SDD312

Finding all the threats: AWS threat detection and remediation

Ross Warren
Security Specialist, AWS WWCS
Geo Solution Architect

aws SUMMIT

Workshop agenda

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

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

Please follow directions

Amazon Web Services (AWS) Event Engine

- We will be using the AWS Event Engine. Please don’t use one of your own accounts.

https://dashboard.eventengine.run

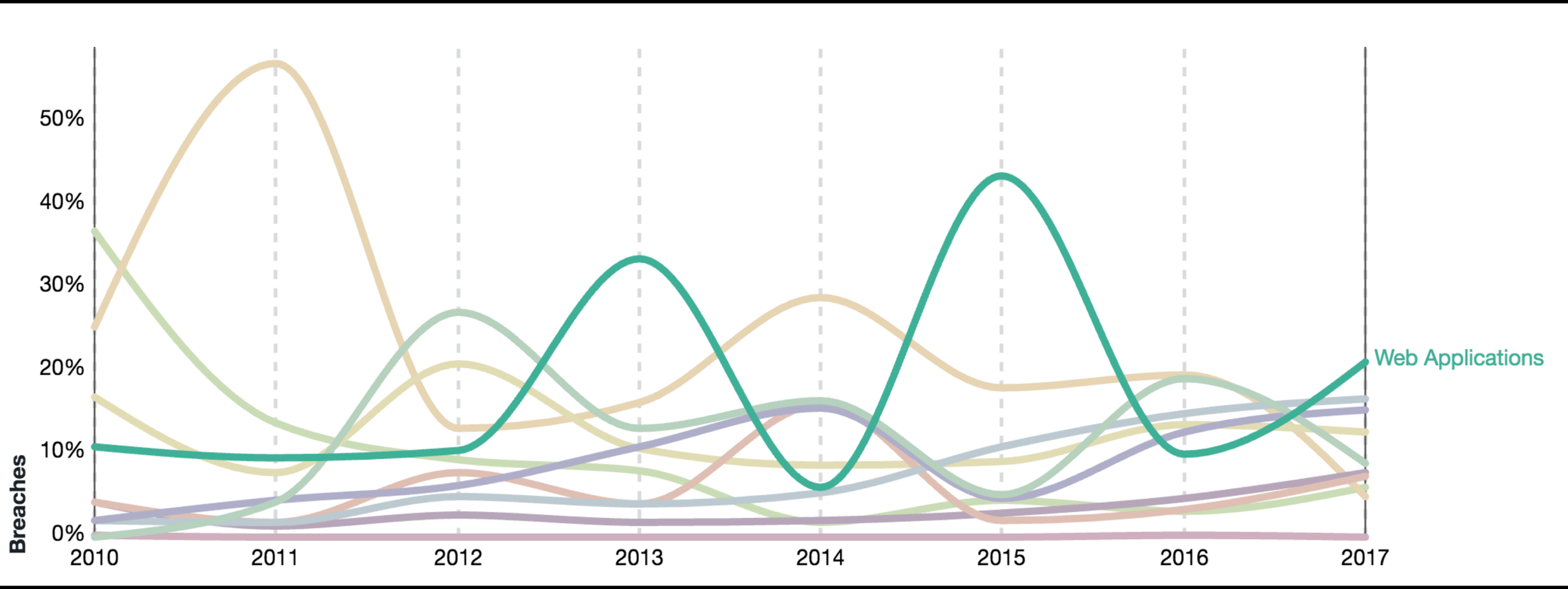
You will enter the hash that was given to you at the above URL

Event Name : Scaling threat detection and response in AWS

- **Click “AWS Console” Button**
- **Click “Open Console” Button**
- **Verify you are in AWS Management Console in the us-west-2 region!**

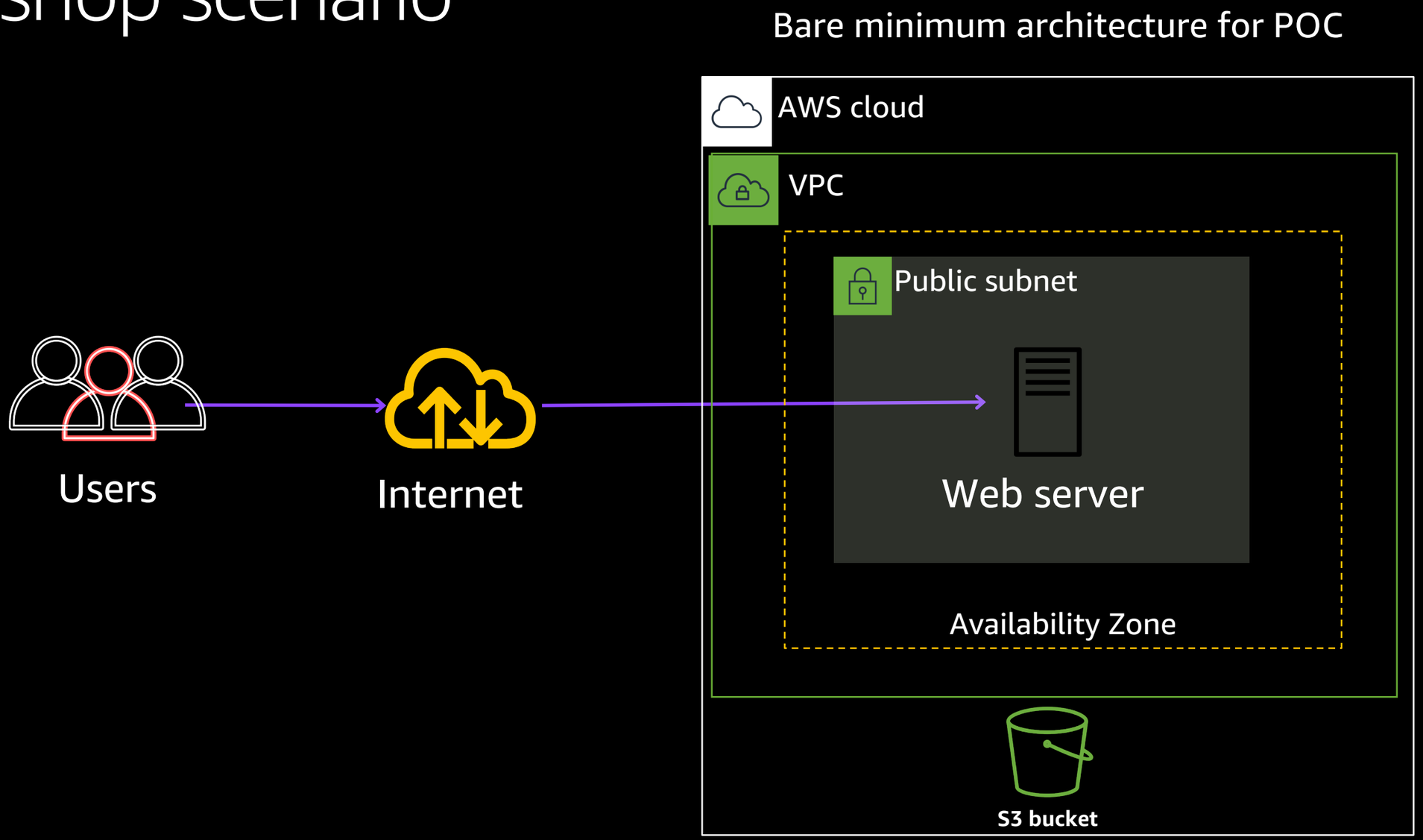
Verizon 2018 Data Breach Investigations Report

