



# INNOVATE2018

## ONLINE CONFERENCE



# AWS Security for Builders: Best Practices (Level 200)

Myles Hosford, Principal Security Architect

# What to expect from this session

Learn **security best practices** for **builders** in the following topics:

- Identity & Access Management
- Logging & Monitoring
- Infrastructure Security
- Data Protection
- Incident Response

# Introduction

Before...

# Introduction

Before...

Move fast

Stay secure

# Introduction

Before...

Move fast

OR

Stay secure

# Introduction

Now...

Move fast

AND

Stay secure

# AWS Cloud Security Epics

## Core 5 Security Epics

Identity & Access Management

Logging & Monitoring

Infrastructure Security

Data Protection

Incident Response

## Augmenting the Core 5

Secure CI/CD:  
DevSecOps

Compliance Validation

Resilience

Configuration &  
Vulnerability Analysis

Security Big Data &  
Analytics

# AWS Native Security Services



## Identity

AWS Identity & Access Management (IAM)  
AWS Organizations  
AWS Cognito  
AWS Directory Service  
AWS Single Sign-On



## Detective control

AWS CloudTrail  
AWS Config  
Amazon CloudWatch  
Amazon GuardDuty  
VPC Flow Logs



## Infrastructure security

Amazon EC2 Systems Manager  
AWS Shield  
AWS Web Application Firewall (WAF)  
Amazon Inspector  
Amazon Virtual Private Cloud (VPC)



## Data protection

AWS Key Management Service (KMS)  
AWS CloudHSM  
Amazon Macie  
Certificate Manager  
Server Side Encryption



## Incident response

AWS Config Rules  
AWS Lambda



# Identity & Access Management

# IAM 1: Do not use 'root' account

- The root user has complete access to all AWS services and resources in the account.
- Do not use the root user for your everyday tasks, even the administrative ones.
- We recommended creating an AWS IAM user, even for admin.



# IAM 1: Do not use 'root' account

- The root user has complete access to all AWS services and resources in the account.
- Do not use the root user for your everyday tasks, even the administrative ones.
- We recommended creating an AWS IAM user, even for admin.



John



Chloe

# IAM 2: Enable MFA

- AWS supports software and hardware MFA tokens
- Significantly reduces the likelihood of account compromise
- Easy to use and setup!

Account:

User Name:

Password:

☒ I have an MFA Token (more info)

MFA Code:



# IAM 3: Restrict Long Standing Access Keys

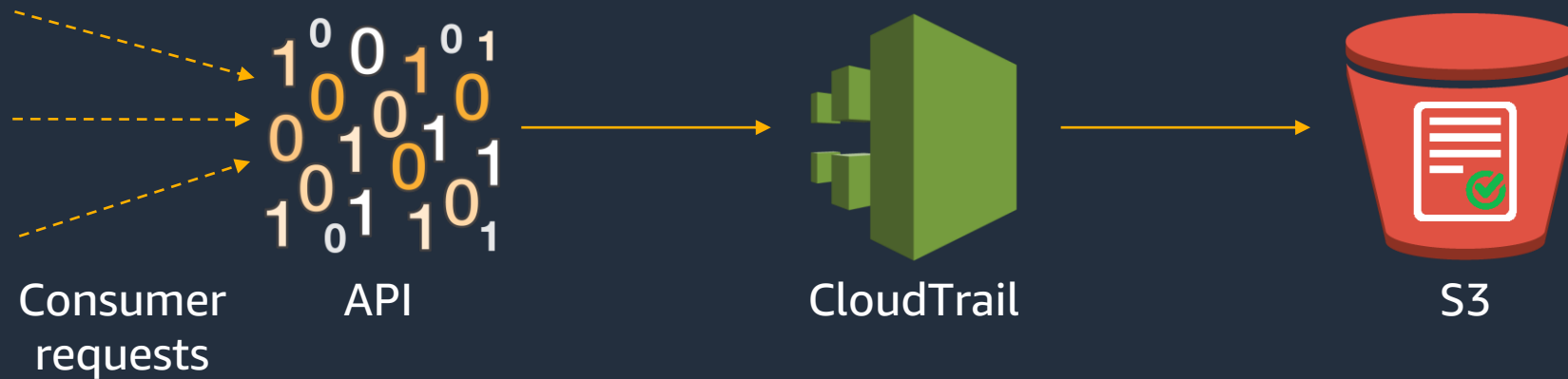


AWS STS

- Programmatic access to AWS typically uses access keys.
- Developers accessing AWS from their dev laptops
- EC2 instances accessing the wider AWS eco-system
- Solution: Assume Role to request temporary, time bound credentials.

