Threat Detection and Remediation Workshop

Module 2

Agenda

- Module 2: run the CloudFormation template (~5 min)
- Threat detection and remediation intro presentation (~20 min)
- Lab intro (~5 min)

aws

Workshop GitHub Repo Link – Start Module 2

https://tinyurl.com/y84cc3pj
(https://github.com/aws-samples/aws-security-workshops/tree/master/threat-detection-wksp)

Directions:

- Browse to the URL https://tinyurl.com/y84cc3pj
- In the Modules section at the end of the page, click on **Attack Simulation**
- Run through this module (which just involves running a CloudFormation template / ~5 min) then we will do a presentation

aws

Threat Detection

Why is traditional threat detection so hard?

Large datasets

Signal to noise

Skills shortage

aws

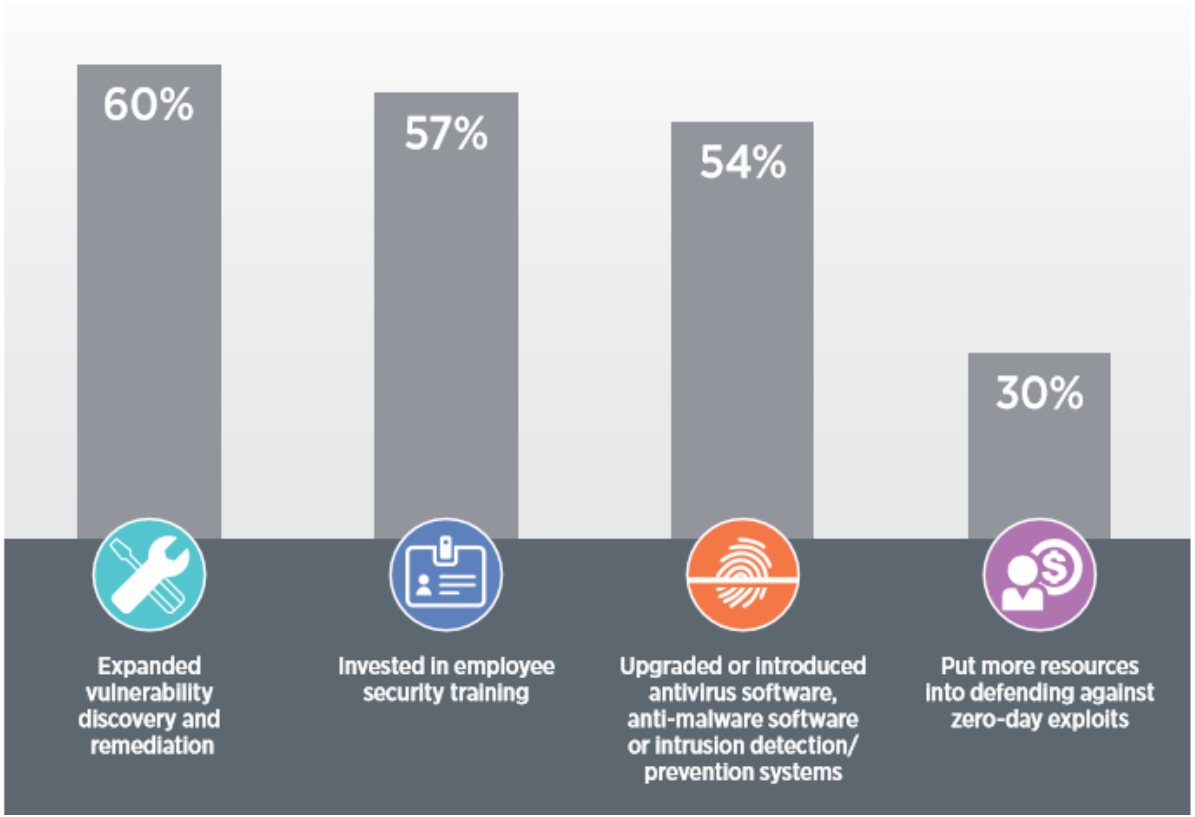
Business Top Security Focus Areas

Security Continues to Top Executive Concerns and Compete with Innovative Initiatives. Here's where GuardDuty can help.