Data breach patterns



Source: 2018 Data Breach Investigation Report, Verizon, 11th edition 2018

Workshop scenario



Module 1: Build detective controls

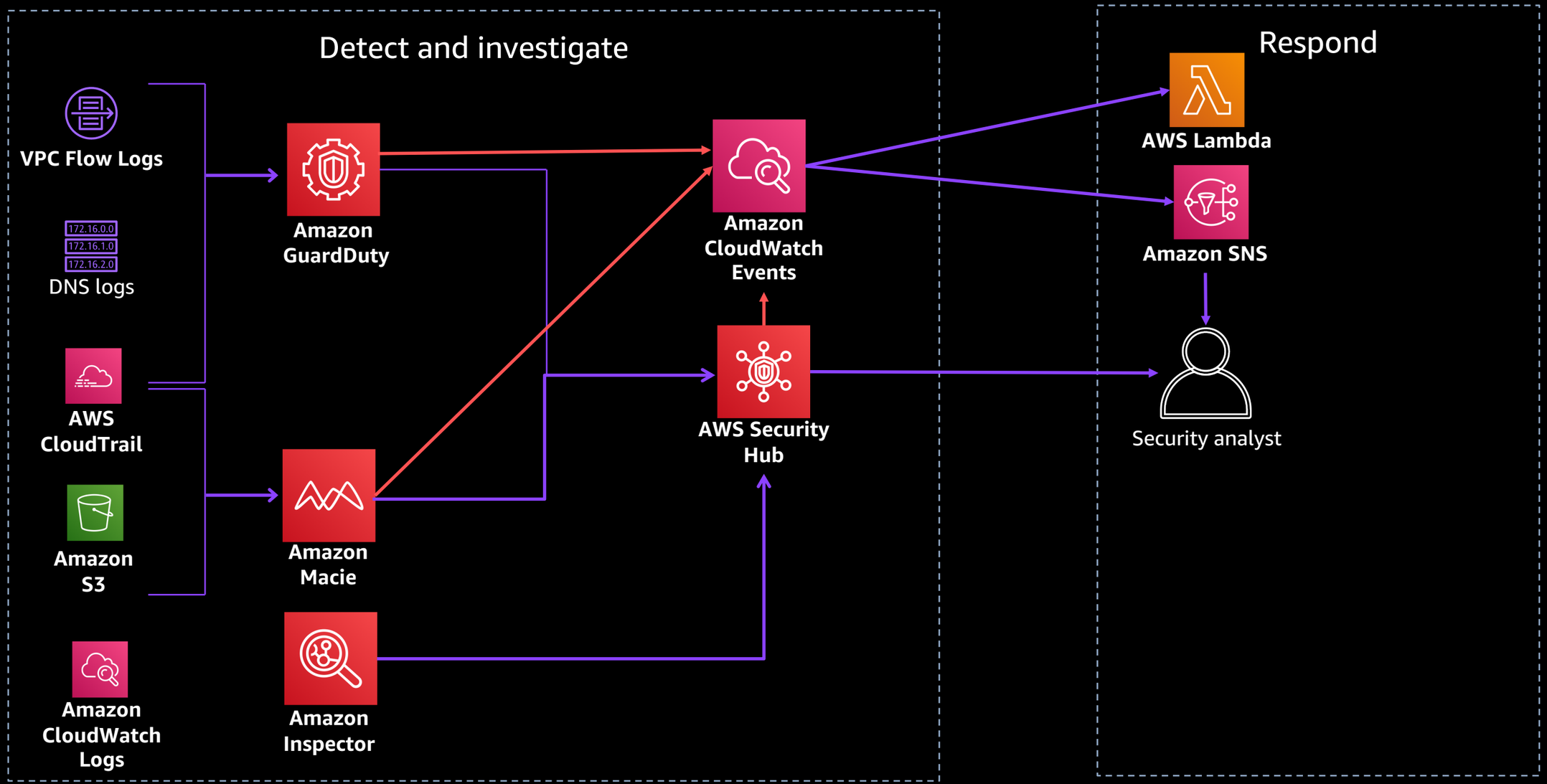
- Run the AWS CloudFormation template (~5 minutes)

  Before moving on, make sure the stack status = CREATE_COMPLETE.

  You will get an email from SNS asking you to confirm the subscription. Confirm the subscription so you can receive email alerts from AWS services during the workshop.

- Manual setup steps (~15 minutes)

Module 1: Build detective controls



aws SUMMIT

Module 1: Build detective controls

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

https://dashboard.eventengine.run

https://tinyurl.com/yyc6tvph

Directions:

1. Browse to URL
2. Read through the workshop scenario
3. Choose **Module 1: Environment Build** in the outline on the left
4. Complete the module (~15 min.) and then stop

PLEASE FOLLOW DIRECTIONS
Do not skip the Manual steps

aws SUMMIT

Module 2: Attack kickoff

- Run the AWS CloudFormation template (~5 min.)

  Do not move on to Module 3

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

Module 2: Attack kickoff

https://dashboard.eventengine.run

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

https://tinyurl.com/yyc6tvph

Directions:

1. Browse to URL
2. Choose **Module 2: Attack Simulation** in the outline on the left
3. Complete the module (~5 min.) and then stop
4. Do not move on to Module 3

Threat detection and response

Introduction

aws SUMMIT

Why is threat detection so hard?

