



The logo for AWS re:Invent features the word "AWS" in a small, white, sans-serif font above the word "re:Invent" in a large, white, bold, sans-serif font. The "re:" part is positioned to the left of the main "Invent" word. The entire logo is set against a background of a diagonal gradient from dark blue at the top-left to red at the bottom-right.

AWS | re:Invent

# Find All the Threats: AWS Threat Detection and Remediation

Greg McConnel  
Senior Solutions Architect, Security Specialist  
AWS

Jesse Fuchs  
Senior Solutions Architect, Security Specialist  
AWS

Mike Wasielewski  
Senior Solutions Architect, Security Specialist  
AWS

Ram Ramani  
Senior Solutions Architect, Security Specialist  
AWS

# Agenda

- Intro
- Module 1: Environment setup (20 min.)
- Module 2: Attack kickoff (and presentation) (40 min.)
- Module 3: Detect, investigate & respond (45 min.)
- Module 4: Review, questions & cleanup (15 min.)

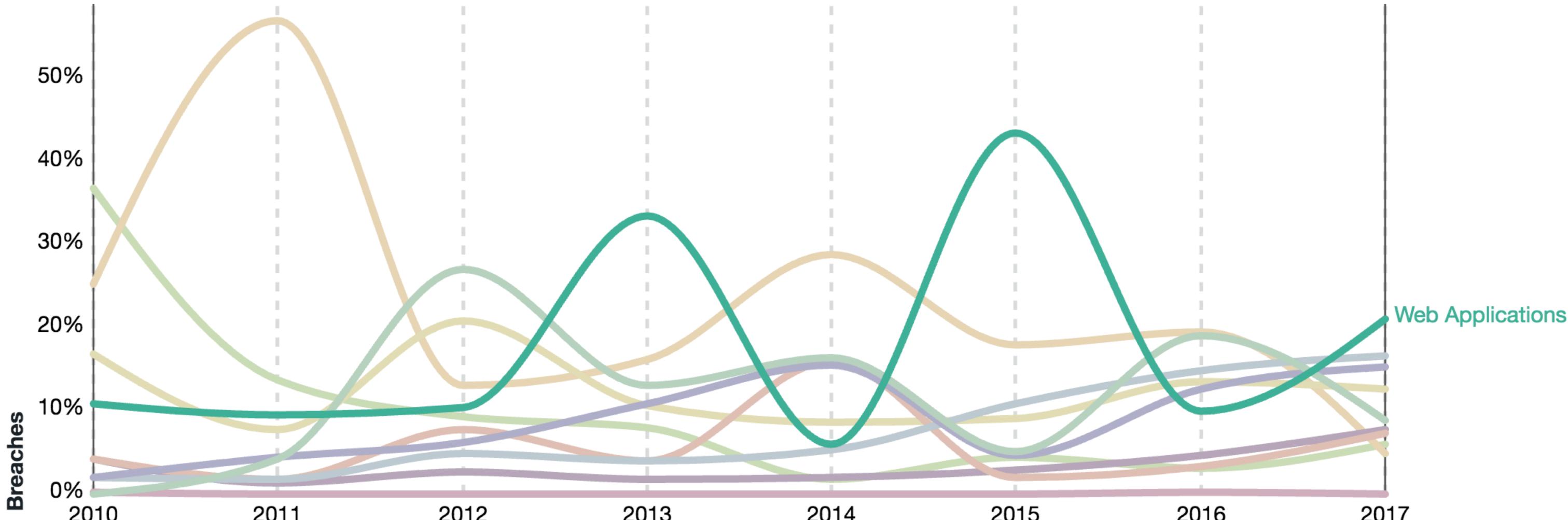
# Amazon Web Services (AWS) account housekeeping

- You need an AWS account – please don't use one of your work accounts
- We provide credits – the credit form has info on how to enter it
- Please use an AWS Identity and Access Management (IAM) user, not the root user
- The facilitators will be walking around to help set up AWS accounts, enter credits, etc.



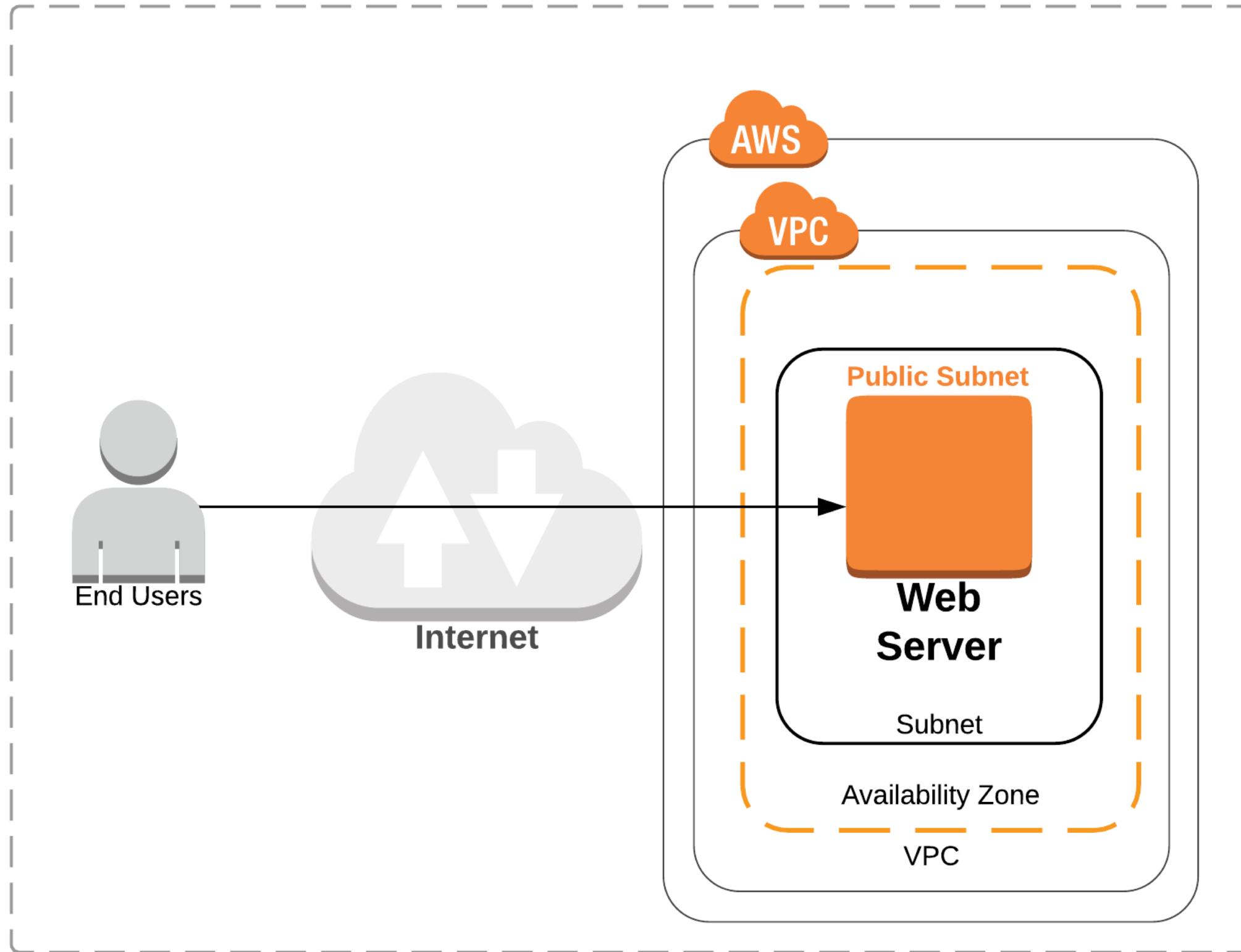
# Verizon 2018 Data Breach Investigations Report