# Logging & Monitoring

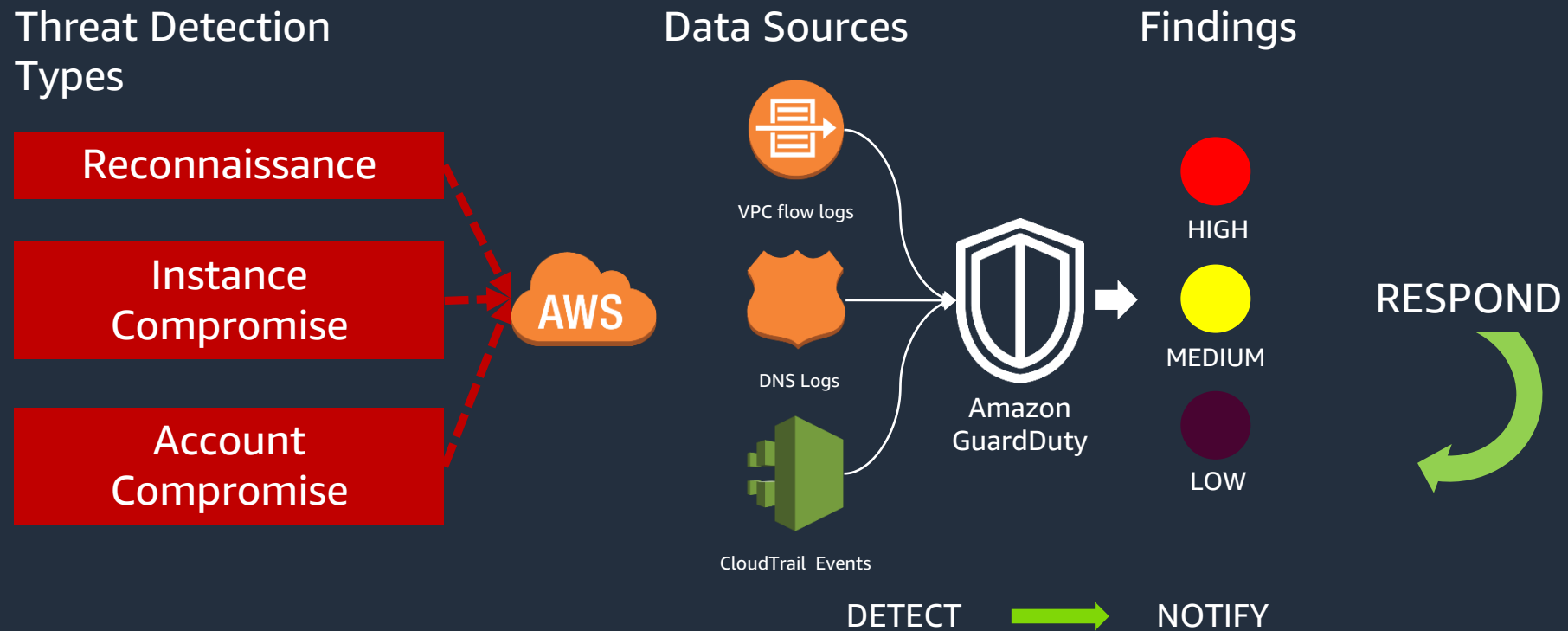
# LOG 1: Enable AWS CloudTrail



CloudTrail provides:

- **Who** did **what** from **where** and exactly **when**
- **Stored** for audit and inspection
- **Reviewed** periodically

# LOG 2: Enable Amazon GuardDuty





# LOG 3: Build Automated Notifications



Examples:

- Root login
- GuardDuty findings
- Security group changes
- KMS Key activity

# Infrastructure Security

# INF 1: Patch Your Systems

## AWS Systems Manager



Run command



State manager



Inventory



Maintenance window



Patch manager



Automation

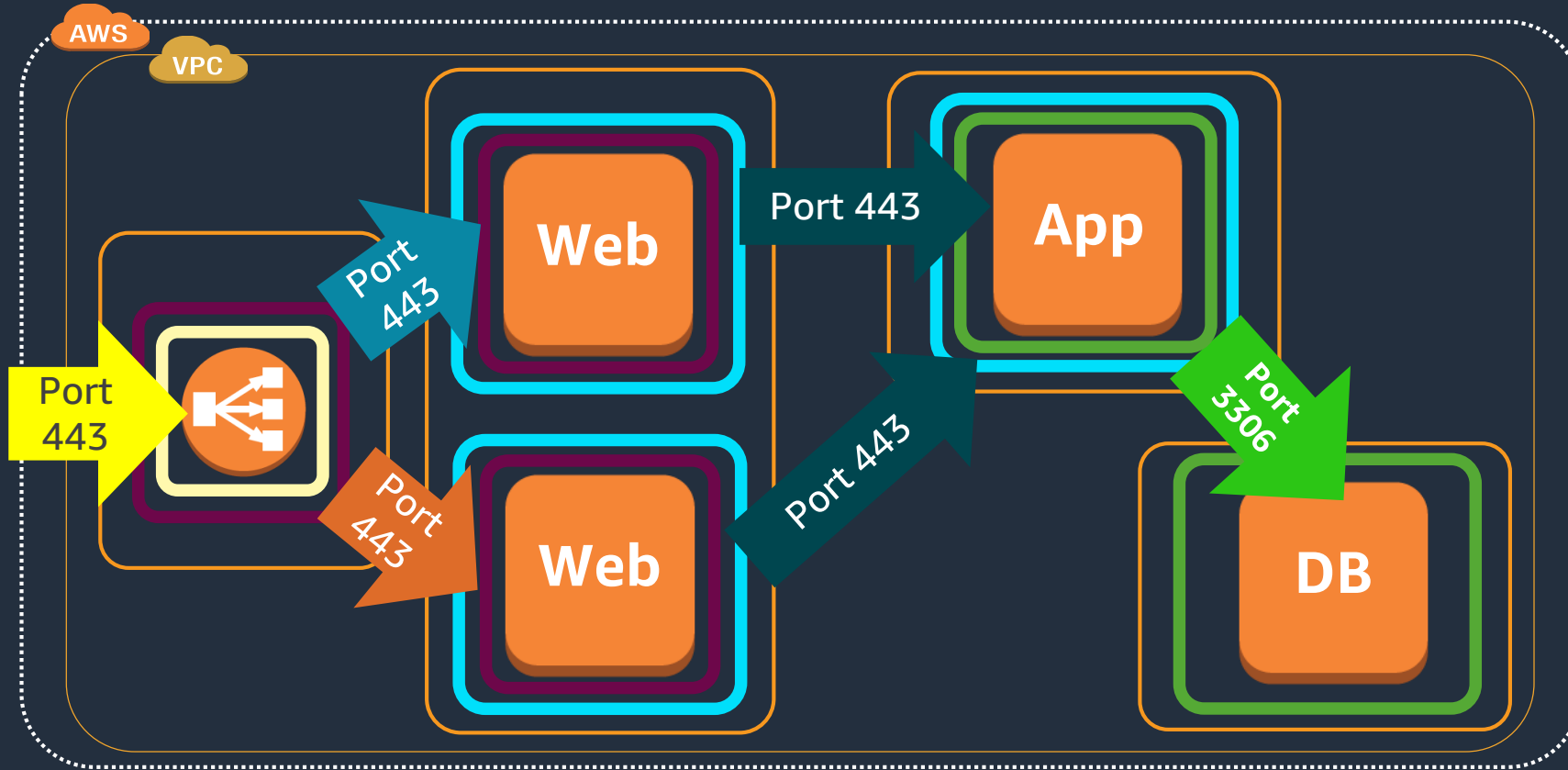


Parameter store



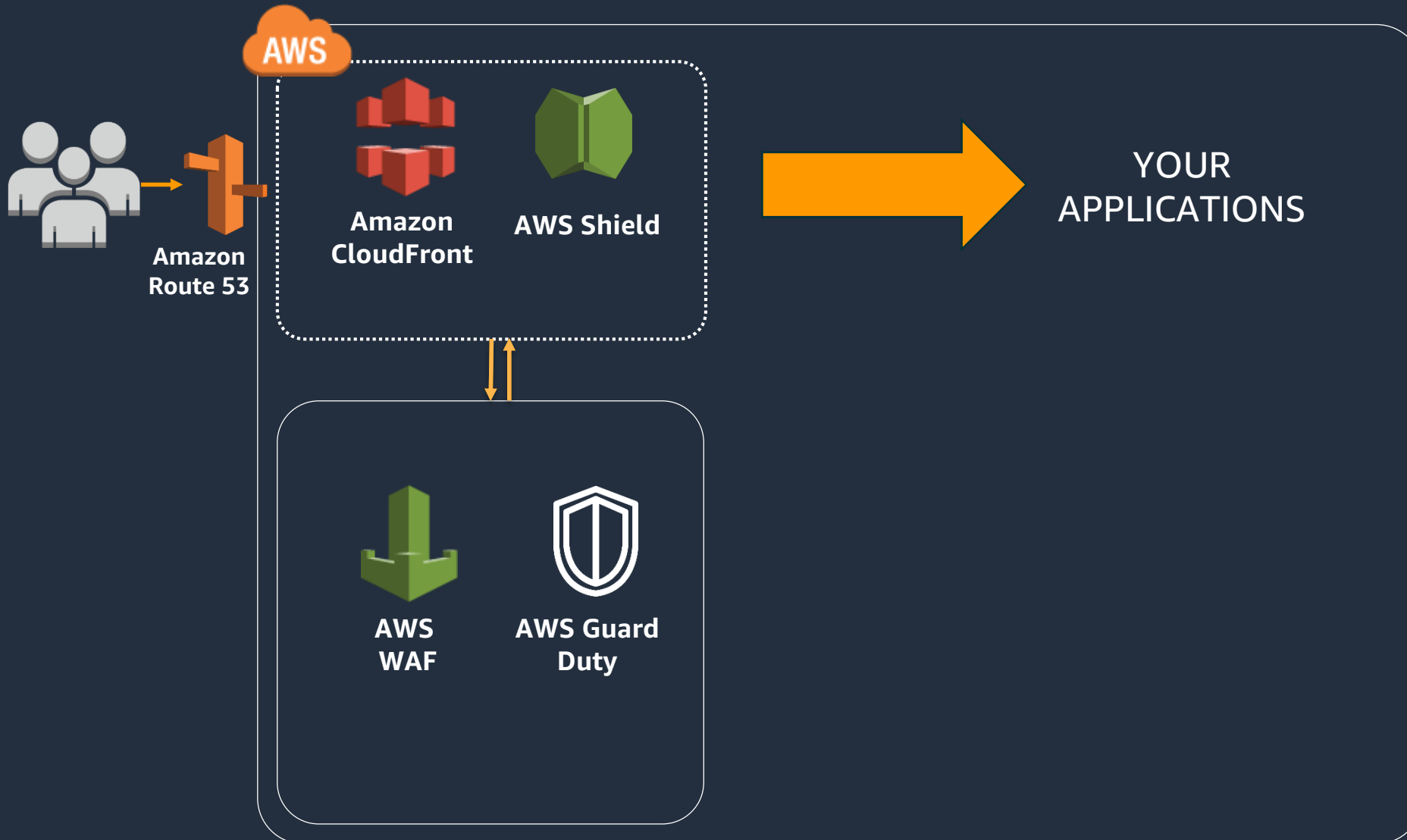
Documents

# INF 2: Reduce Your Attack Surface



- ✓ Private Subnets
- ✓ Restrict Security Groups
- ✓ Bastion Hosts