Large datasets

Signal to noise

Skills shortage

Deep set of security tools

Identity

AWS Identity and Access Management (IAM)

AWS Single Sign-On

AWS Directory Service

Amazon Cognito

AWS Organizations

AWS Secrets Manager

AWS Resource Access Manager

Detect

AWS Security Hub

Amazon GuardDuty

AWS Config

AWS CloudTrail

Amazon CloudWatch

VPC Flow Logs

Infrastructure protection

AWS Systems Manager

AWS Shield

AWS WAF (web application firewall)

AWS Firewall Manager

Amazon Inspector

Amazon Virtual Private Cloud (VPC)

Data protection

AWS Key Management Service (KMS)

AWS CloudHSM

AWS Certificate Manager

Amazon Macie

Server-side encryption

Respond

AWS Config Rules

AWS Lambda

AWS Systems Manager

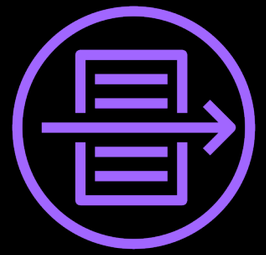
AWS threat detection services

aws SUMMIT

Threat detection: Log data inputs

AWS CloudTrail

Track user activity and API usage



Flow logs

IP traffic to/from network interfaces in a VPC

Amazon CloudWatch

Monitor apps using log data, store, and access log files

DNS logs

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

Threat detection: Machine learning

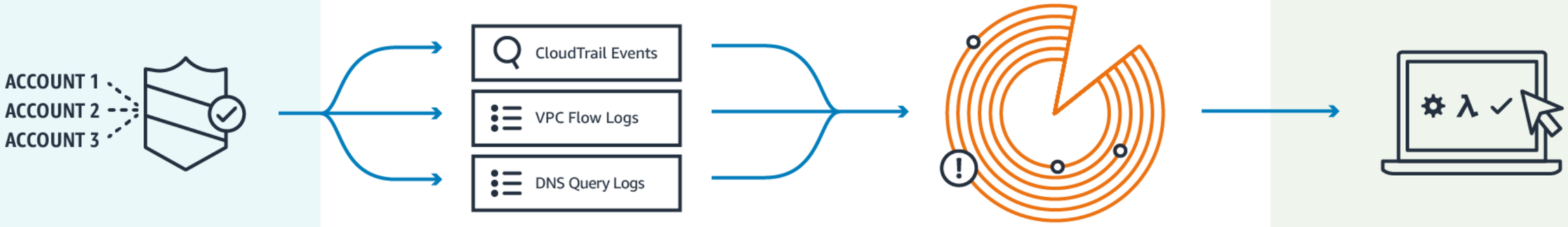
Amazon GuardDuty

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

Amazon Macie

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

Threat detection: Amazon GuardDuty



Enable GuardDuty

With a few clicks in the console, monitor your AWS accounts without additional security software or infrastructure to deploy or manage

Continuously analyze

Automatically analyze network and account activity at scale providing broad, continuous monitoring of your AWS accounts and workloads

Intelligently detect threats

Utilize managed rule-sets, integrated threat intelligence, anomaly detection, and machine learning to intelligently detect malicious or unauthorized behavior

Leverage actionable alerts

Review detailed findings in the console, integrate into event management or workflow systems, or trigger AWS Lambda for automated remediation or prevention