## Data Breach Patterns



Source: 2018 Data Breach Investigation Report, Verizon, 11<sup>th</sup> edition 2018

# Workshop scenario

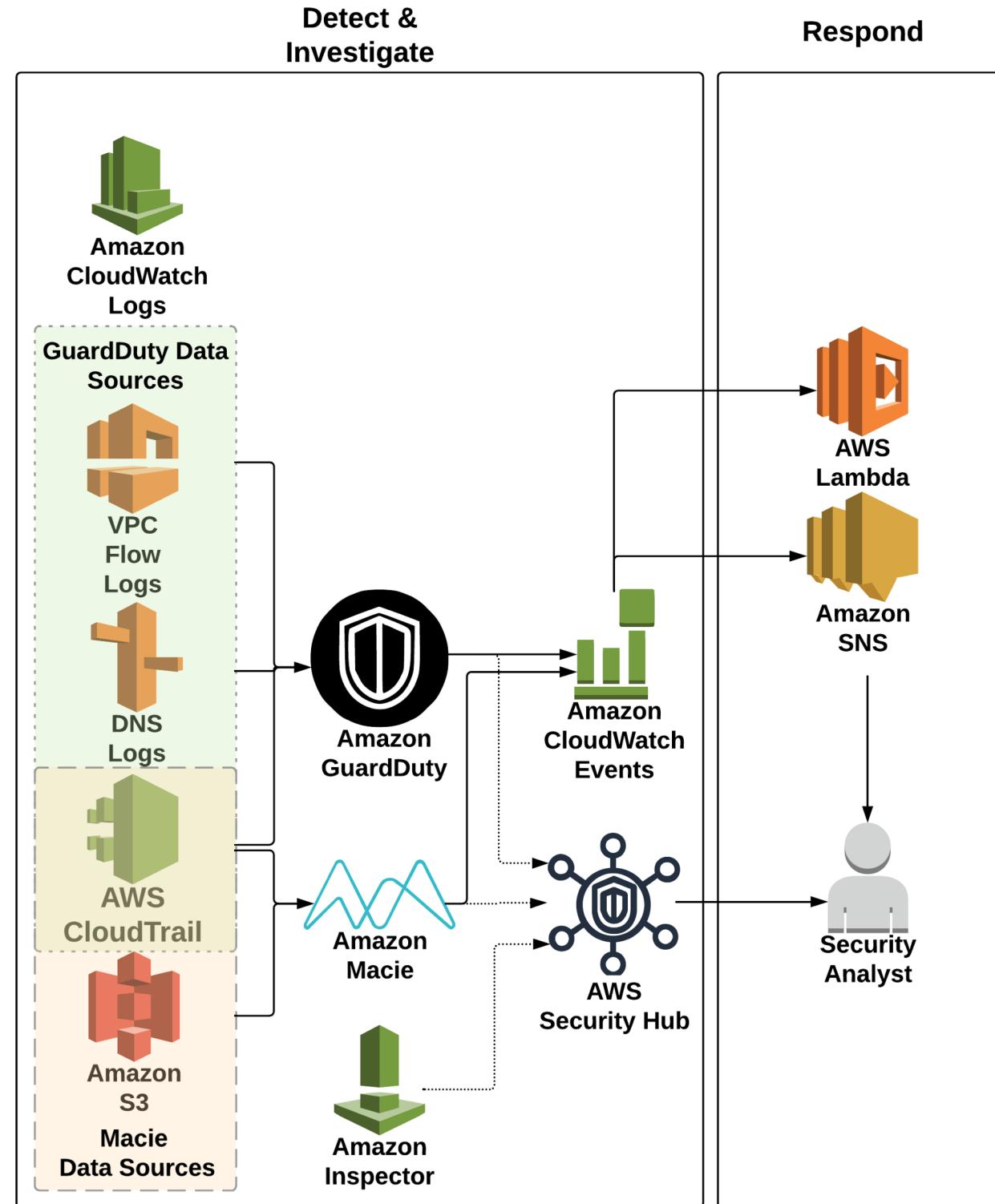


# Module 1

# Module 1 Agenda

- Run the AWS CloudFormation template (~5 min.)
- Manual setup steps (~15 min.)

# Module 1 setup



# Start module 1

Use: US West (Oregon)  
us-west-2

<https://tinyurl.com/y6v2c5x3>

(<https://awssecworkshops.com/level-300/threat-detection-remediation/>)

## Directions:

Browse to <https://tinyurl.com/y6v2c5x3>

- Read through the workshop scenario
- Click on **Module 1: Environment Build** in the outline on the left
- Complete the module (~15 min.) and then stop

# Module 2

# Module 2 Agenda

- Run the CloudFormation template (~5 min.)
- Threat detection and response presentation (~30 min.)
- Workshop walk-through (~5 min.)

# Start module 2

Use: US West (Oregon)  
us-west-2

<https://tinyurl.com/y6v2c5x3>

(<https://awssecworkshops.com/level-300/threat-detection-remediation/>)

## Directions:

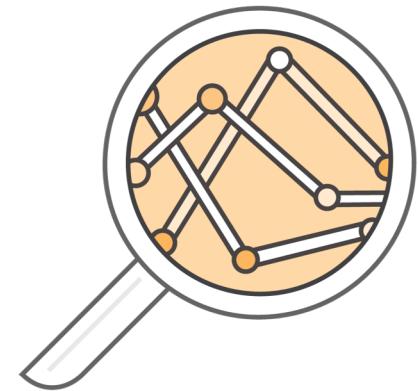
Browse to <https://tinyurl.com/y6v2c5x3>

- Click on **Attack Simulation** in the outline on the left
- Complete the module (~5 min.) then stop (we will do a presentation next)

# Threat Detection & Response

## Intro

# Why is threat detection so hard?



Large datasets

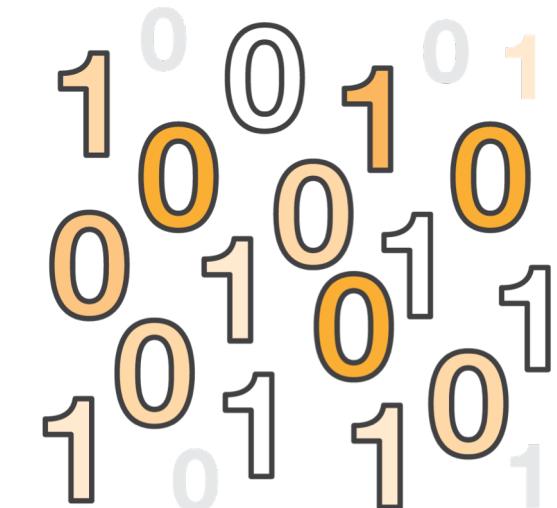
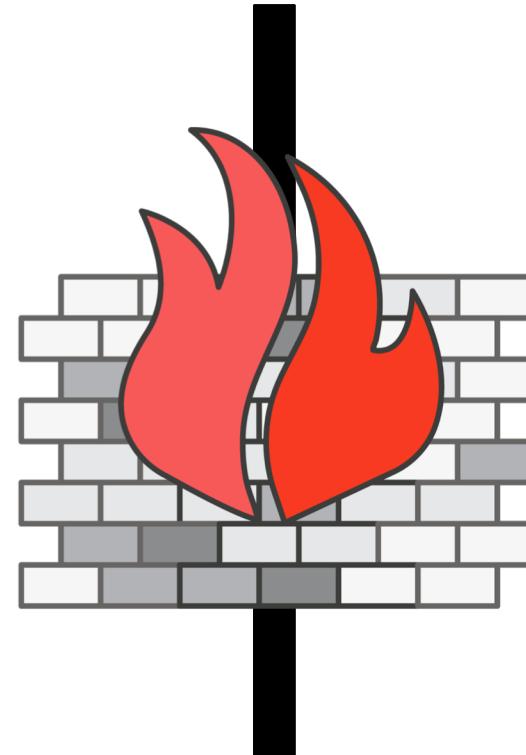
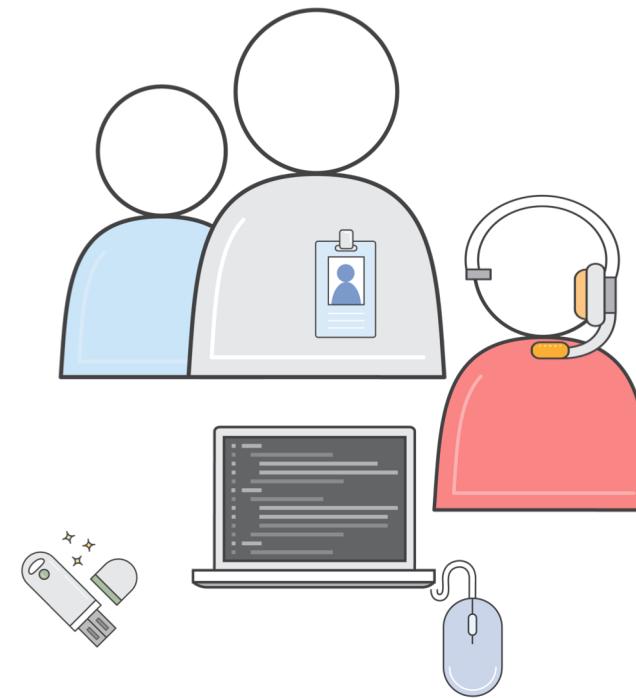