- Implement Protections from Known Threats
- Shift from Reactive to Proactive Strategies
- Detect Successful Security Breaches
- Defend Against Zero Day Attacks
- Enhance Incident Response Capabilities
- Patching and Remediation of Known Vulnerabilities
- Public Cloud, Big Data, and Mobile Application Development
- Understand how Big Data Lends to Higher Impact Data Compromises

Source: 2017 Forbes Insights – "Enterprises Reengineer Security in the Age of Digital Transformation"

Top Actions Taken to Address Security Issues



Amazon GuardDuty addresses and augments actions taken by security professionals regarding vulnerability discovery and remediation and threat detection and prevention.

Source: 2017 Forbes Insights – "Enterprises Reengineer Security in the Age of Digital Transformation"

Threat Detection Services

Threat Detection: Log Data Inputs

AWS CloudTrail

Track user activity and API usage

VPC Flow Logs

IP traffic to/from network interfaces in your 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

aws

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

aws

Live Role Playing Exercise

Threat Detection: Triggers

AWS Config rules

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

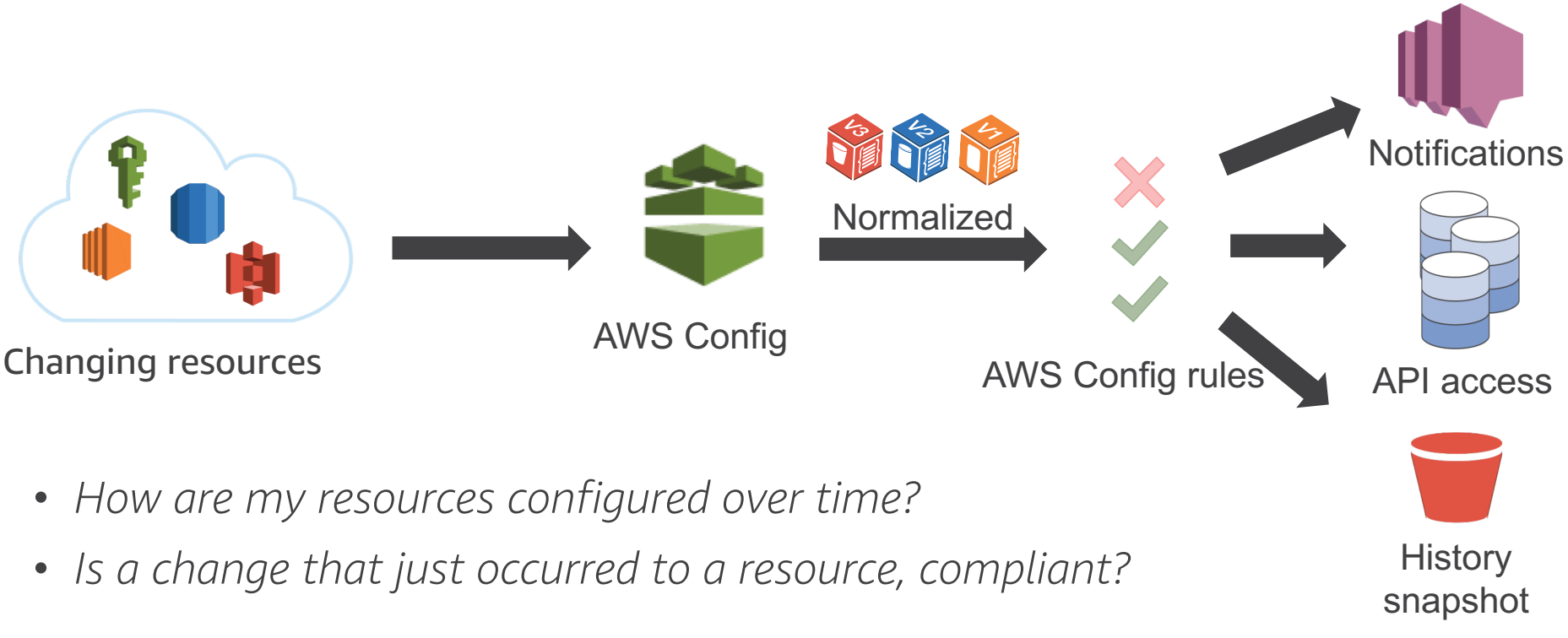
Amazon CloudWatch Events

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

aws

AWS Config Rules

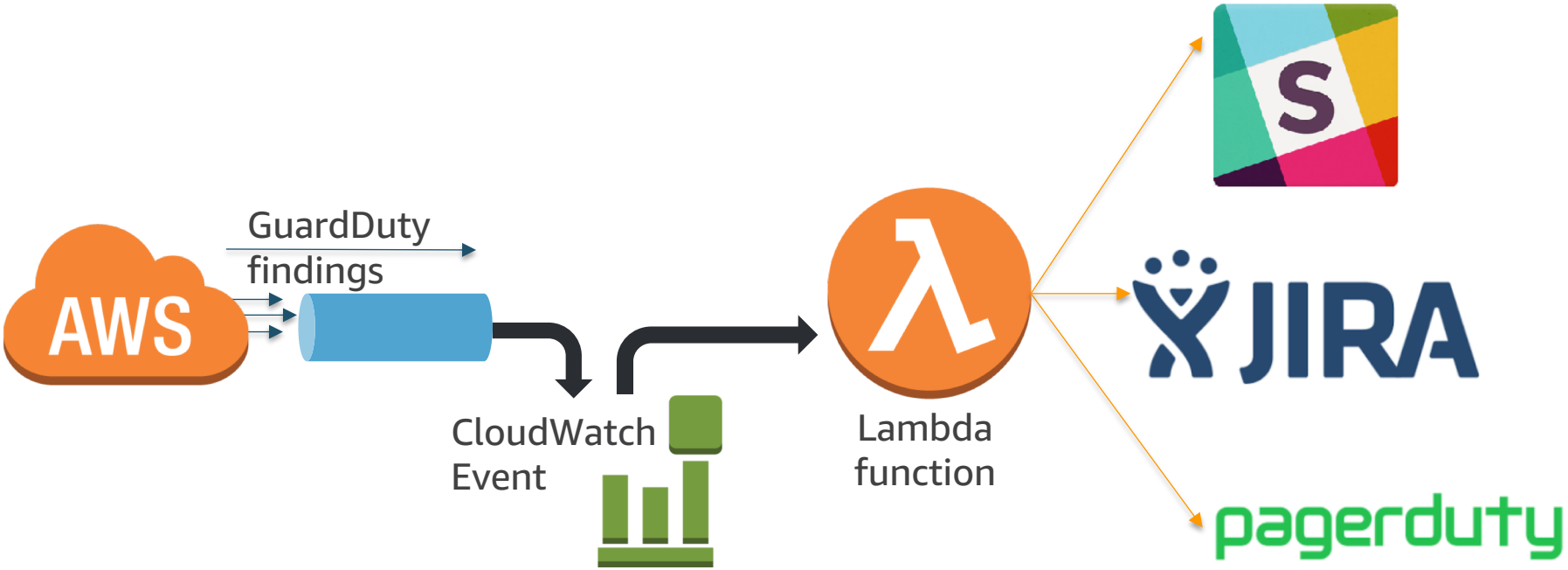
A continuous recording and assessment service



- *How are my resources configured over time?*
- *Is a change that just occurred to a resource, compliant?*

aws

Amazon CloudWatch Events

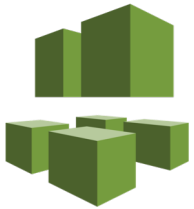


Threat Remediation Services

Threat Remediation: Automation

AWS Lambda

Capture info about the IP traffic going to and from network interfaces in your VPC