Threat detection: AWS Security Hub

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

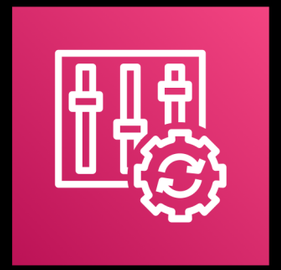
Findings

Security findings providers

Amazon Inspector

Amazon GuardDuty

Amazon Macie

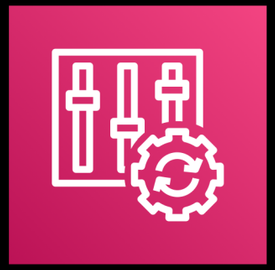


AWS Config

Partner solutions

Other

Threat detection: Evocations/triggers



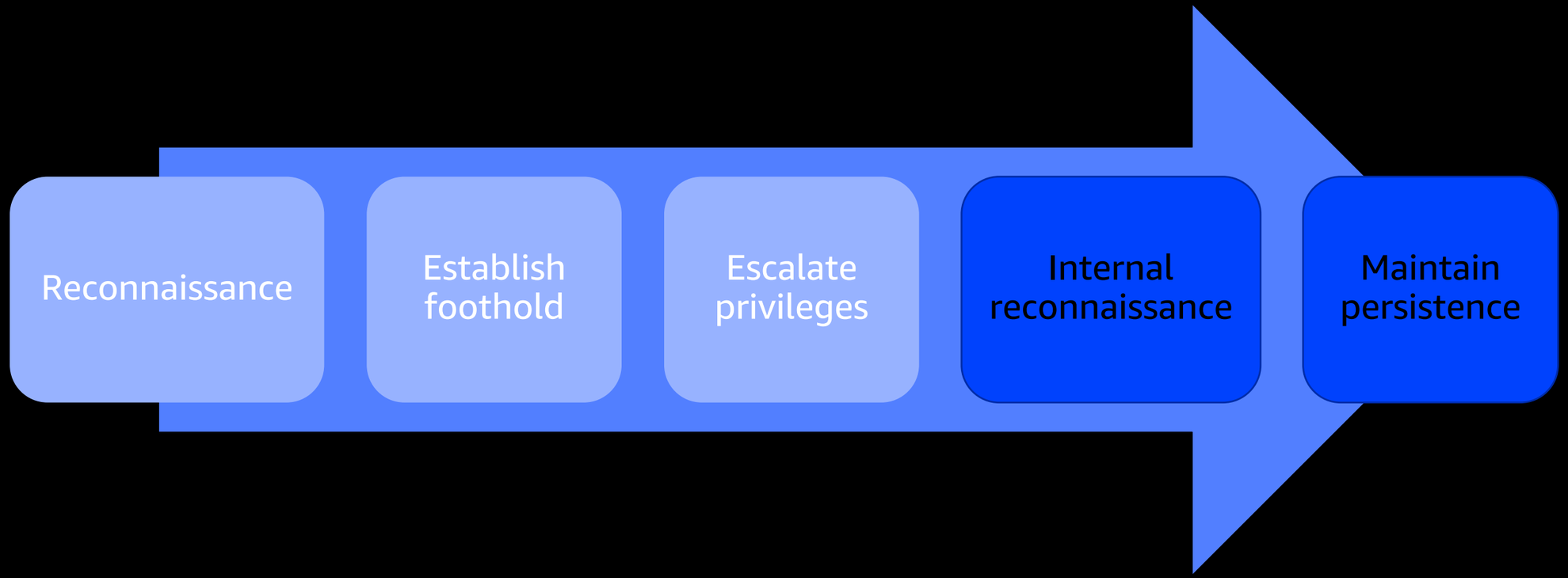