Signal to noise



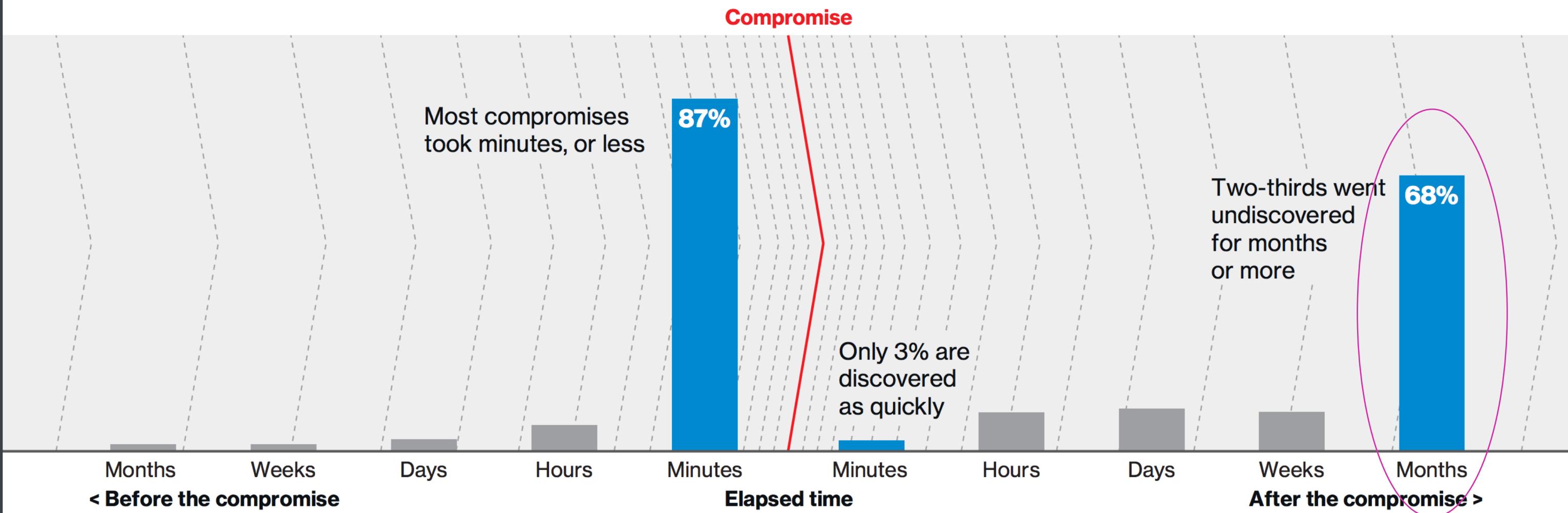
Skills shortage

# Get humans away from the data



**AWS CISO Stephen Schmidt, at re:Invent 2017:** “It's people who make mistakes, it's people who have good intentions but get phished, it's people who use the same credentials in multiple locations and don't use a hardware token for a multi-factor authentication... Get the humans away from the data.”

# Detecting breaches



Source: 2018 Data Breach Investigation Report, Verizon, 11<sup>th</sup> edition 2018

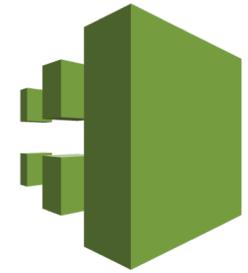
# AWS Security Solutions

<https://www.nist.gov/cyberframework>

Identify	Protect	Detect	Respond	Recover
AWS Systems Manager AWS Config	AWS Systems Manager Amazon Inspector VPC AWS KMS AWS CloudHSM IAM AWS Organizations AWS Cognito AWS Directory Service AWS Single Sign-On AWS Certificate Manager Amazon Inspector	AWS CloudTrail AWS Config Rules Amazon CloudWatch Logs AWS Security Hub Amazon GuardDuty Amazon VPC Flow Logs Amazon Macie AWS Shield AWS WAF	AWS Config Rules AWS Lambda AWS Systems Manager Amazon CloudWatch Events Pro Services AERO	AWS Disaster Recovery and Backup Solutions

# Threat Detection Services

# Threat Detection: Log Data Inputs



## CloudTrail

Track user activity and API usage



## VPC Flow Logs

IP traffic to/from network interfaces in a VPC



## CloudWatch Logs

Monitor apps using log data, store & access log files



## DNS Logs

Log of DNS queries in a VPC when using the VPC DNS resolver

# Threat Detection: Machine Learning



## Amazon GuardDuty

Intelligent threat detection  
and continuous monitoring  
to protect your AWS  
accounts and workloads



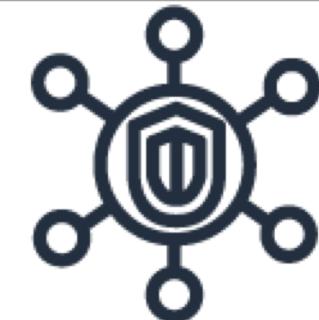
## Amazon Macie

Machine learning-powered  
security service to discover,  
classify & protect sensitive  
data

# Introducing AWS Security Hub – In Preview

## Insights & Standards

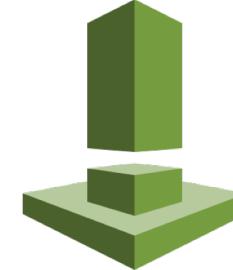
- Comprehensive view of your security and compliance state within AWS
- Aggregates security findings generated by other AWS security services and partners
- Analyze security trends and identify the highest-priority security issues