AWS Systems Manager

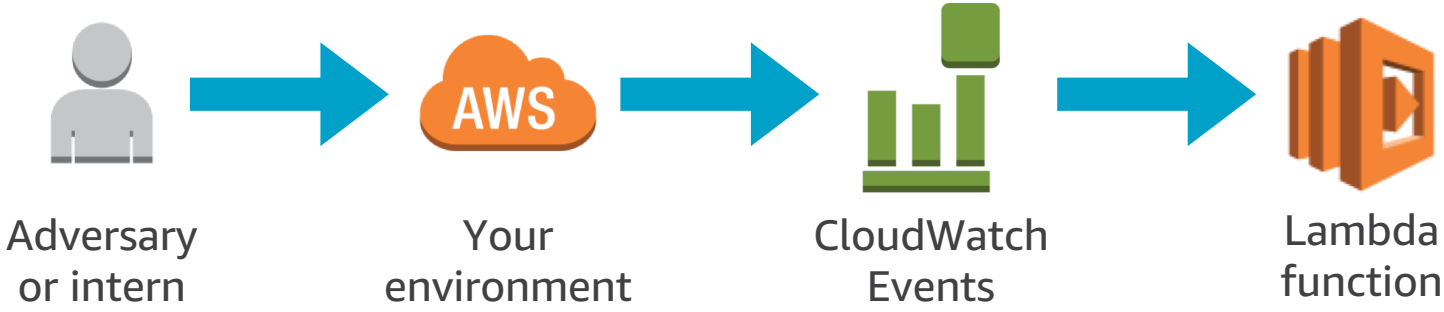
Automate patching and proactively mitigate threats at the instance level

Amazon Inspector

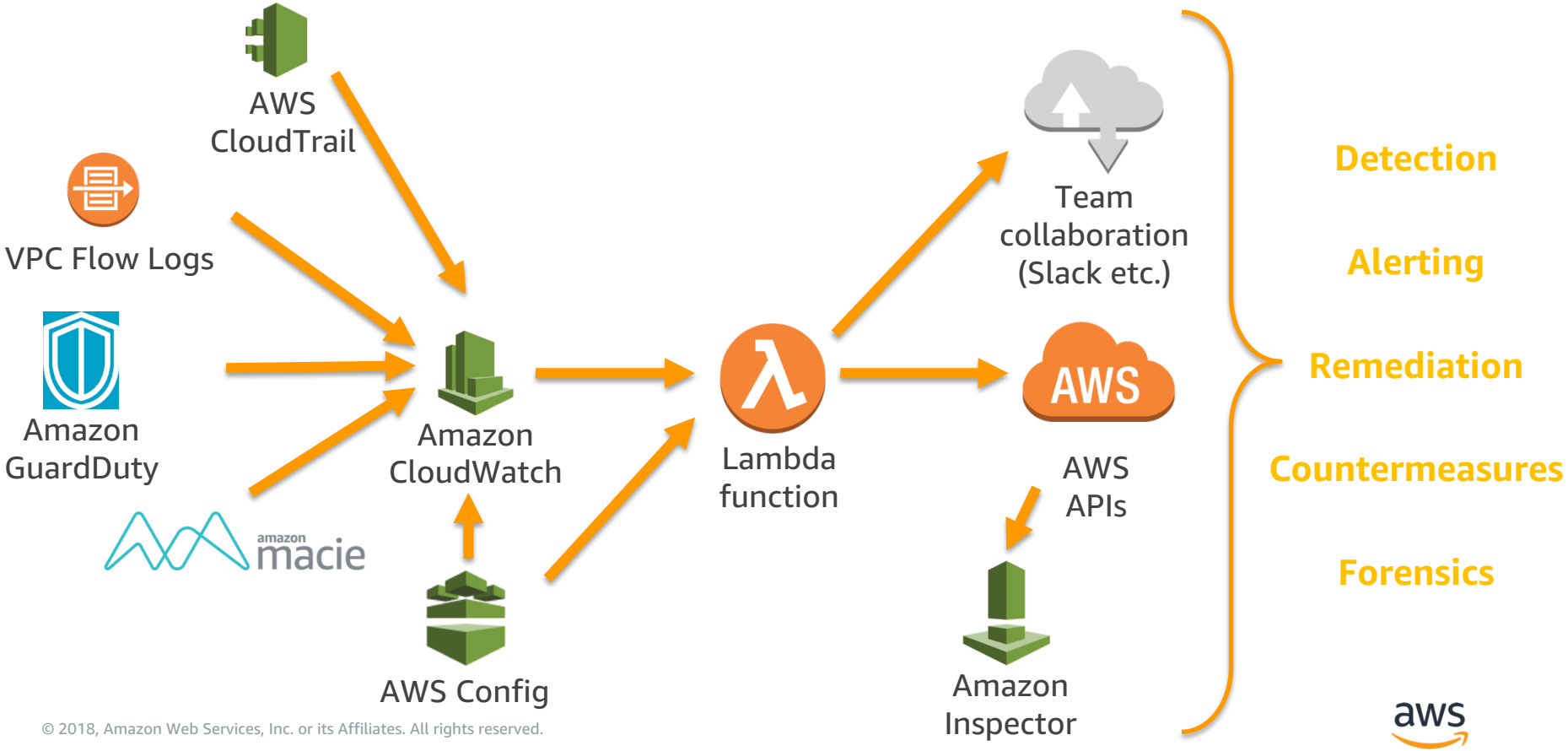
Automate security assessments of EC2 instances