AWS Config

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

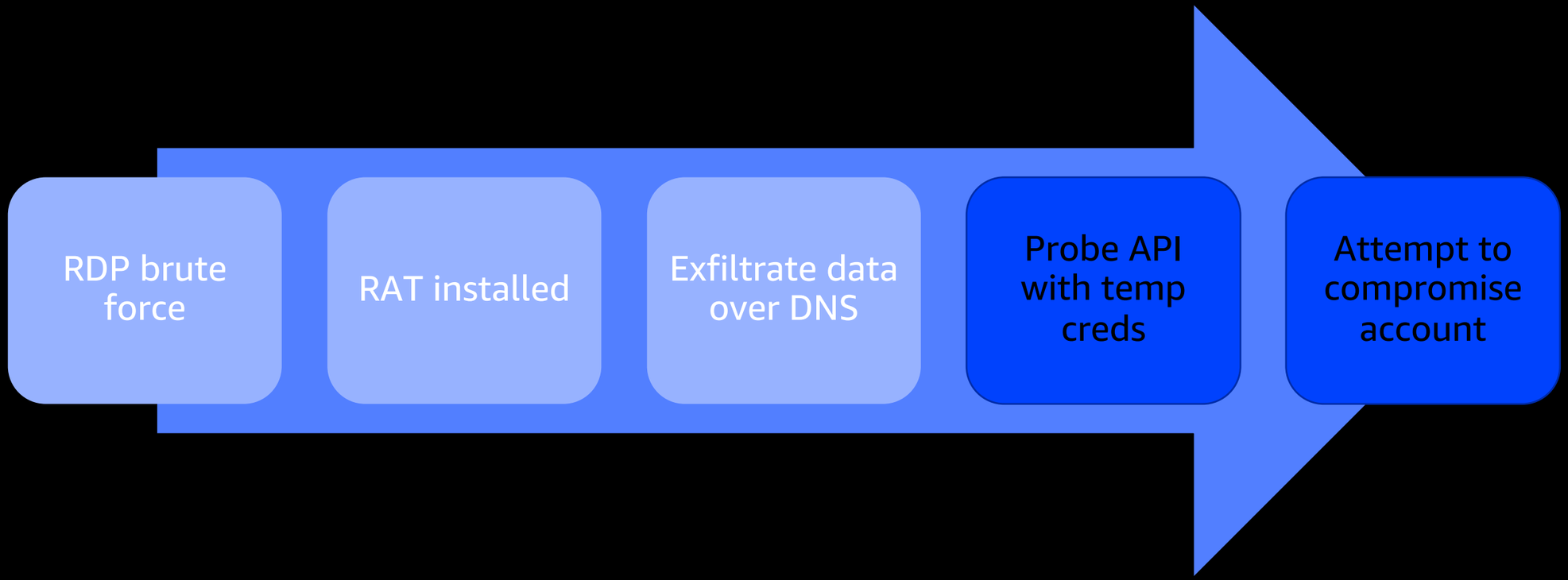
Amazon CloudWatch Events

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

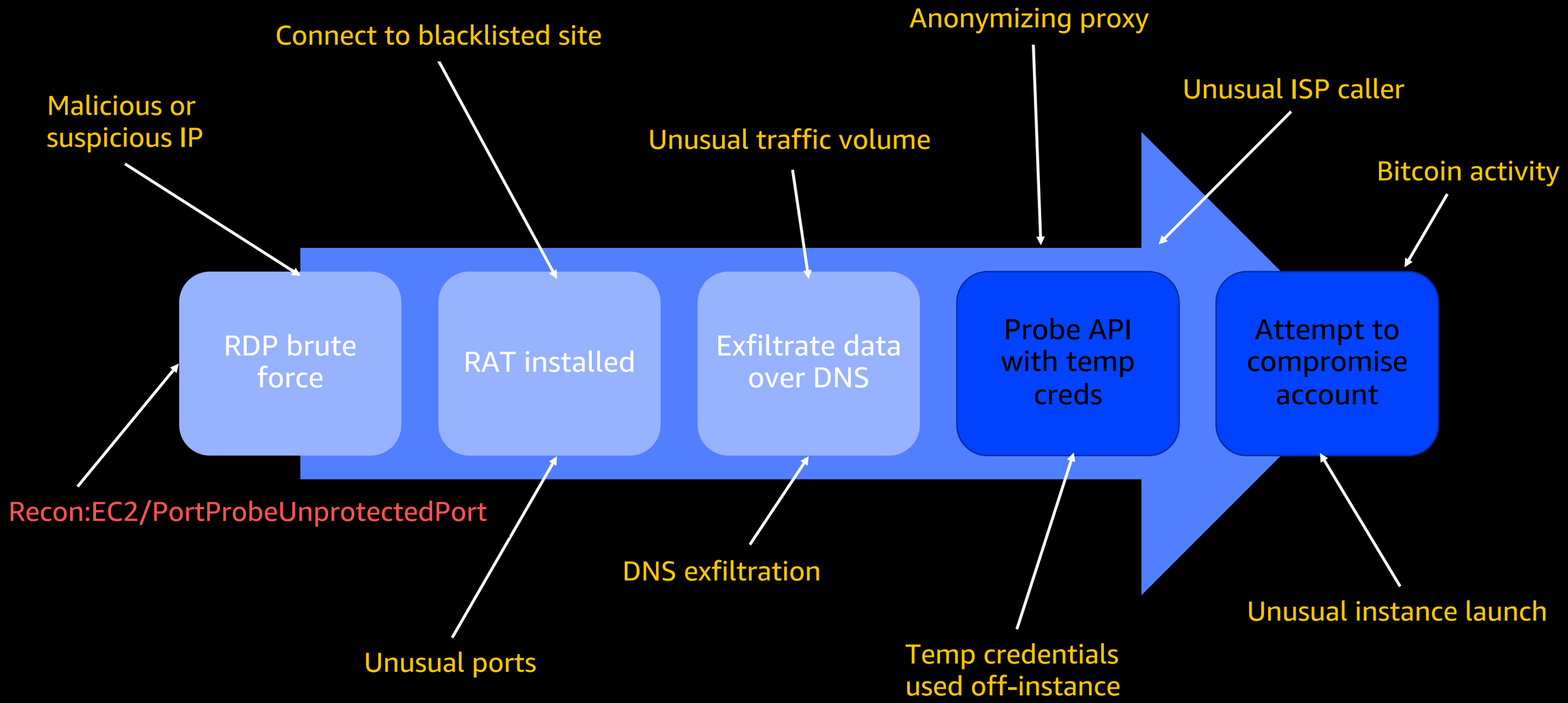
Attacker lifecycle: Stages



Attacker lifecycle: Attacker actions



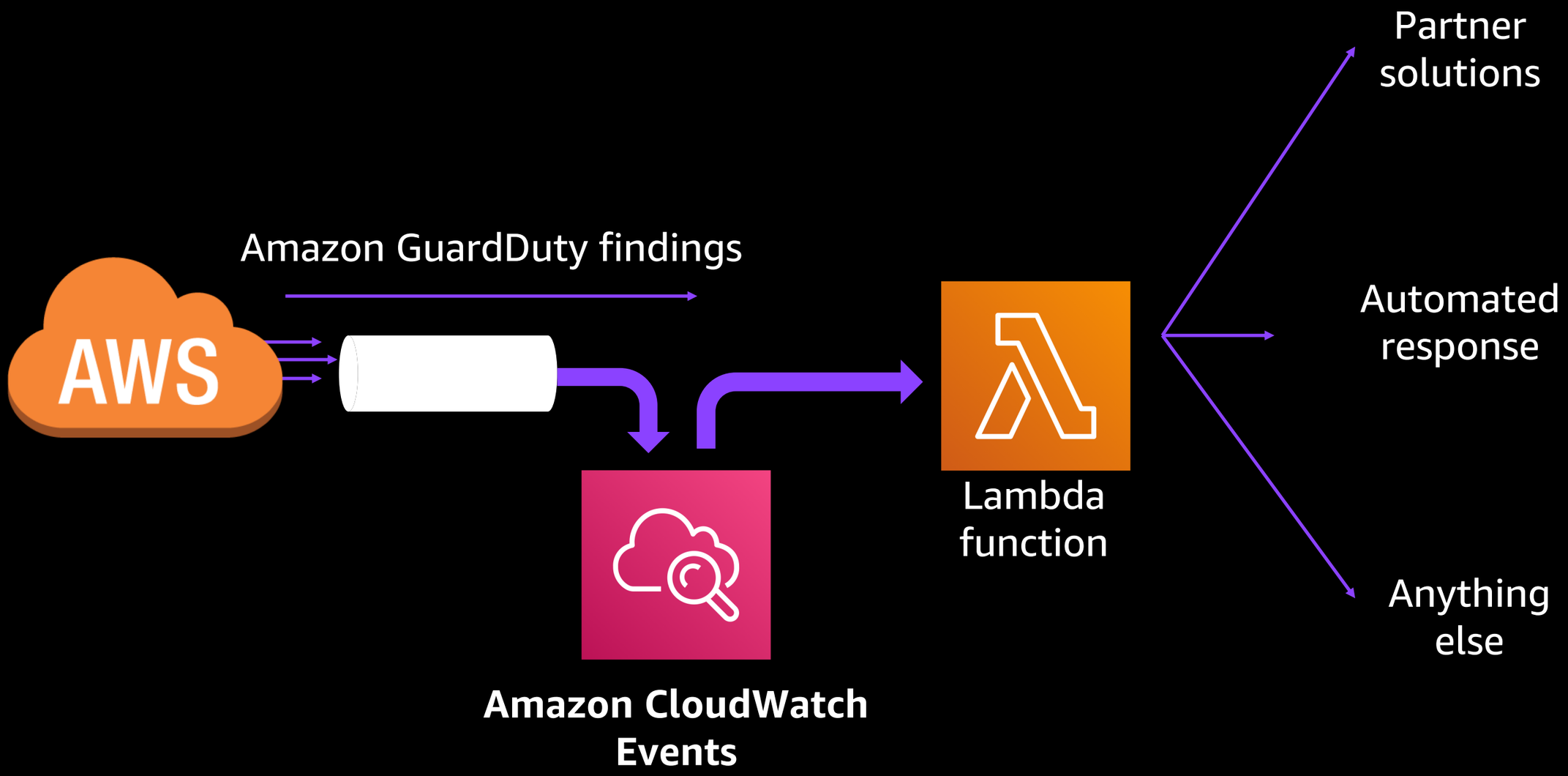
Attacker lifecycle: Amazon GuardDuty findings



