for Software Artifacts

Software Artifacts

Amazon Machine Images (AMIs)

Docker Images

OS Packages

Deployment Services

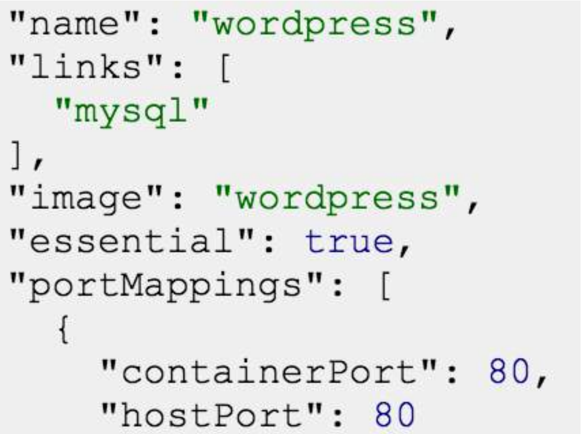
Amazon EC2 Container Service

AWS CloudFormation

AWS CodeDeploy

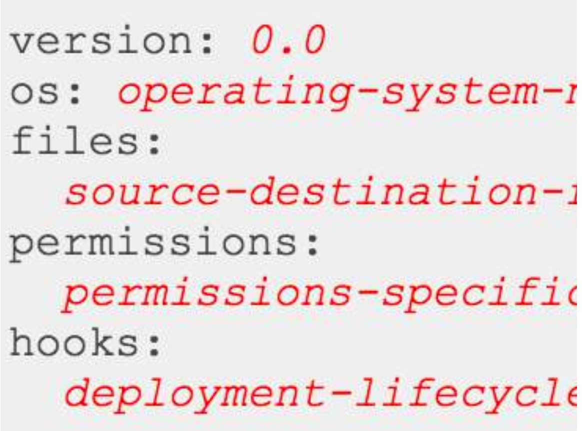
Configuration building blocks

CloudFormation Template



```
"name": "wordpress",
"links": [
  "mysql"
],
"image": "wordpress",
"essential": true,
"portMappings": [
  {
    "containerPort": 80,
    "hostPort": 80
```

Task Definition



```
version: 0.0
os: operating-system-r
files:
  source-destination-f
permissions:
  permissions-specific
hooks:
  deployment-lifecycle
```

Application Specification File (AppSpec file)

…and more.

Amazon EC2 Systems Manager

- Announced at Re:Invent 2016
- See sessions WIN401 (https://www.youtube.com/watch?v=Eal9K0aGLYI) and WIN402 (https://www.youtube.com/watch?v=L5TglwWI5Yo)