aws

High-Level Playbook



High-Level Playbook



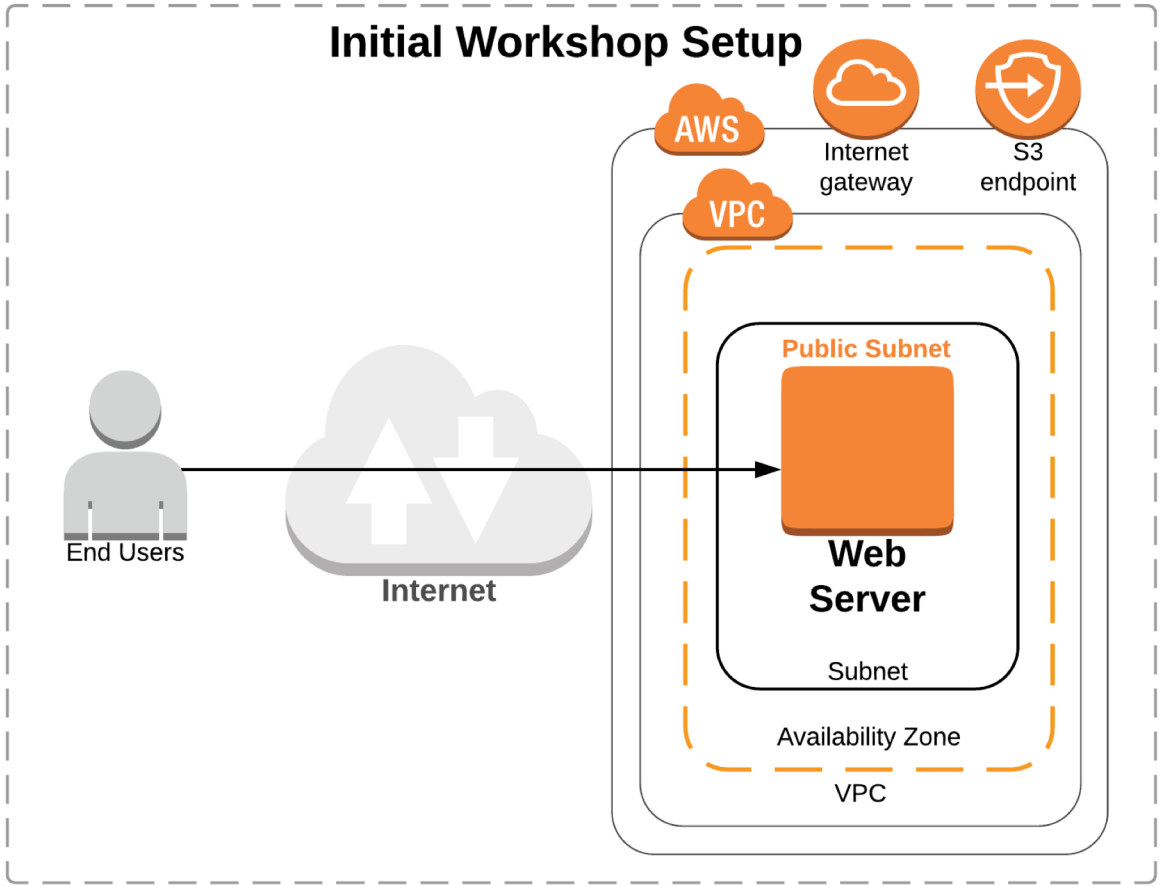
Review Questions

- How soon before enabling GuardDuty do you need to enable VPC Flow Logs?
- How do GuardDuty and Macie differ?
- How can you calculate the cost of GuardDuty? What about Macie?
- What performance impact does GuardDuty have on your account if you have more then 100 VPCs?
- Which of the services discussed have access directly to your EC2 Instances?