# INF 3: Create a DDoS Resilient Architecture

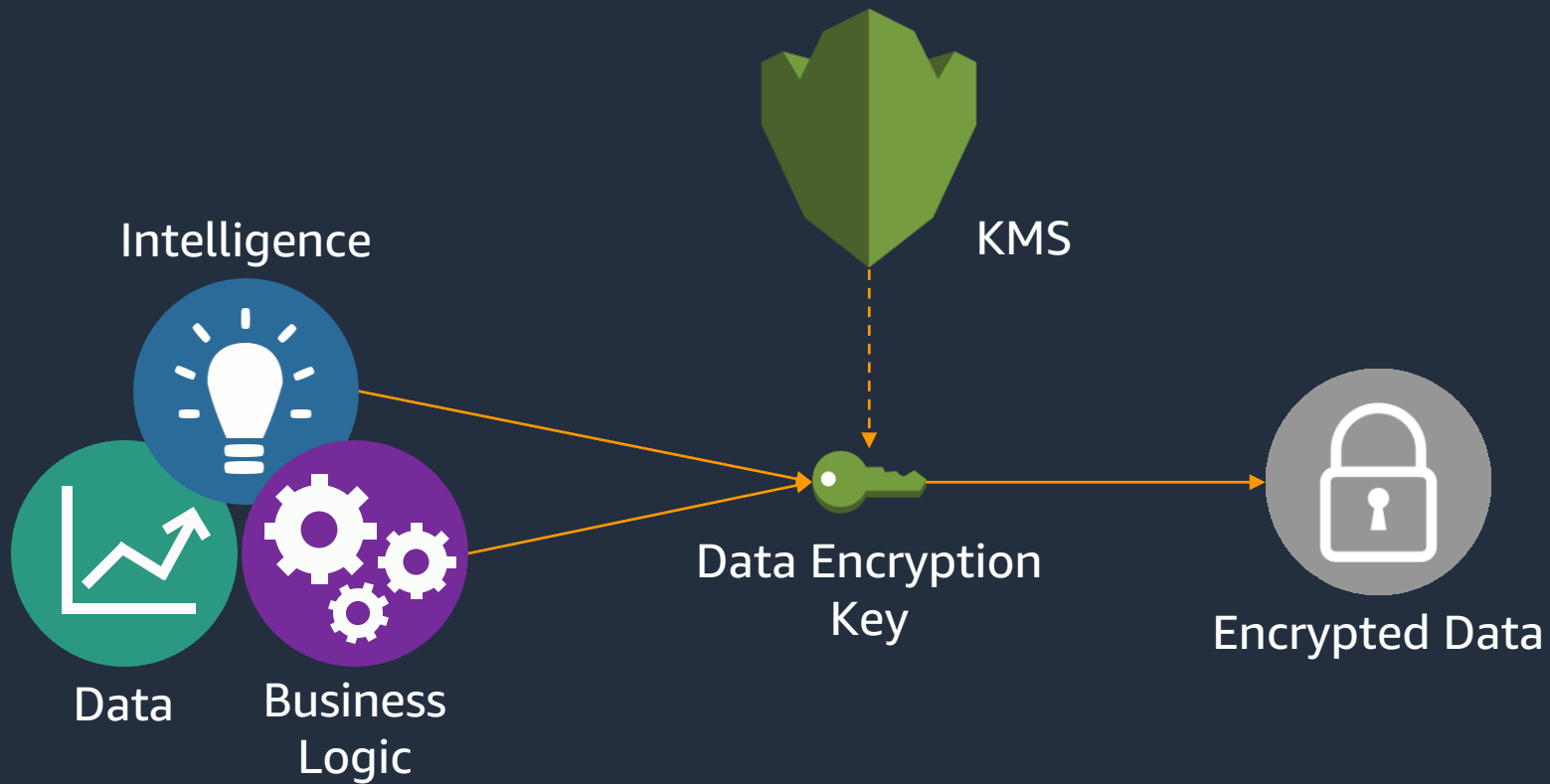


- ✓ Amazon Route53
- ✓ Amazon CloudFront
- ✓ AWS WAF
- ✓ AWS Shield

# Data Protection

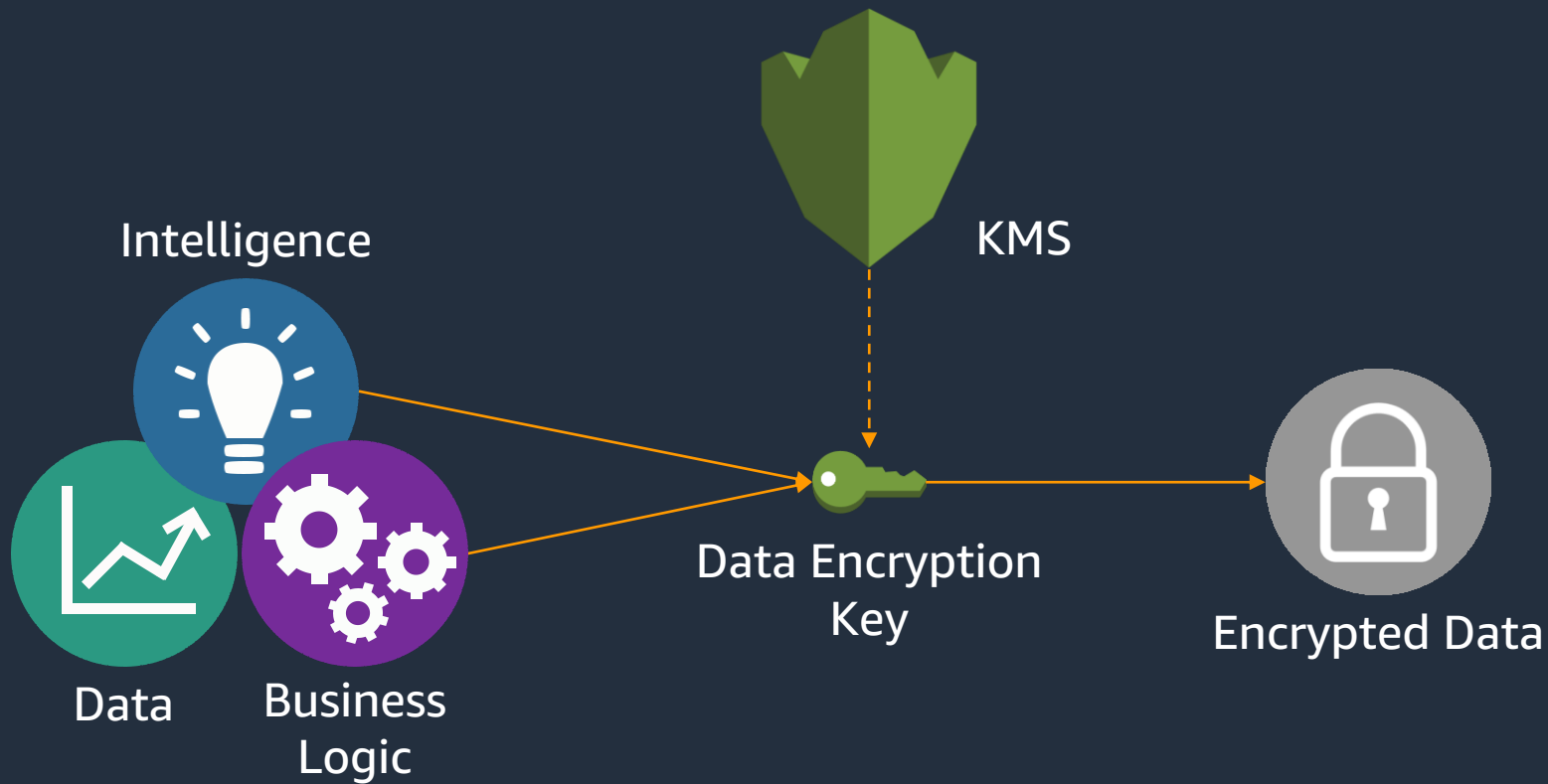
# DP 1: Encrypt Everything

## AWS Key Management Service



# DP 1: Encrypt Everything

## AWS Key Management Service



**Create Volume** [X]

Type ⓘ General Purpose (SSD) ▼

Size (GiB) ⓘ 100 (Min: 1GiB, Max: 1024GiB)

IOPS ⓘ 300 / 3000 (3000 IOPS bursts and baseline of 3 IOPS per GB)

Availability Zone ⓘ us-east-1b ▼

Snapshot ID ⓘ Search (case-insensitive)

Encryption ⓘ ☒ Encrypt this volume

Master Key ⓘ CriticalData ▼

**Key Details**

Description	This key protects critical data in my account
Account	This account (109007692119)
KMS Key ID	e3a34145-7757-4c74-a0ec-33d40cac295

Cancel Create



# DP 2: Implement Strong Access Control

Everyone

**⚠ This bucket will have public access**  
Everyone will have access to one or all of the following: list objects, write objects, read and write permissions.