AWS Security Hub

## Findings

### Security findings providers



Amazon Inspector



Amazon GuardDuty



Amazon Macie



AWS Config



Partner Solutions



Other

# Introducing AWS Security Hub – In Preview



# Live Role-Playing Demo

# Threat Detection: Evocations/Triggers



## AWS Config

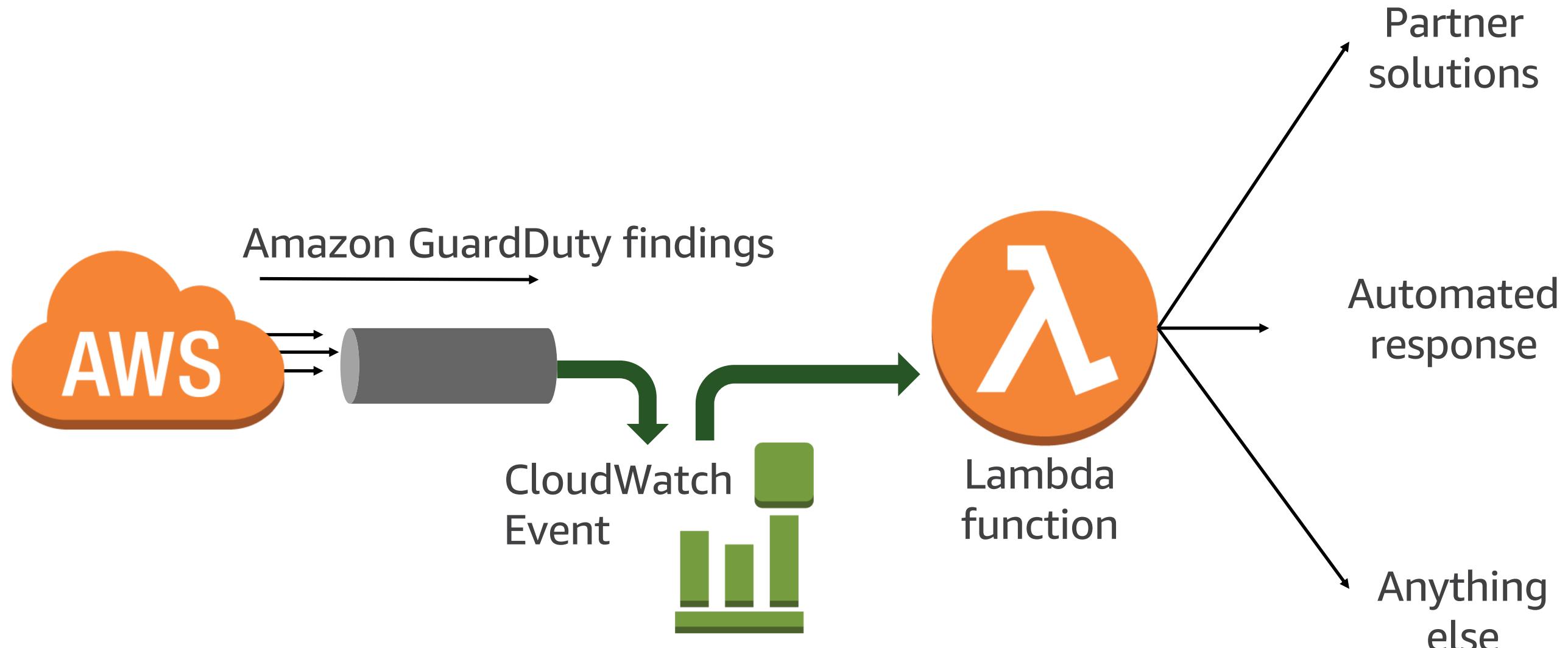
Continuously tracks your resource configuration changes and if they violate any of the conditions in your rules



## Amazon CloudWatch events

Delivers a near real-time stream of system events that describe changes in AWS resources

# Amazon CloudWatch Events



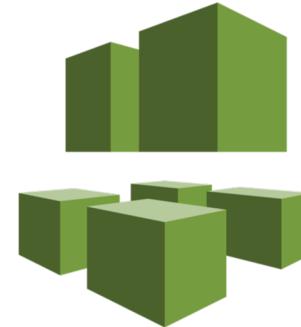
# Respond

# Threat Response



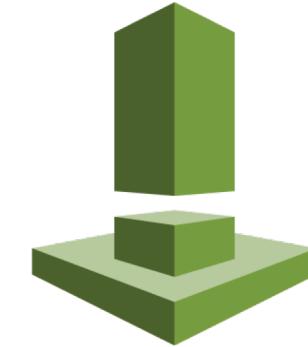
AWS  
Lambda

Run code for virtually  
any kind of  
application or  
backend service –  
zero administration



AWS Systems  
Manager

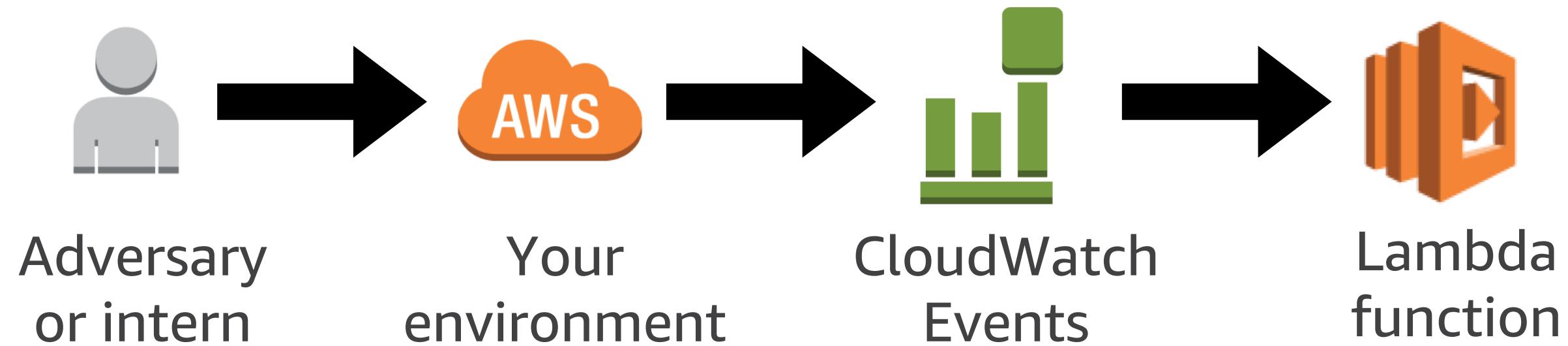
Gain operational  
insights and take  
action on AWS  
resources