Respond

aws SUMMIT

Threat response: Amazon CloudWatch Events



Threat response: Services

AWS Lambda

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

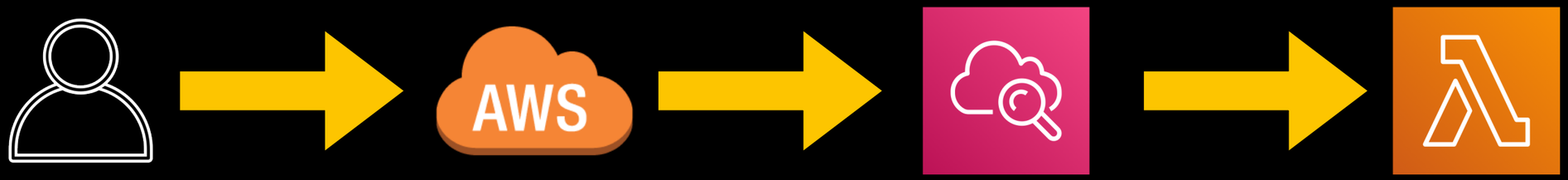
AWS Systems Manager

Gain operational insights and take action on AWS resources

Amazon Inspector

Automate security assessments of Amazon EC2 instances

Threat response: High-level playbook



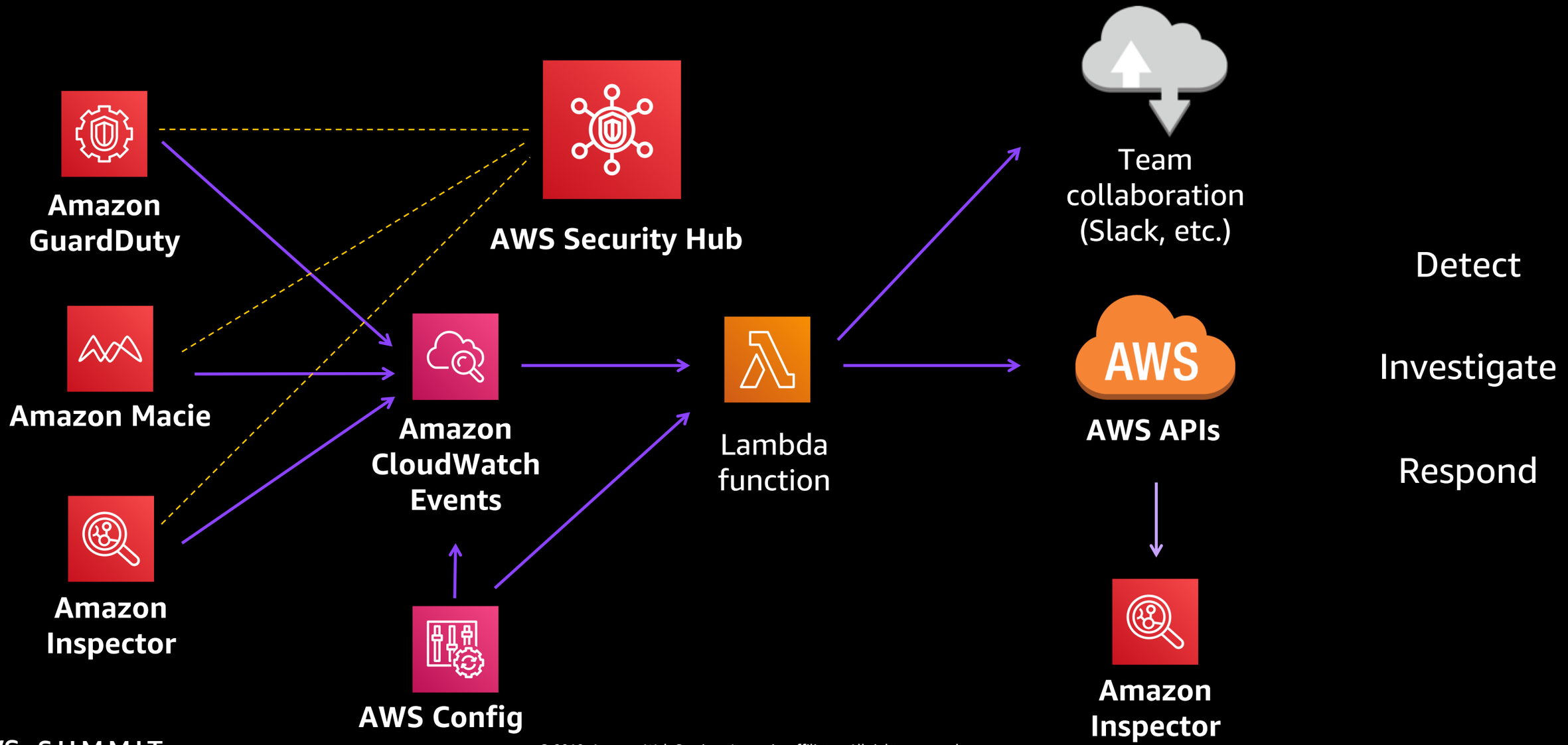
Adversary or intern

Your environment

CloudWatch Events

Lambda function

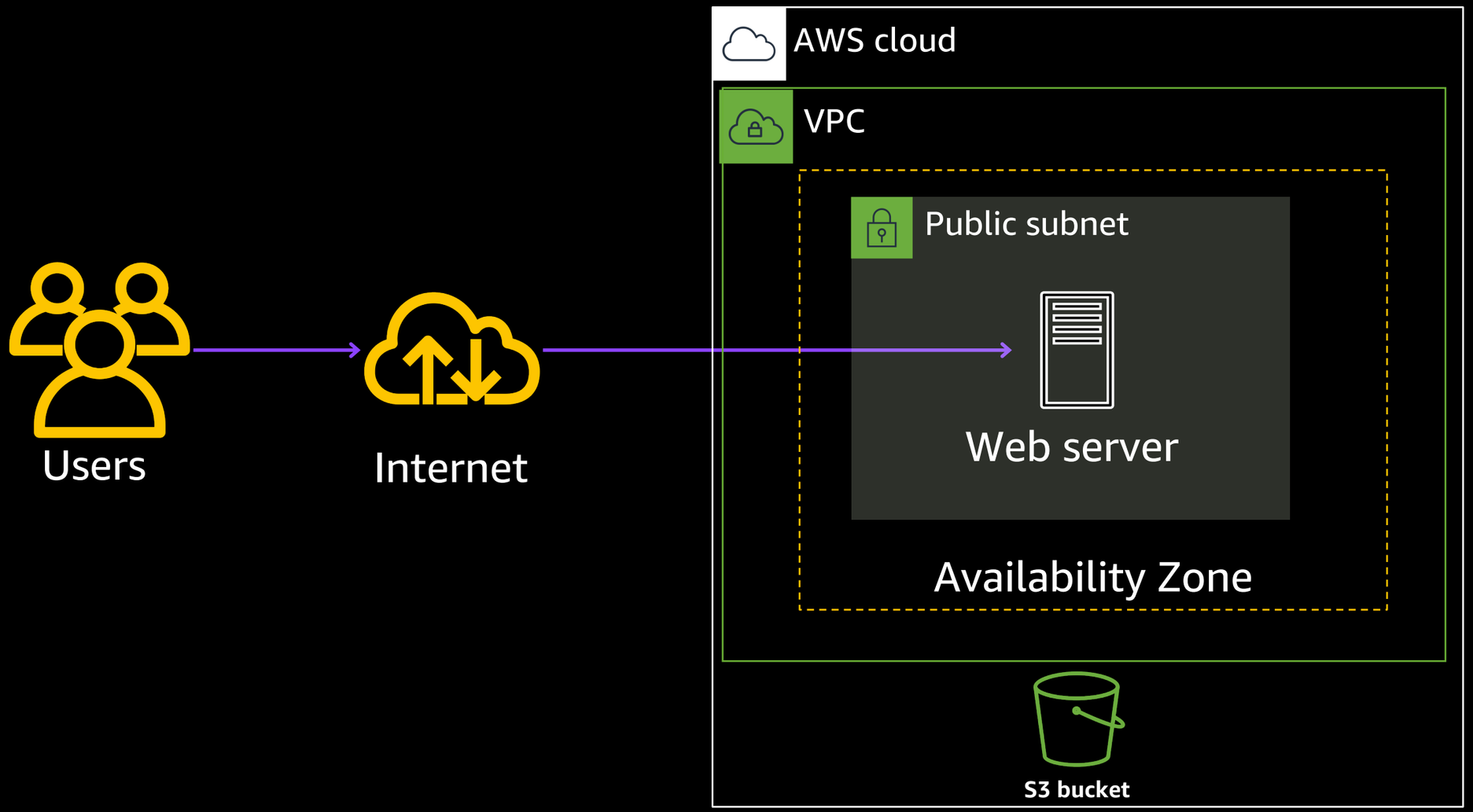
Threat response: Detailed playbook



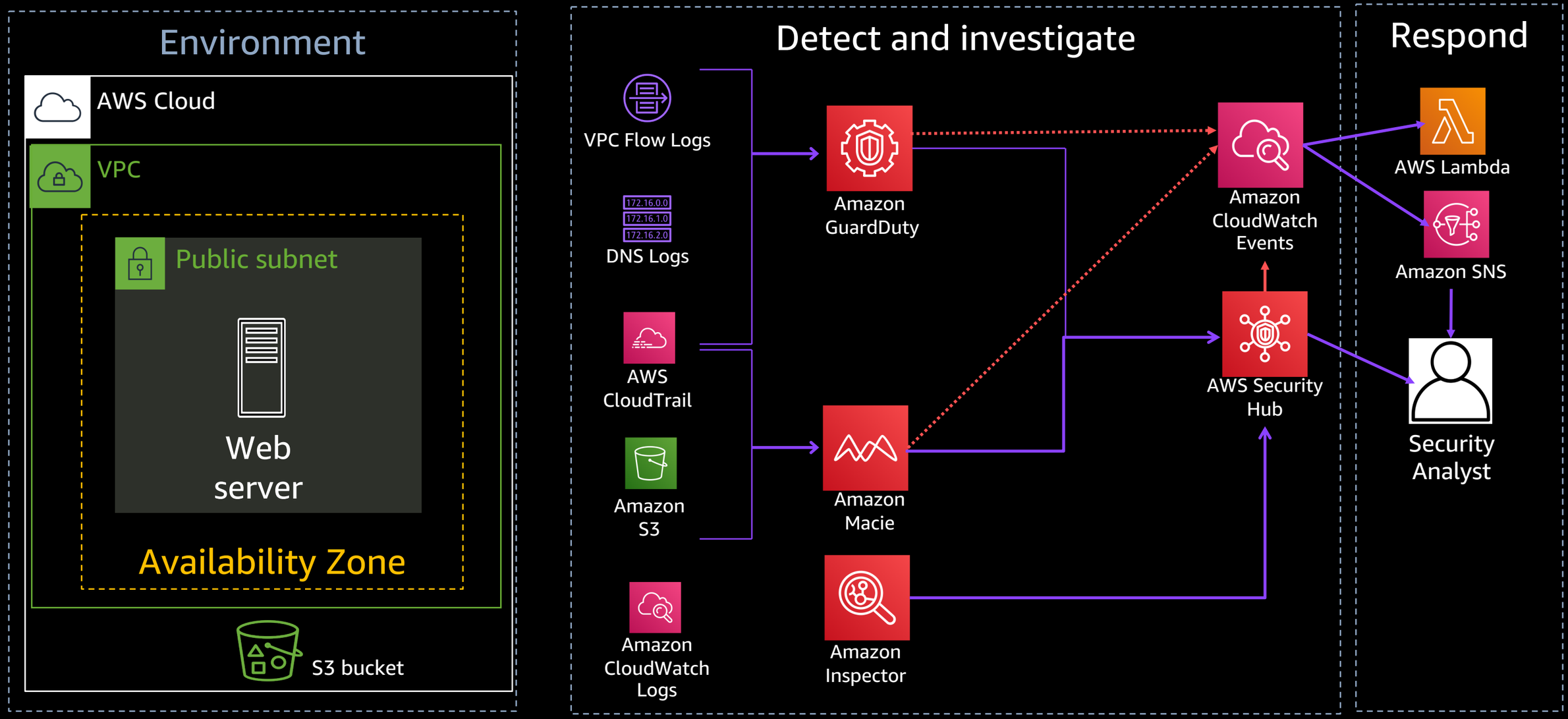
Workshop walk-thru: What happened?