Access to the objects

- ☒ List objects
- ☒ Write objects

Access to this bucket's ACL

- ☒ Read bucket permissions

Cancel Save

## PREVENT

- IAM Policies

## DETECT

- CloudWatch Events
- Config Rules
- SNS

# DP 3: Do not Store Secrets in Clear-Text

## AWS Secrets Manager

- ✓ Rotate secrets safely
- ✓ Manage access with fine-grained policies
- ✓ Secure and audit secrets centrally

Step 1  
**Secret type**

Step 2  
Name and description

Step 3  
Configure rotation

Step 4  
Review

AWS Secrets Manager > Secrets > Store a new secret

### Store a new secret

**Select secret type** [Info](#)

☒ Credentials for RDS database ☐ Credentials for other database ☐ Other type of secrets (e.g. API key)

Specify the user name and password to be stored for this secret. [Info](#)

User name:

Password:

☐ Show password

**Select the encryption key** [Info](#)

Select the AWS KMS key to use to encrypt your secret information. You can encrypt using the default service encryption key that AWS Secrets Manager creates on your behalf or a customer master key (CMK) that you have stored in AWS KMS.

[Add new key](#) [↗](#)

**Select which RDS database this secret will access** [Info](#)

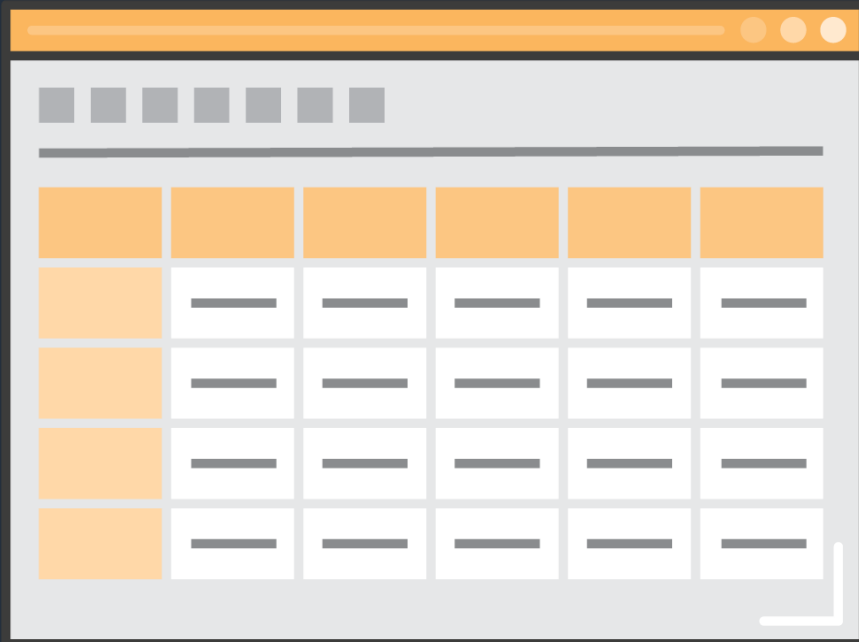
< 1 >

	DB instance	DB Engine	Status	Creation date
<input checked="" type="radio"/>	twitterapp2	aurora	available	04/02/2018
<input type="radio"/>	twitterapp2-us-east-1a	aurora	available	04/02/2018