Systems Manager Capabilities

Configuration Administration

- Run Command
- State Manager

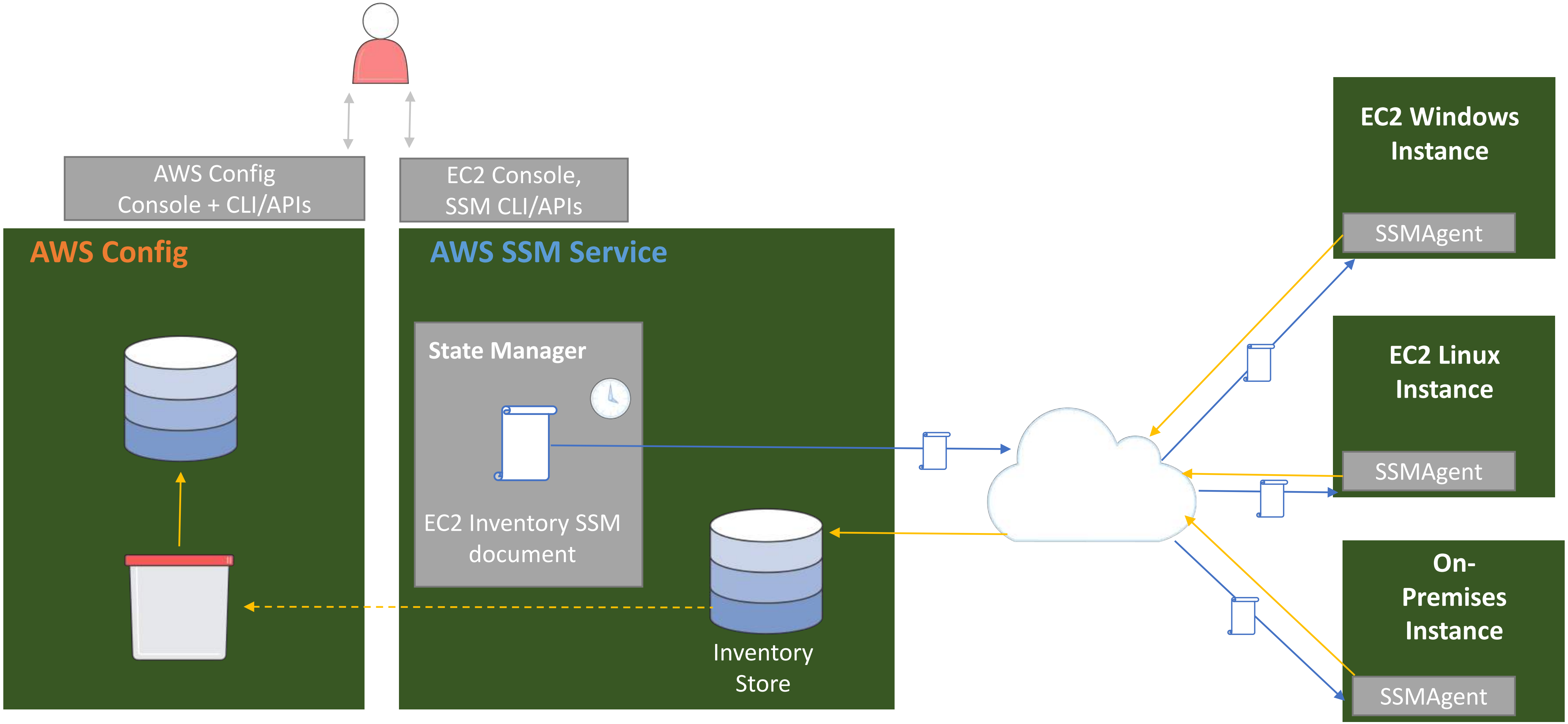
Shared Capabilities

- Maintenance Windows
- Parameter Store

Update and Track

- Automation
- Inventory
- Patch Manager

Inventory – System Diagram



State Manager Associations

```
aws ssm create-association
--document-name WebServerDocument
--document-version \$DEFAULT
--schedule-expression cron(0 */30 * * * ? *)
--targets “Key=tag:Name;Values=WebServer”
--output-location "{ \"S3Location\": { \"OutputS3Region\": \“us-east-1\",
\"OutputS3BucketName\": \“MyBucket\", \"OutputS3KeyPrefix\": \“MyPrefix\" } }“
```

Configures all instances that match the tag query and reapplies every 30 minutes

Parameter Store Substitution

```
$ aws ssm put-parameter
--name myprivatekey
--type SecureString
--value “-----BEGIN RSA PRIVATE KEY-----
WtcUTC+57cf…”
--key-id <KMS keyID>
$ aws ssm send-command
--name Insert-Websvr-Private-Key
--parameters commands=[“cat {{ssm:myprivatekey}} >
/etc/apache2/keys/private.key ; chmod 400
/etc/apache2/keys/private.key ; chown webserver:webserver
/etc/apache2/keys/private.key”]
--target Key=tag:Name,Values=WebServer
```

AWS Marketplace Security Partners

Infrastructure Security

- CISCO
- f5
- CiTRIX
- SOPHOS
- Barracuda
- FORTINET
- intel Security
- paloalto networks
- Check Point We Secure the Internet.
- IMPERVA

Logging & Monitoring

- ALERTLOGIC
- splunk>
- sumologic
- CloudPassage
- loggly

Identity & Access Control

- okta
- CIPHERGRAPH networks
- Elastic SSO
- conjur
- onelogin

Configuration & Vulnerability Analysis

- QUALYSGUARD
- TREND MICRO
- tenable network security
- RAPID7
- evident.io

Data Protection

- gemalto security to be free
- Vormetric Data Security Simplified
- HYTRUST
- KeyNexus
- Townsend SECURITY
- druva

Summary

- AWS security benefits:
  - Integrated security & compliance
  - Global resilience, visibility, & control
  - Maintain your privacy and data ownership
  - Agility through security automation
  - Security innovation at scale
  - Broad security partner & marketplace solutions

Helpful Resources

Compliance Enablers:	https://aws.amazon.com/compliance/compliance-enablers/
Risk & Compliance Whitepaper:	https://aws.amazon.com/whitepapers/overview-of-risk-and-compliance/
Compliance Centre Website:	https://aws.amazon.com/compliance
Security Centre:	https://aws.amazon.com/security
Security Blog:	https://blogs.aws.amazon.com/security/
Well-Architected Framework:	https://aws.amazon.com/blogs/aws/are-you-well-architected/
AWS Audit Training:	awsaudittraining@amazon.com