aws SUMMIT

Module 2: Attack target

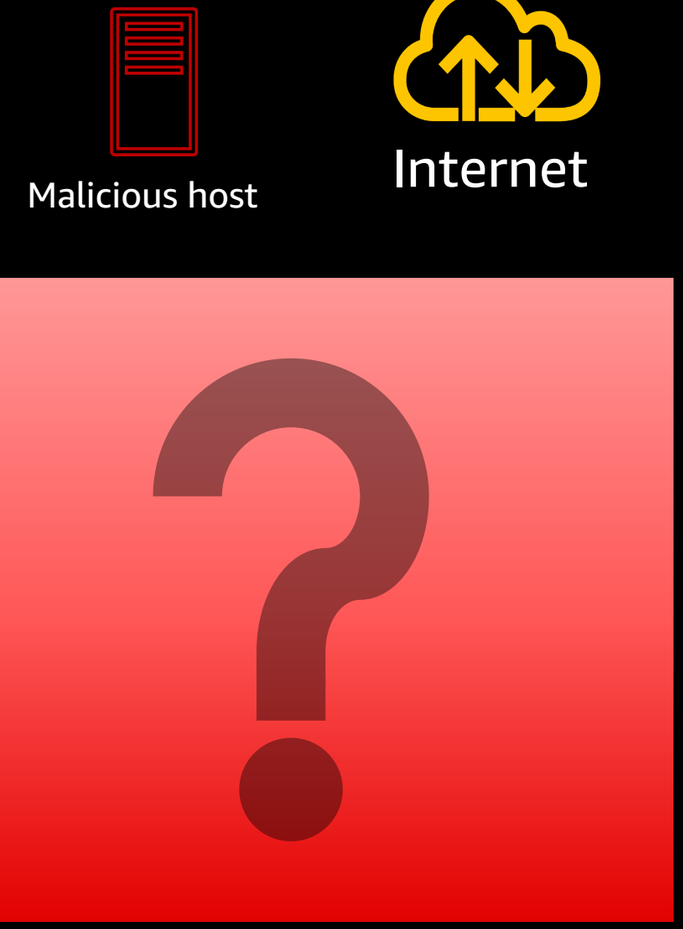


Module 2: Setup



aws SUMMIT

Module 2: The attack



aws SUMMIT

Module 3: Detect & Response

https://dashboard.eventengine.run

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

https://tinyurl.com/yyc6tvph

Directions:

1. Browse to URL
2. Choose **Module 3: Detect & Respond** in the outline on the left
3. Run through the module (~45 min.)

Do not use the `CONTAINS` command

aws SUMMIT

Review, questions, and cleanup

aws SUMMIT

Module 4: What happened?

- Review (5 minutes)
- Questions (10 minutes)
- Cleanup

aws SUMMIT

Module 4: What happened?

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

https://tinyurl.com/yyc6tvph

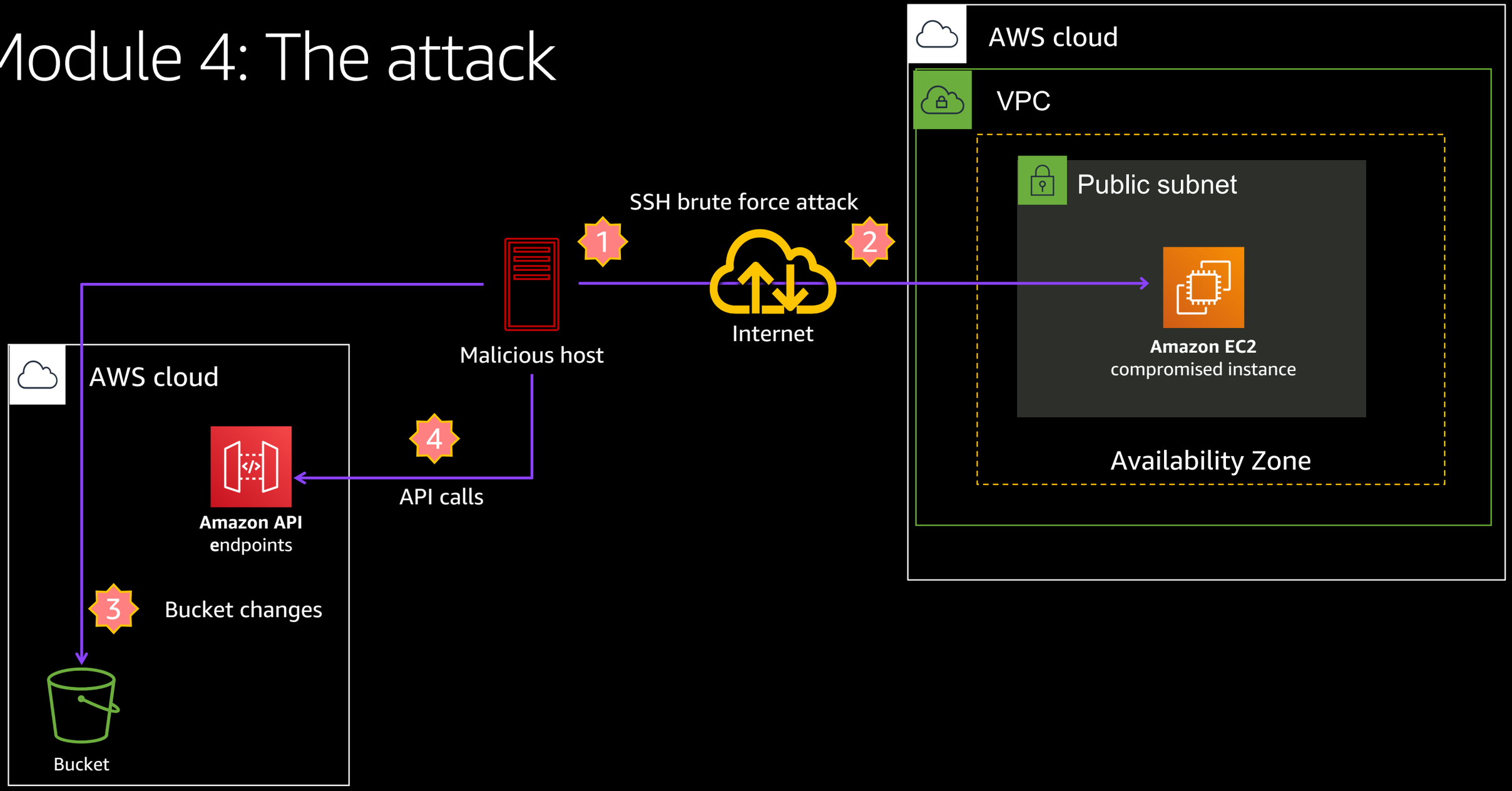
Directions:

1. Browse to URL
2. Choose **Module 4: Discussion** in the outline on the left
3. We will do a summary of the workshop, then questions
4. Do not need to do - Account cleanup instructions

Scenario discussion

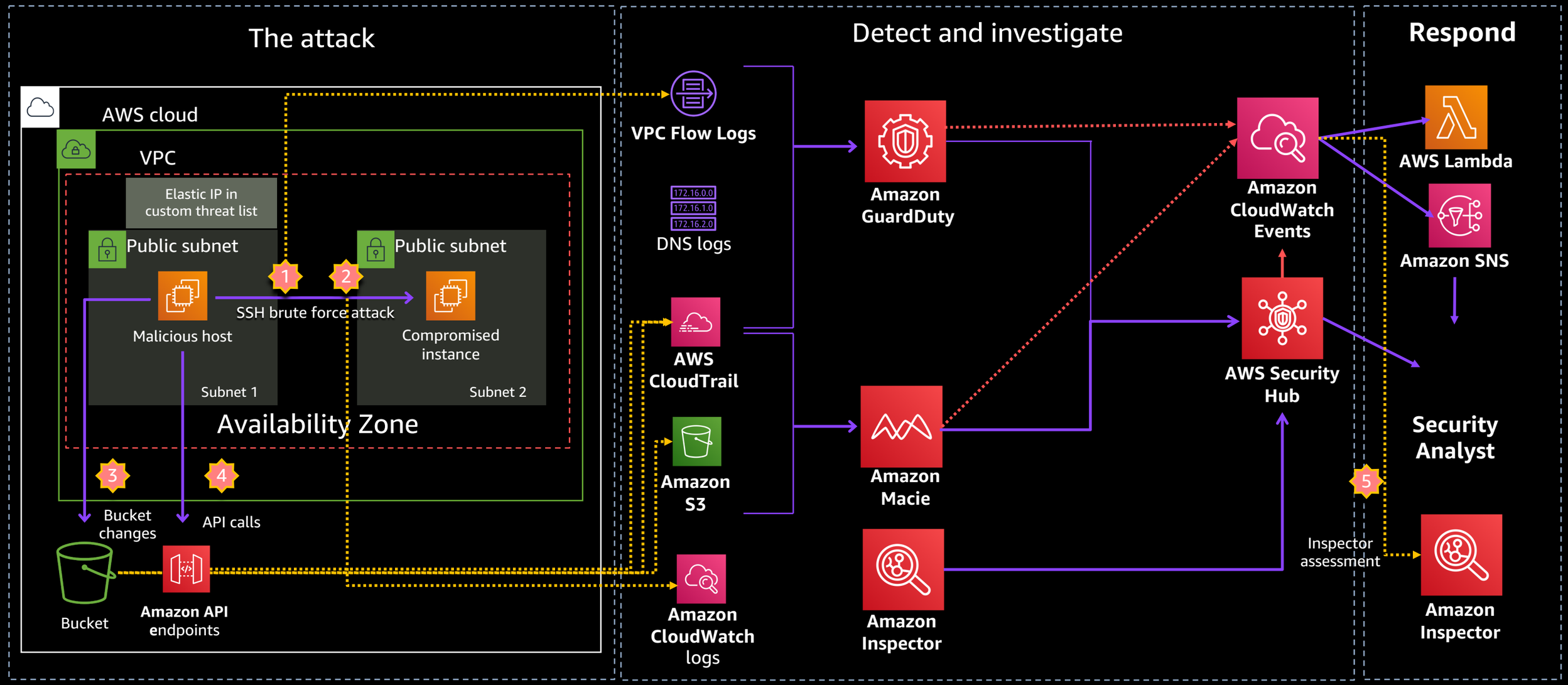
aws SUMMIT

Module 4: The attack



aws SUMMIT

Module 4: What really happened?



Questions

aws SUMMIT

Workshop questions #1

- Which of the following AWS services have direct access to your Amazon EC2 instances?
- What performance impact does GuardDuty have on your account if you have more than 100 VPCs?
- How do you kick off notifications or actions based on events in GuardDuty?
- What is the difference between Macie and GuardDuty?

Workshop questions #2

The lab mentions you can ignore the high-severity SSH brute force attack finding. Why?

Why did the API calls from the “malicious host” generate GuardDuty findings?

What is required for CloudWatch logs to capture evidence to help investigate an SSH Brute force attack?

What key remediation step was missed regarding the SSH brute force attack?

Wrap-up: Lessons learned from incident response

Use a strong tagging strategy!!!

How are my AWS resources classified?

- Ownership?
- Where does this instance come from?
- What is the purpose of this instance?
- Which account is this?
- What to prioritize?

Wrap-up: Lessons learned from incident response

Questions to ask during the investigation

- Who or what is causing this finding?
  - Internal or external?
- How long has this been going on?
  - Is this the first time I've seen it?
- What is the source of the intel?
- What is the risk to my environment?

Wrap-up: Lessons learned from incident response

Enrich GuardDuty and get the full picture of your environment

- Network intrusion detection
- Firewall alerts
- WAF alerts
- Identity (UBA)
- Endpoint and compute events (AV, EDR,)
- OS-level Information
- Application level logs

Centralize GuardDuty findings into a SIEM

Thank you!

Ross Warren
ross@amazon.com

aws SUMMIT

Useful links

https://aws.amazon.com/security/

https://enterprise.verizon.com/resources/reports/dbir/

https://www.nist.gov/cyberframework

https://d0.awsstatic.com/whitepapers/AWS_CAF_Security_Perspective.pdf

https://aws.amazon.com/security/penetration-testing/

SUMMIT

CITY NAME