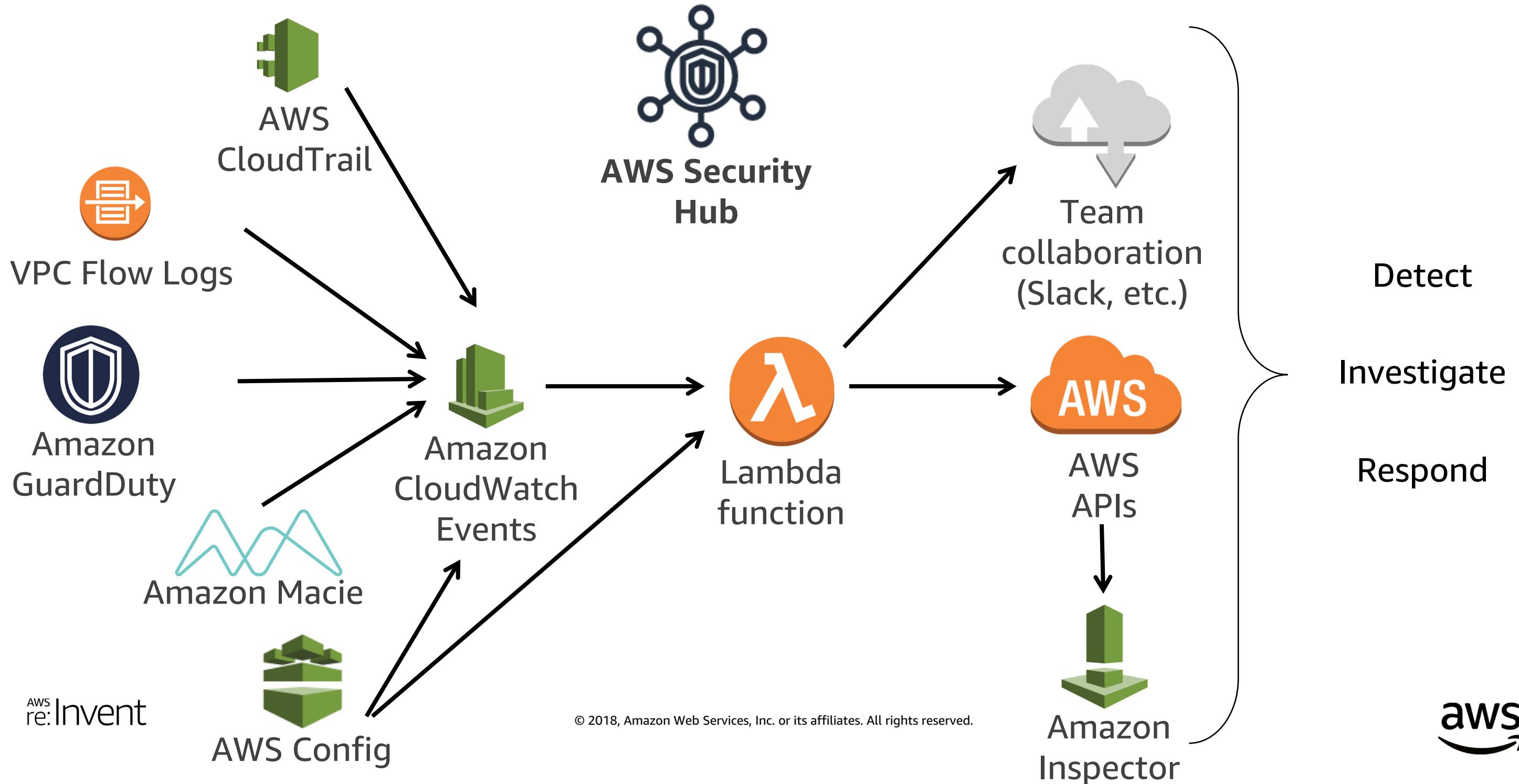
Amazon  
Inspector

Automate security  
assessments of  
Amazon EC2  
instances

# High-Level Playbook



# Detailed Playbook

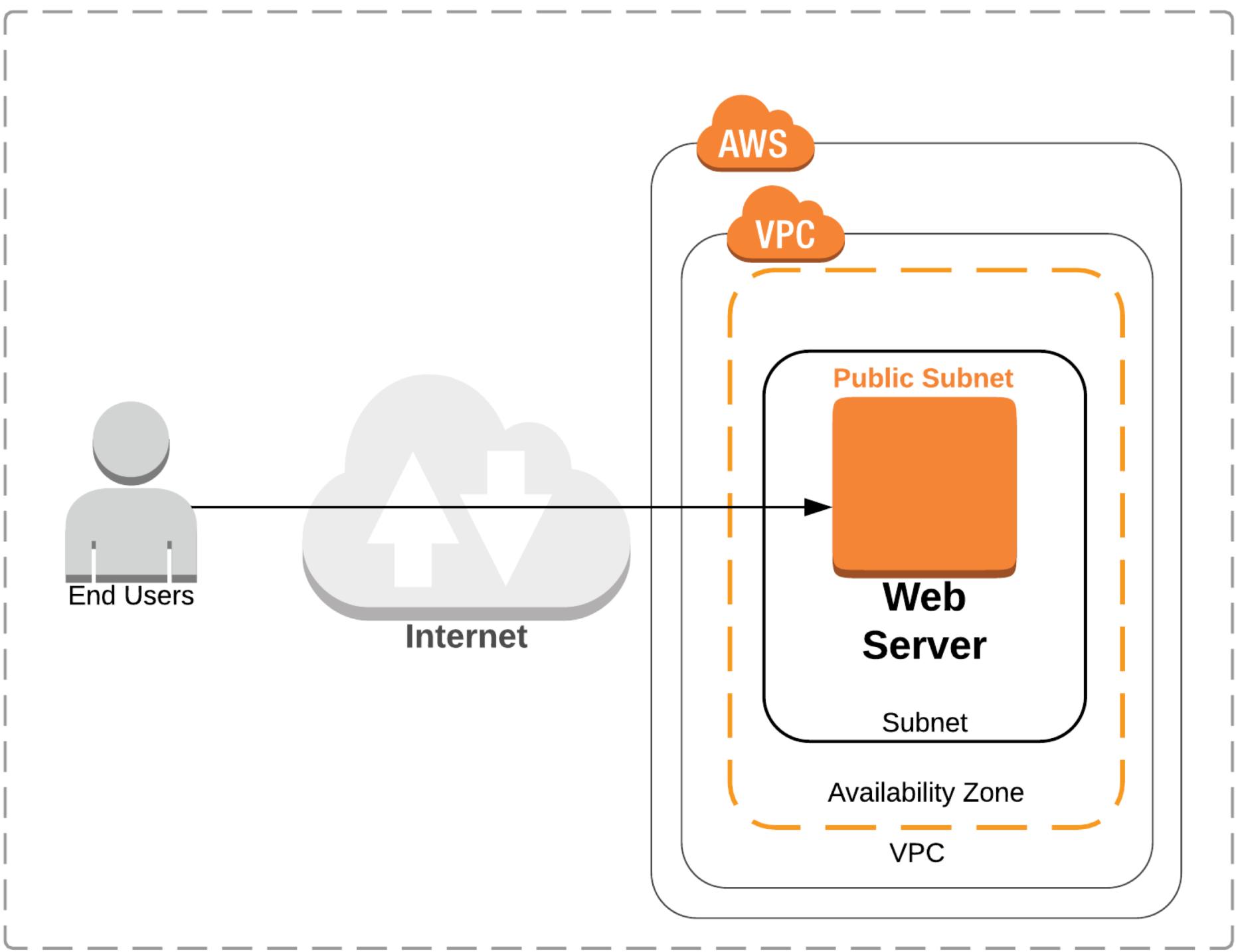


# Review Questions

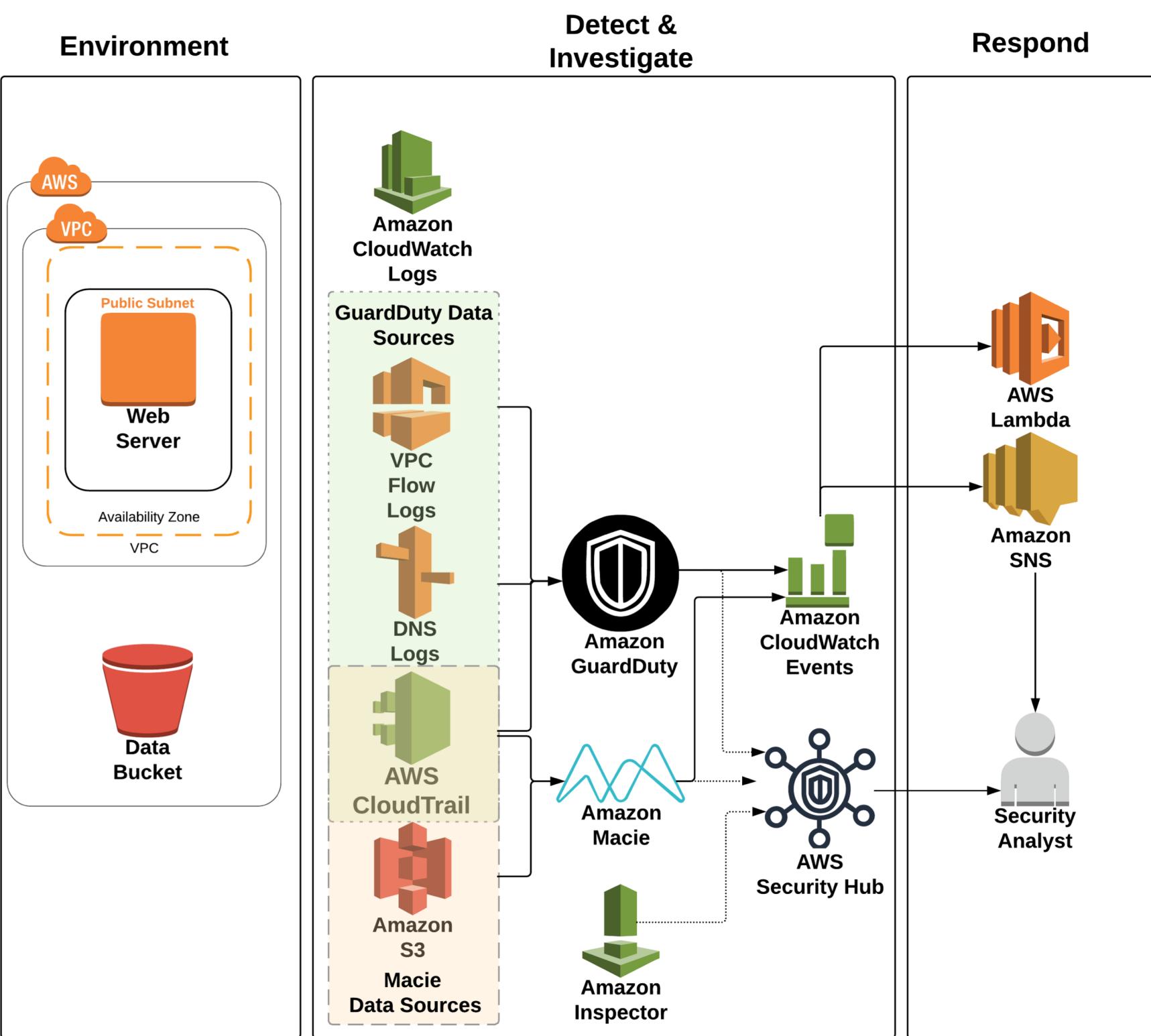
- How do GuardDuty and Macie differ when it comes to CloudTrail analysis?
- What services are important for the automation of responses?
- What performance impact does GuardDuty have on your account if you have more than 100 VPCs?