Cancel **Next**

# Incident Response

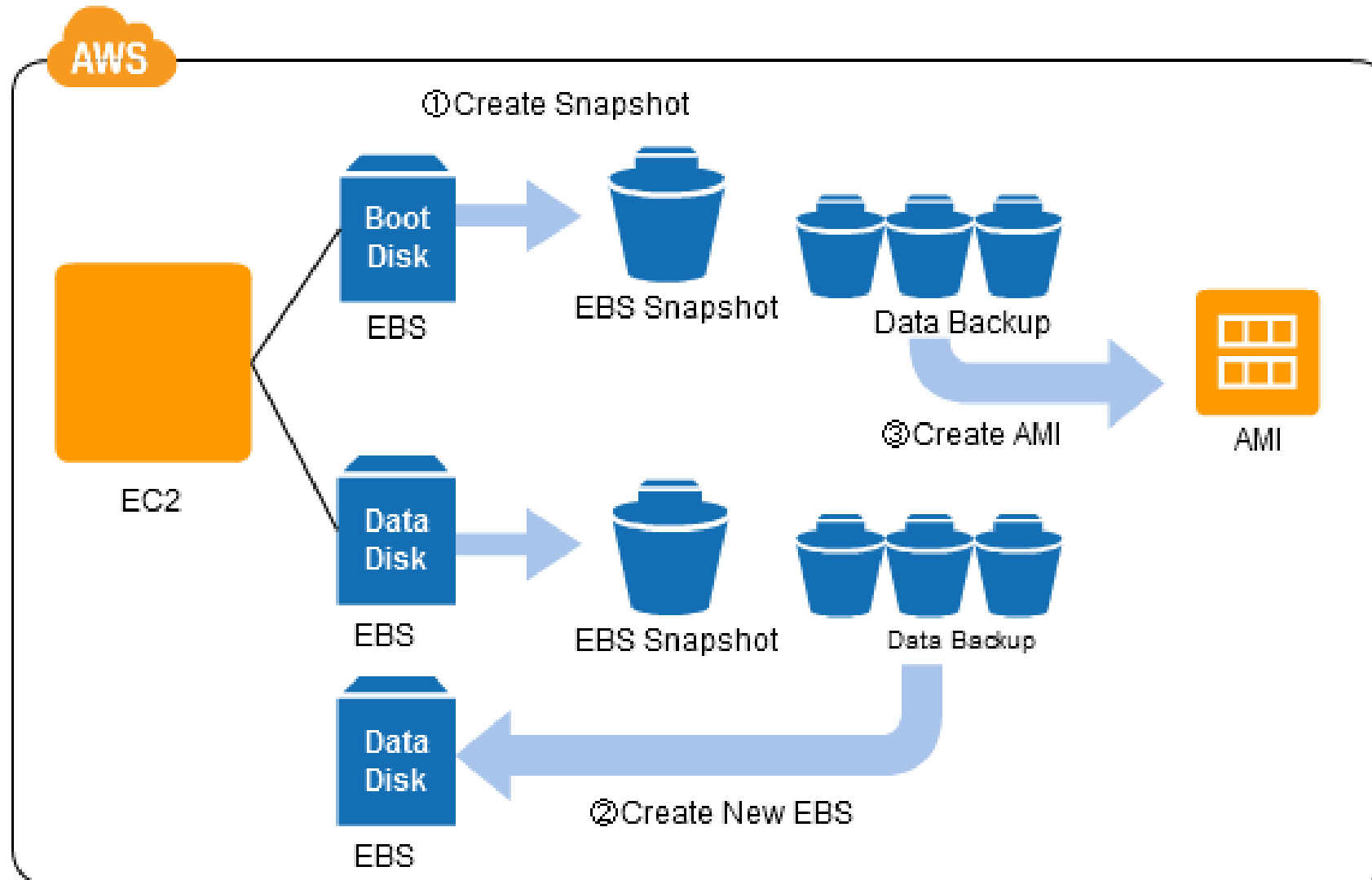
# IR 1: Have a Plan & Test It



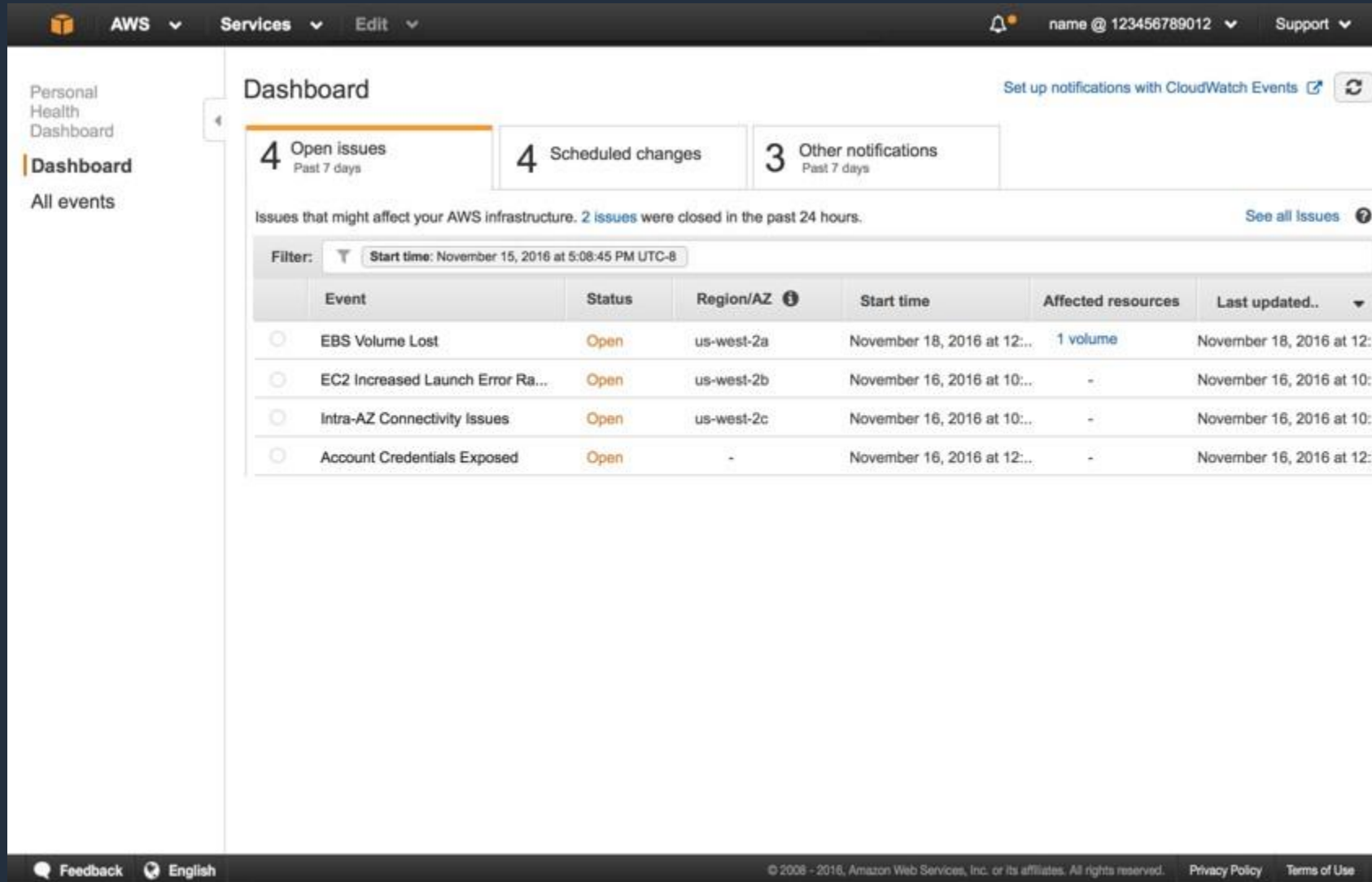
## Elements of a Incident Response Plan

- Roles & Responsibilities
- Identify
- Contain
- Respond
- Recover

# IR 2: Backup and Restore



# IR 3: Personal Health Dashboard & Trusted Advisor









The screenshot displays the AWS Personal Health Dashboard. The top navigation bar includes the AWS logo, 'Services', 'Edit', a user profile 'name @ 123456789012', and a 'Support' link. The left sidebar shows 'Personal Health Dashboard' and 'Dashboard' (selected). The main content area is titled 'Dashboard' and features three summary cards: '4 Open issues Past 7 days', '4 Scheduled changes', and '3 Other notifications Past 7 days'. Below these cards, a message states 'Issues that might affect your AWS infrastructure. 2 issues were closed in the past 24 hours.' with a 'See all issues' link. A filter section shows 'Start time: November 15, 2016 at 5:08:45 PM UTC-8'. A table lists four open issues:

Event	Status	Region/AZ	Start time	Affected resources	Last updated..
EBS Volume Lost	Open	us-west-2a	November 18, 2016 at 12:...	1 volume	November 18, 2016 at 12:...
EC2 Increased Launch Error Ra...	Open	us-west-2b	November 16, 2016 at 10:...	-	November 16, 2016 at 10:...
Intra-AZ Connectivity Issues	Open	us-west-2c	November 16, 2016 at 10:...	-	November 16, 2016 at 10:...
Account Credentials Exposed	Open	-	November 16, 2016 at 12:...	-	November 16, 2016 at 12:...

The footer contains 'Feedback', 'English', copyright information '© 2008 - 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved.', and links for 'Privacy Policy' and 'Terms of Use'. The AWS and Intel logos are in the bottom right corner.

# Sources of Best Practices

## AWS Cloud Adoption Framework

 BUSINESS	 PLATFORM
 PEOPLE	 SECURITY
 GOVERNANCE	 OPERATIONS

<https://amzn.to/2GyBclB>

## CIS Foundations Benchmark



<http://bit.ly/aws-cis>

## AWS Well-Architected



<https://amzn.to/2k9VRKp>

# Conclusion

- Build a '**security backlog**' and implement security as features
- Cover the 5 core epics (then explore the other 5):
  - Identity
  - Logging & Monitoring