New Security and Compliance Webinar Series

- Getting Started with AWS Security: https://www.brighttalk.com/webcast/9019/256391
- AWS Security Checklist:
  https://www.brighttalk.com/webcast/9019/257297
- Automating Security Event Response: https://www.brighttalk.com/webcast/9019/258547
- Compliance with AWS – Verifying AWS Security: https://www.brighttalk.com/webcast/9019/260695
- Securing Enterprise Big Data Workloads: https://www.brighttalk.com/webcast/9019/261911
- Architecting Security across Multi-Acct Architectures: https://www.brighttalk.com/webcast/9019/261915
- AWS Security Best Practices: https://www.brighttalk.com/webcast/9019/264011
- Software Security and Best Practices: https://www.brighttalk.com/webcast/9019/264917

AWS

SUMMIT

Thank you!

amazon web services

AWS

SUMMIT

Security at Scale on AWS

Dave Walker – Specialist Solutions Architect, Security and Compliance

Chris Astley – Head of Cloud Ops, Tech Solutions KPMG UK

28/06/17

amazon
web services

KPMG CloudOps

3 years

150+ Projects

250+ Production workloads

25 Engineers

All sectors

Banking

Global investment banking client

Public Sector

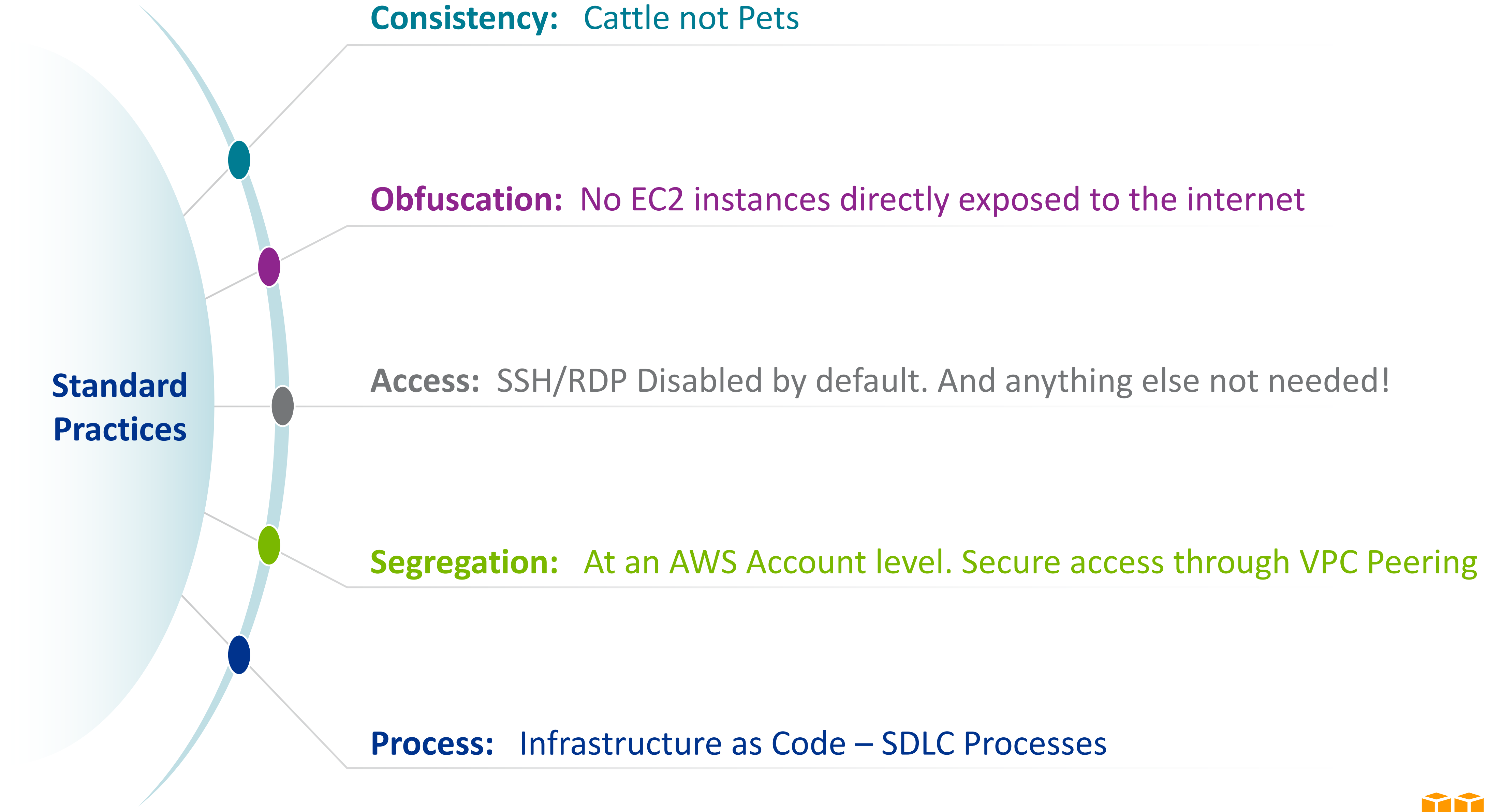
Government Civil Service

Retail

Multi-national FMCG retailer

Tax and Audit

KPMG Tax



Standard Practices

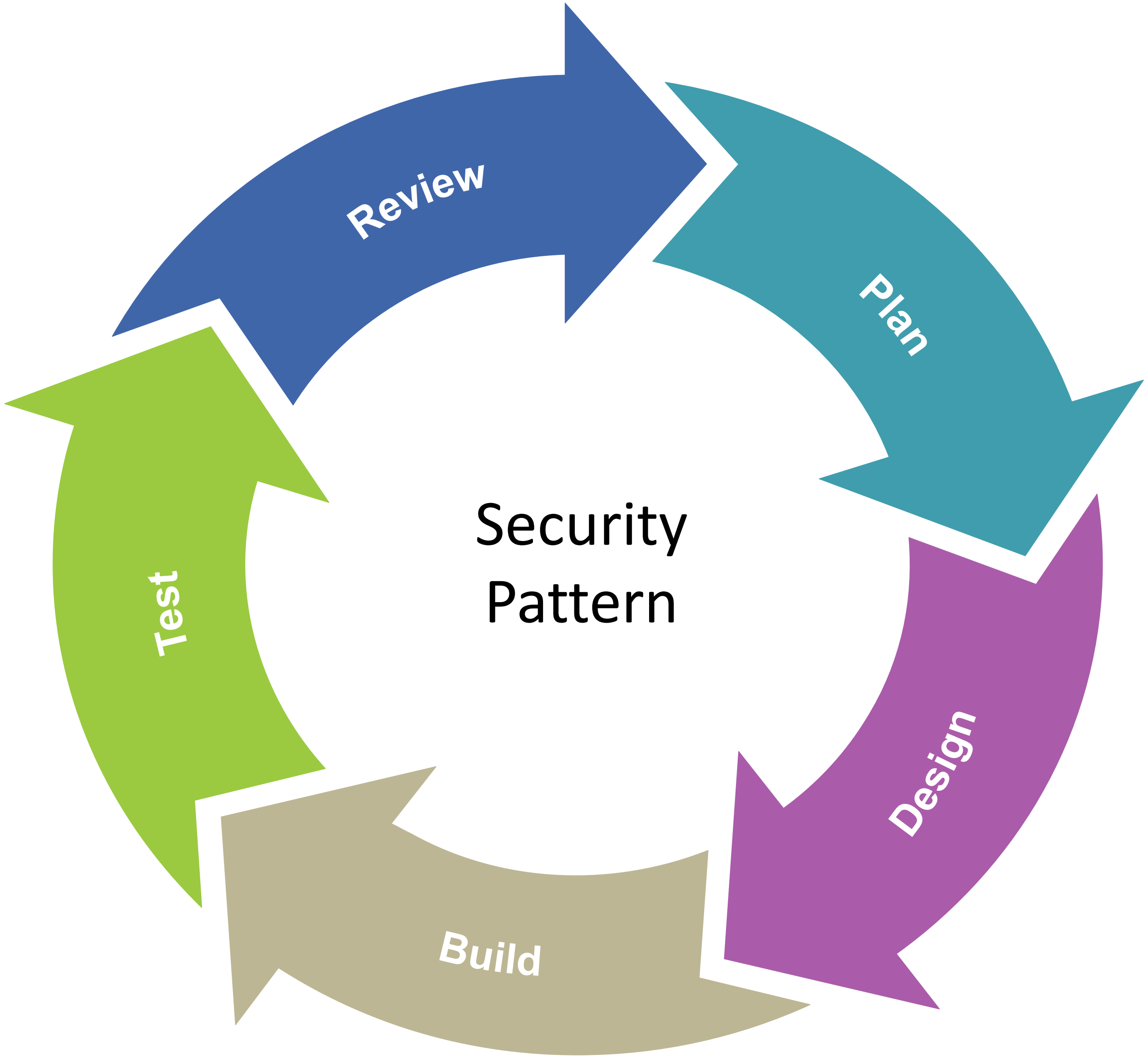
Consistency: Cattle not Pets

Obfuscation: No EC2 instances directly exposed to the internet

Access: SSH/RDP Disabled by default. And anything else not needed!

Segregation: At an AWS Account level. Secure access through VPC Peering

Process: Infrastructure as Code – SDLC Processes

Review
Plan
Design
Build
Test
Security
Pattern

Cloud	On-Premise
No instances internet facing	LOTS of instances internet facing
RDS for automated DB patching	Manual DB patching – limited HA
SMB disabled in Security Groups	Limited internal network restrictions
Account segregation – limit blast radius	One instance could expose the estate
Gold AMI patched and rolled out	Individual servers patched in-line

AWS SUMMIT

Thank you!

amazon web services