- Which of the services discussed have direct access to your Amazon EC2 instances?

# Workshop walk-through

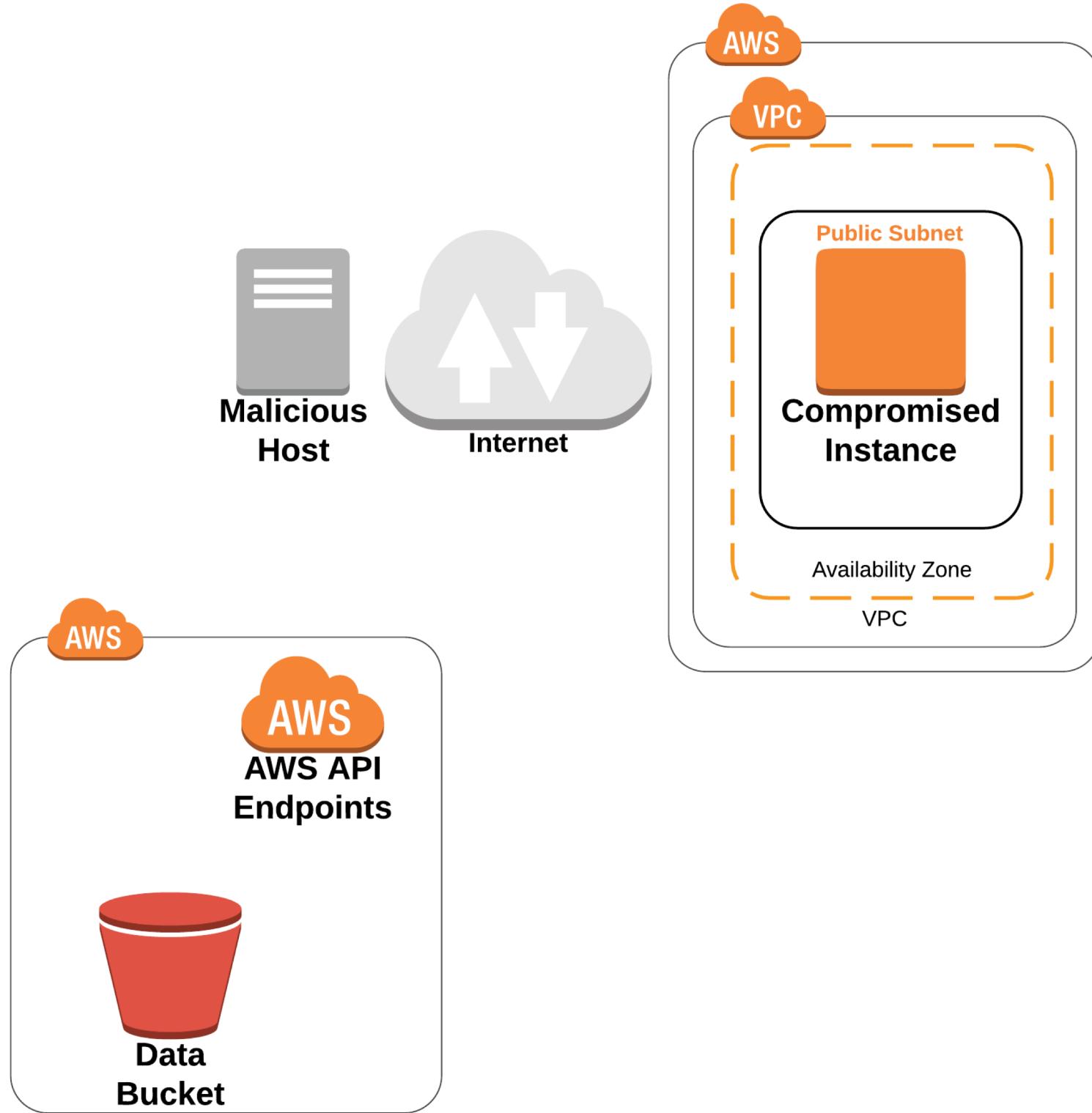
# Attack Target



# Module 2 setup



# The Attack



# Start module 3

Use: US West (Oregon)  
us-west-2

<https://tinyurl.com/y6v2c5x3>

(<https://awssecworkshops.com/level-300/threat-detection-remediation/>)

## Directions:

Browse to <https://tinyurl.com/y6v2c5x3>

- Click on **Detect & Respond** in the outline on the left
- Run through the module (~45 min.)