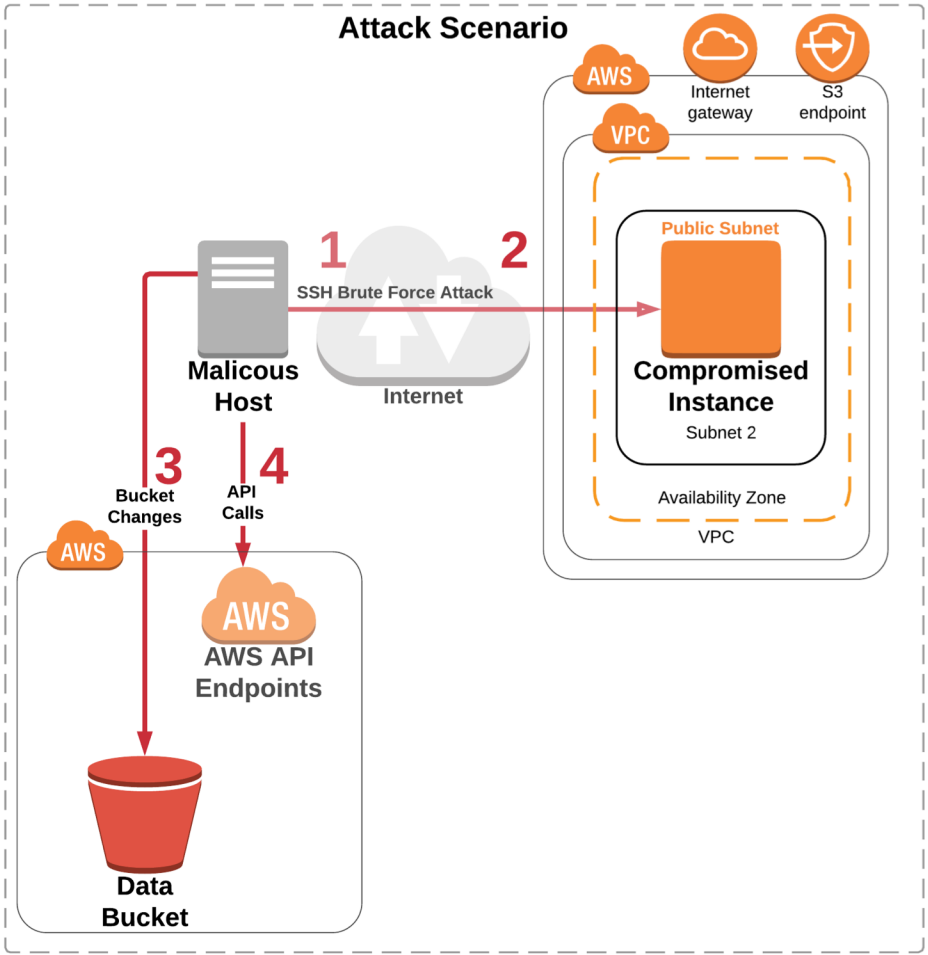
aws

Lab Info

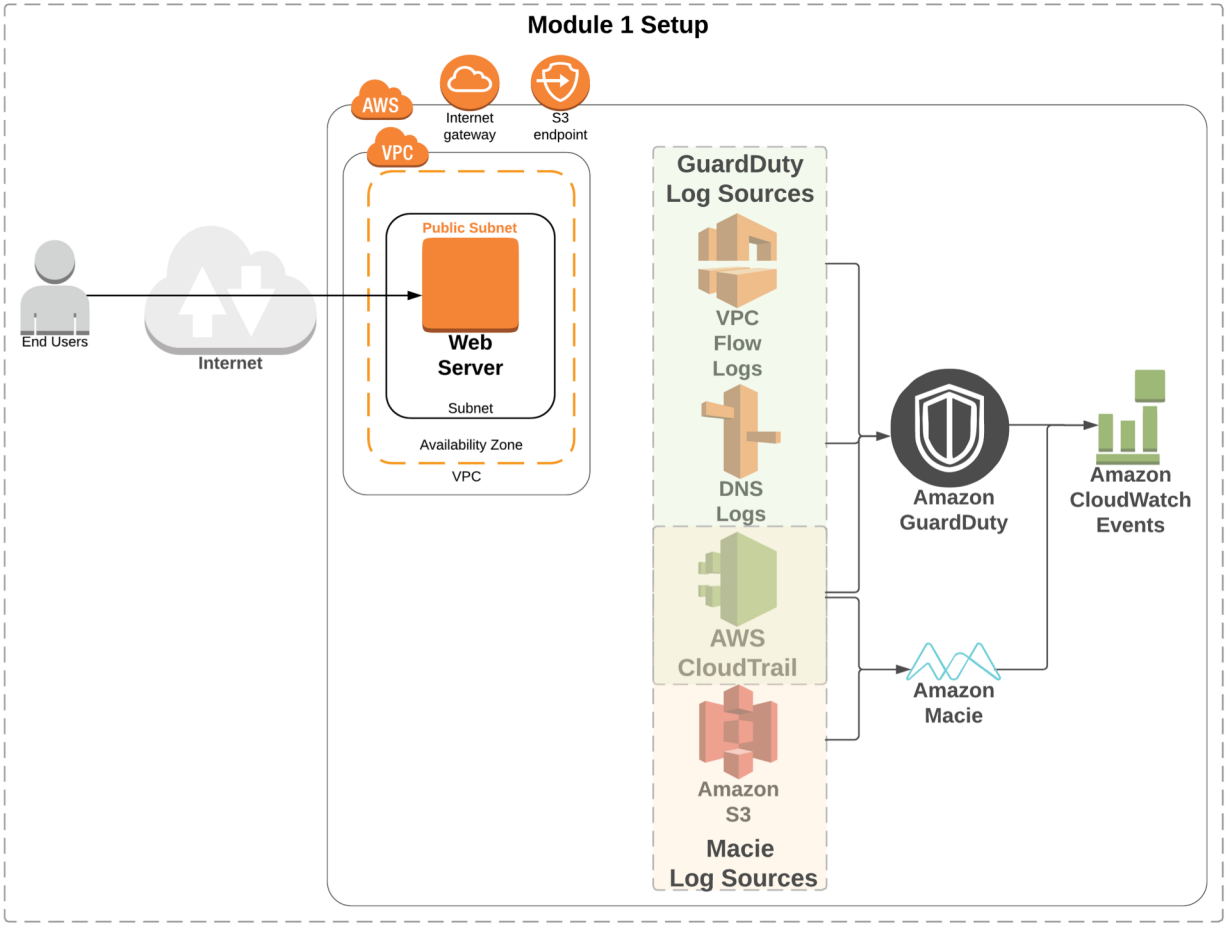
The initial setup



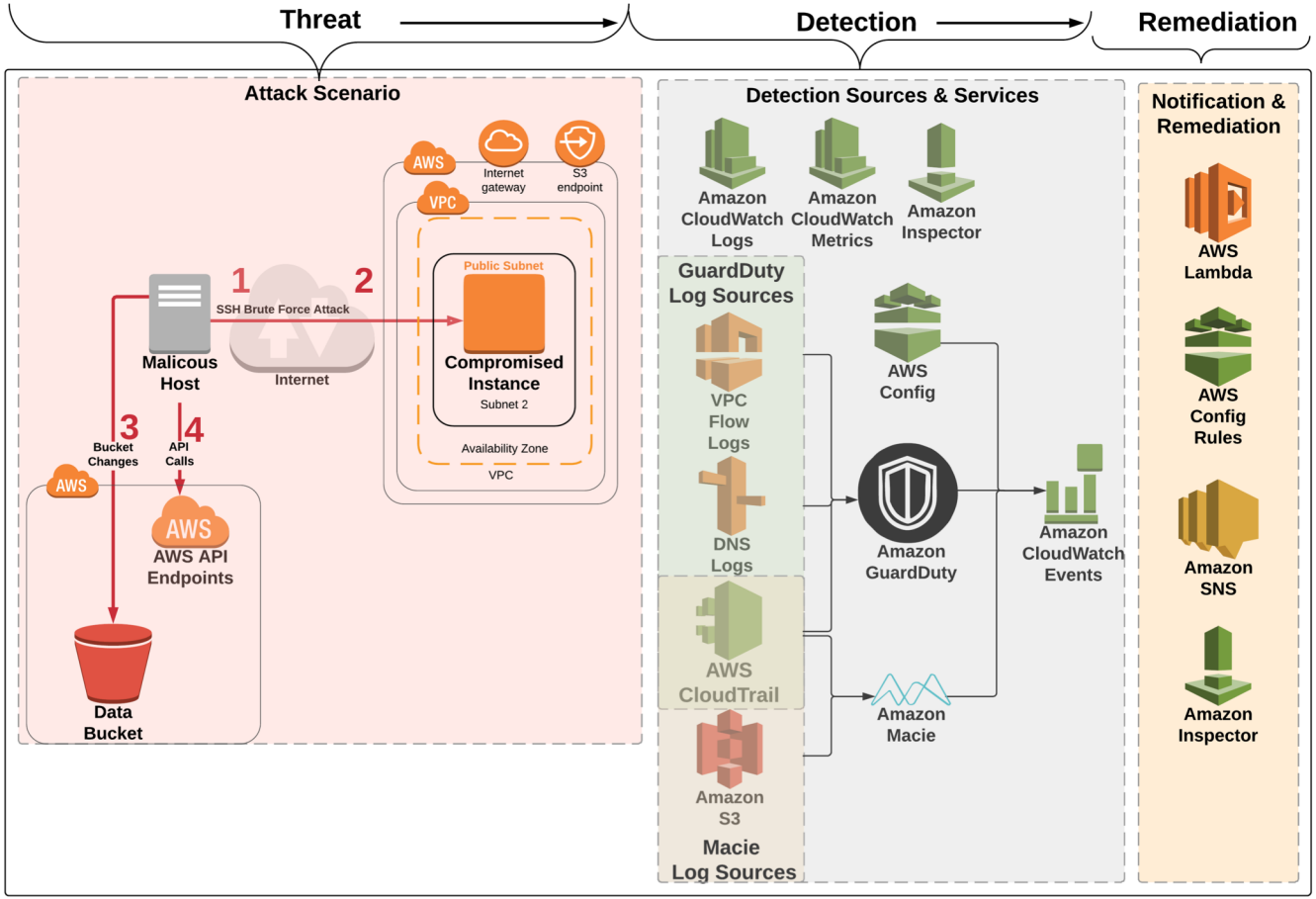
The Attack



Module 1 setup



Module 2 setup



Workshop GitHub Repo Link – Start Module 3

https://tinyurl.com/y84cc3pj
(https://github.com/aws-samples/aws-security-workshops/tree/master/threat-detection-wksp)

Directions:

- Browse to the URL https://tinyurl.com/y84cc3pj
- In the Modules section at the end of the page, click on **Detection & Remediation**
- Run through this module (~30 min) then we will do a presentation

aws

Thank you!