  - Infrastructure Security
  - Data Protection
  - Incident Response
- Establish a '**security champion**' within your dev team, rotate amongst the team.
- Use AWS native security features to **help your security team** on the journey.



# Learn from AWS experts. Advance your skills and knowledge. Build your future in the AWS Cloud.



## Digital Training

Free, self-paced online courses built by AWS experts



## Classroom Training

Classes taught by accredited AWS instructors



## AWS Certification

Exams to validate expertise with an industry-recognized credential

Ready to begin building your cloud skills?  
Get started at: <https://www.aws.training/>

# With deep expertise on AWS, APN Partners can help your organization at any stage of your Cloud Adoption Journey.



## AWS Managed Service Providers

APN Consulting Partners who are skilled at cloud infrastructure and application migration, and offer proactive management of their customer's environment.



## AWS Competency Partners

APN Partners who have demonstrated technical proficiency and proven customer success in specialized solution areas.



## AWS Marketplace

A digital catalog with thousands of software listings from independent software vendors that make it easy to find, test, buy, and deploy software that runs on AWS.



## AWS Service Delivery Partners

APN Partners with a track record of delivering specific AWS services to customers.

Ready to get started with an APN Partner?  
Find a partner: <https://aws.amazon.com/partners/find/>  
Learn more at the AWS Partner Network Booth

# Thank You for Attending AWS Innovate

We hope you found it interesting! A kind reminder to **complete the survey.**

Let us know what you thought of today's event and how we can improve the event experience for you in the future.



[aws-apac-marketing@amazon.com](mailto:aws-apac-marketing@amazon.com)



[twitter.com/AWSCloud](https://twitter.com/AWSCloud)



[facebook.com/AmazonWebServices](https://facebook.com/AmazonWebServices)



[youtube.com/user/AmazonWebServices](https://youtube.com/user/AmazonWebServices)



[slideshare.net/AmazonWebServices](https://slideshare.net/AmazonWebServices)



[twitch.tv/aws](https://twitch.tv/aws)