# Review, Questions & Cleanup

# Module 4 Agenda

- Review (5 min.)
- Questions (10 min.)
- Cleanup

# Start module 4

<https://tinyurl.com/y6v2c5x3>

(<https://awssecworkshops.com/level-300/threat-detection-remediation/>)

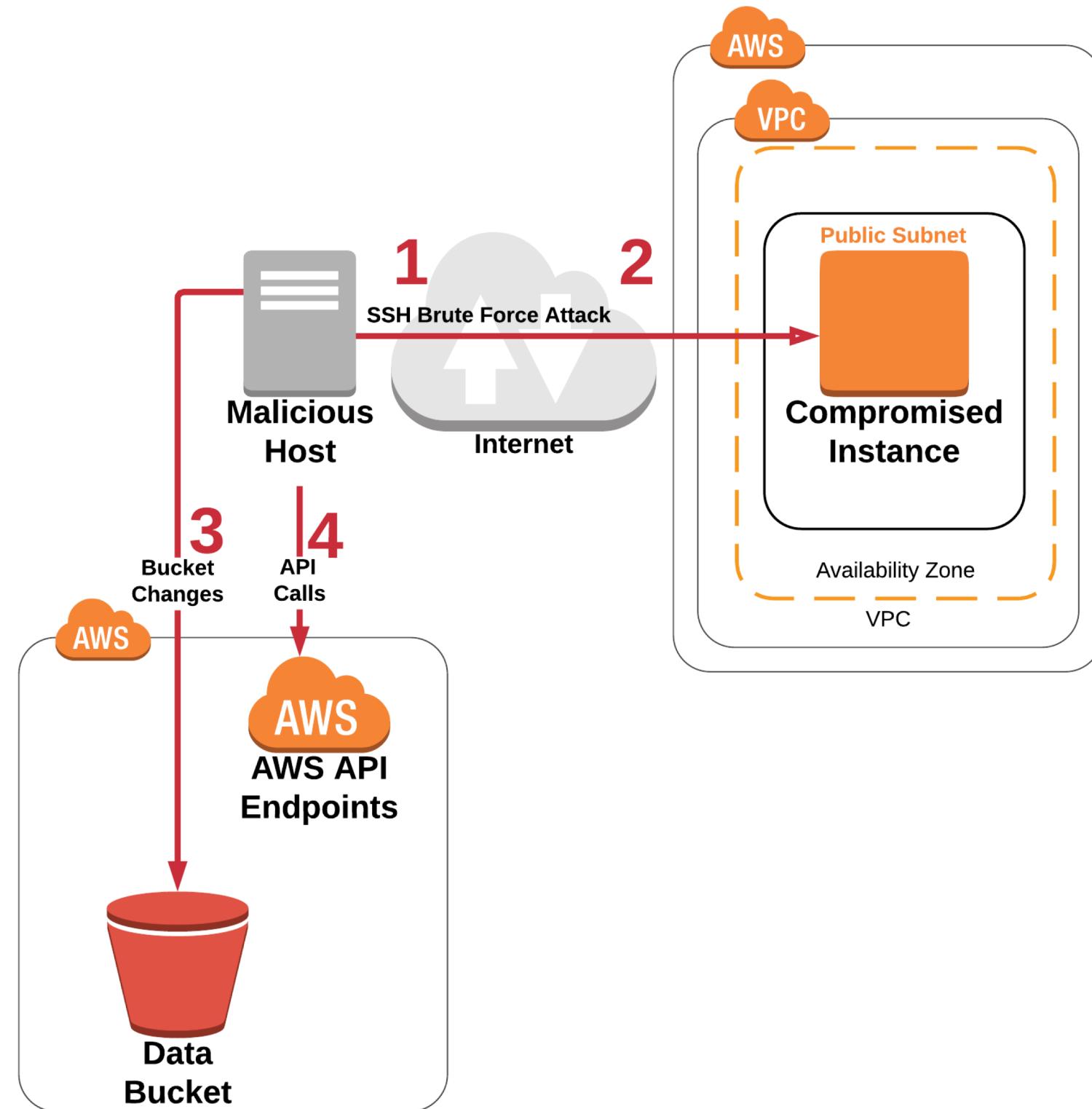
## Directions:

Browse to <https://tinyurl.com/y6v2c5x3> or click on the link at the end of Module 3

- Click on **Discussion** in the outline on the left
- We will do a summary of the workshop then questions
- Account cleanup instructions are toward the end of the page

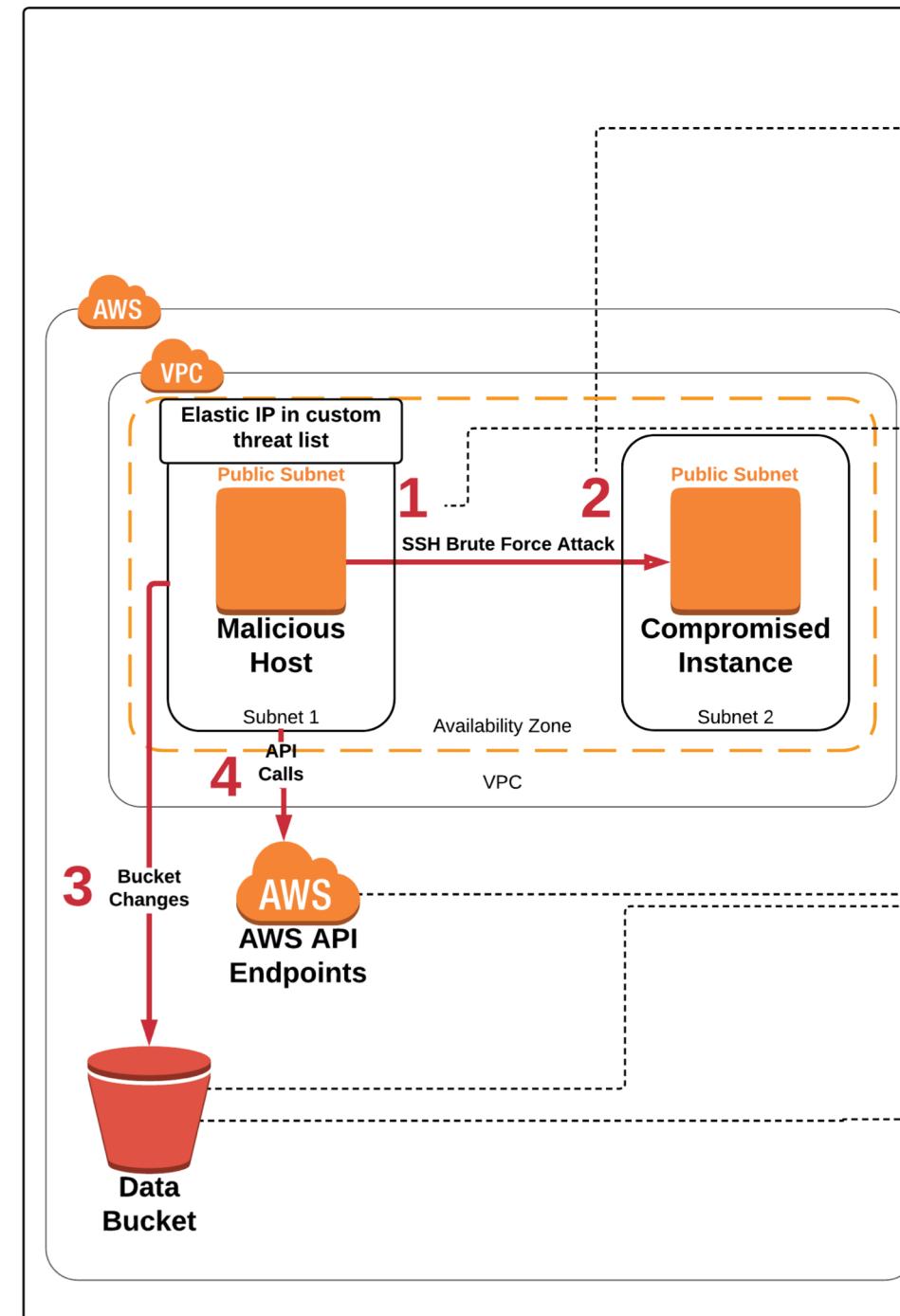
# Scenario discussion

# The Attack

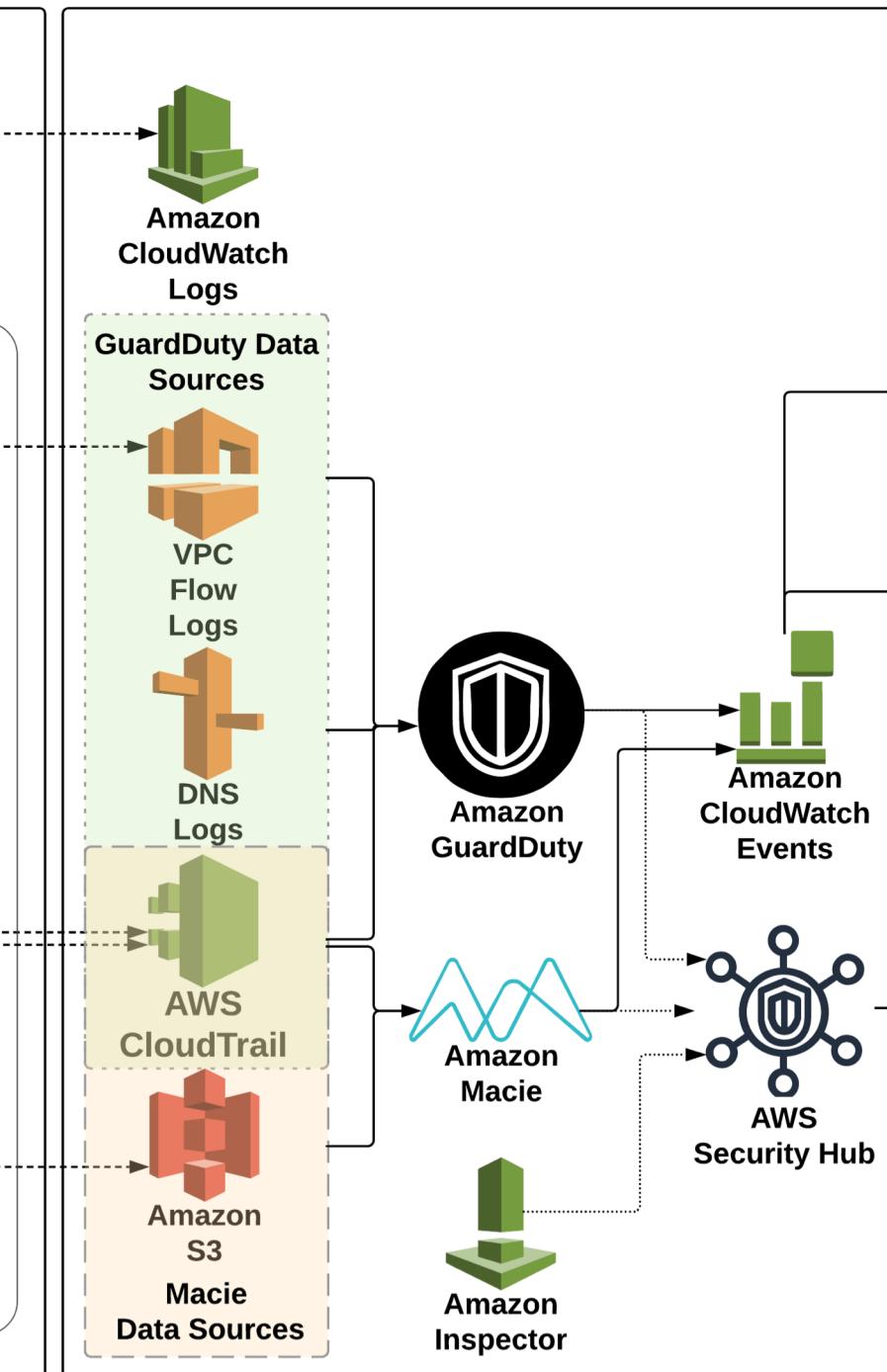


# What really happened?

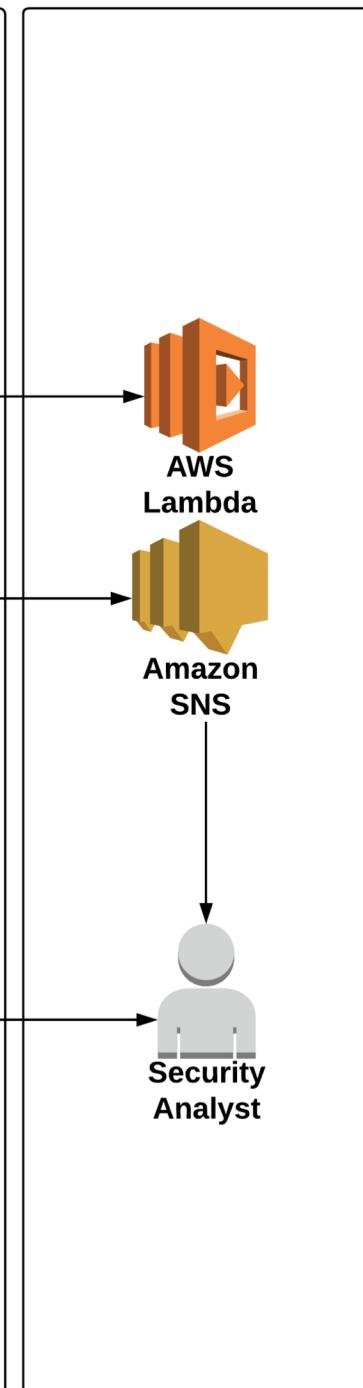
## The Attack



## Detect & Investigate



## Respond



# Questions

# Workshop question – Automation

- For the manual remediations in the workshop, which would be safe to automate?
- What information would you need before you would be willing to automate revoking the IAM temp credentials?
- In general, how do you determine what should be automated vs. what should require manual investigation?

# Workshop questions – Amazon EC2 & GuardDuty

- Why did the API calls from the “malicious host” generate GuardDuty findings?
- The lab mentions you can ignore the high-severity SSH brute force attack finding. Why?
- How does that differ from the low severity SSH brute force finding we investigated? What does this say about the types of threats GuardDuty prioritizes?
- What key remediation step was missed regarding the SSH brute force attack? How would you remediate it?

# Workshop questions – AWS Security Hub

We use AWS Security Hub to investigate the threat. Is AWS Security Hub a detect or response service (or both – or other)?

<https://www.nist.gov/cyberframework>

Identify	Protect	Detect	Respond	Recover
AWS Systems Manager AWS Config	AWS Systems Manager Amazon Inspector VPC AWS KMS AWS CloudHSM IAM	AWS CloudTrail AWS Config Rules Amazon Macie Amazon GuardDuty	AWS Config Rules AWS Lambda AWS Systems Manager Amazon CloudWatch Events Pro Services AERO	AWS Disaster Recovery and Backup Solutions

# Workshop questions – Amazon Simple Storage Service (Amazon S3) & Macie

- Macie had an alert for “S3 Bucket IAM policy grants global read rights.” We investigated that bucket in the workshop. Were the objects in the bucket actually publicly accessible?
- What remediation step did we miss for the data Amazon S3 bucket?

# Workshop question – Amazon S3 & Encryption

- What type of server-side encryption was originally used to encrypt the objects in the data bucket?
- Would Macie be able to classify the objects in the data bucket if they were encrypted using AWS Key Management Service (AWS KMS) server-side encryption?
- If the bucket had a bucket policy that allowed global read access, would the encrypted objects be accessible?

# Cleanup

# Useful links

- <https://aws.amazon.com/security/>
- [https://www.verizonenterprise.com/resources/reports/rp\\_DBIR\\_2018\\_Report\\_en\\_xg.pdf](https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf)
- <https://www.nist.gov/cyberframework>
- [https://d0.awsstatic.com/whitepapers/AWS\\_CAF\\_Security\\_Perspective.pdf](https://d0.awsstatic.com/whitepapers/AWS_CAF_Security_Perspective.pdf)

# Thank you!

Greg McConnel  
[gmcconne@amazon.com](mailto:gmcconne@amazon.com)



Please complete the session  
survey in the mobile app.