Threat Detection and Remediation Workshop

Module 2

Agenda

- Module 2: Run the CloudFormation template (~5 min)
- Threat detection and remediation intro presentation (~25 min)
- Workshop walkthrough (~10 min)

aws

Start module 2

use
us-west-2

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

Directions:

- Browse to **https://tinyurl.com/y84cc3pj**
- Click on **Attack Simulation** at the end
- Complete this module (~5 min) then stop
- We will then do a presentation

aws

GDPR and threat detection & remediation

Under GDPR **Controllers** and **Processors** are required to implement appropriate Technical and Organizational Measures (“TOMs”)

(1) Pseudonymisation and encryption of personal data	(2) **Ensure ongoing confidentiality, integrity, availability, and resilience of processing systems and services**
(3) **Ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident**	(4) **Process for regularly testing, assessing, and evaluating the effectiveness of TOMs**

aws

Threat Detection and Remediation Intro

Why is threat detection so hard?

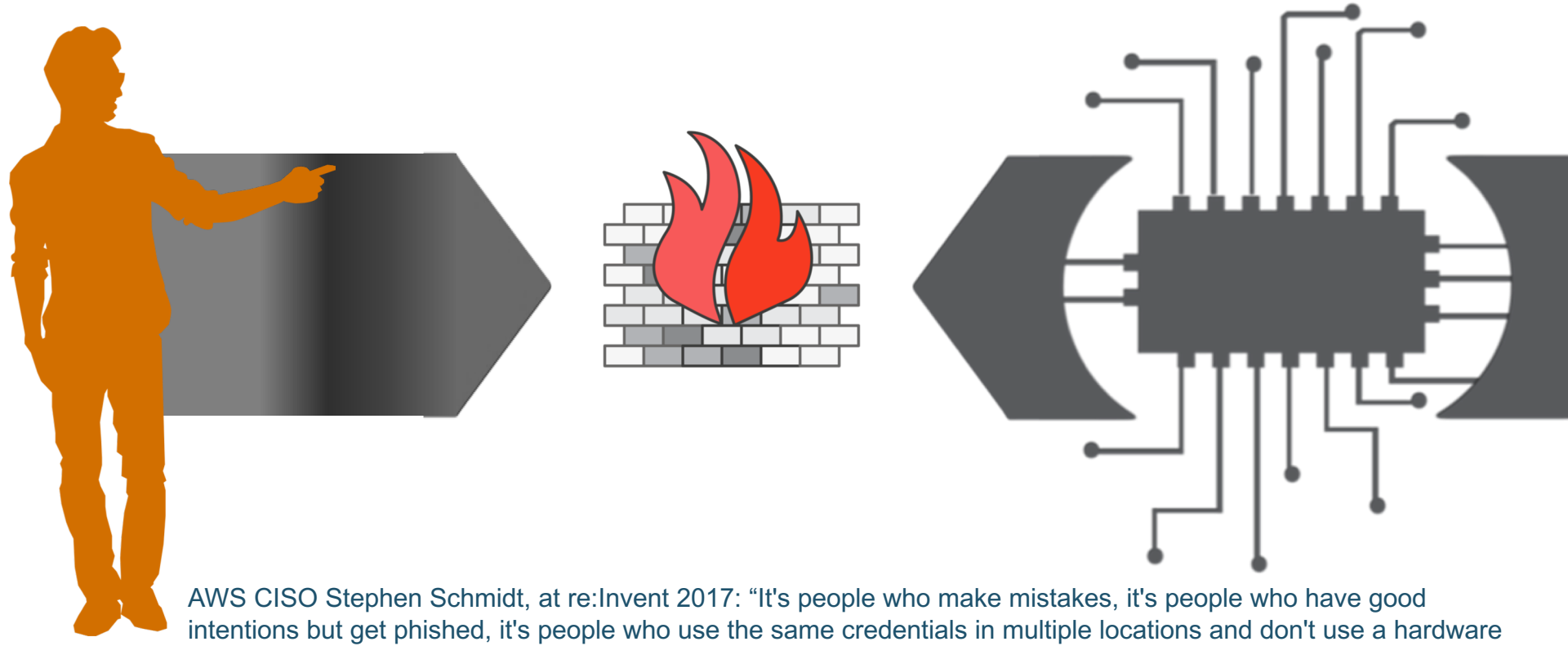
Large datasets

Signal to noise

Skills shortage

aws

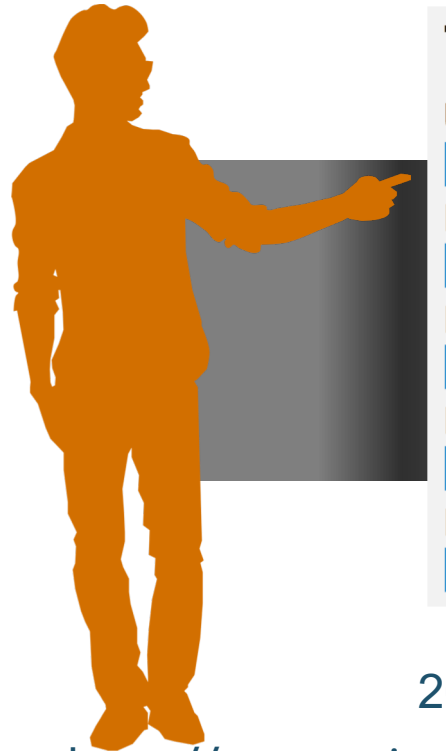
Get humans away from the data and analysis

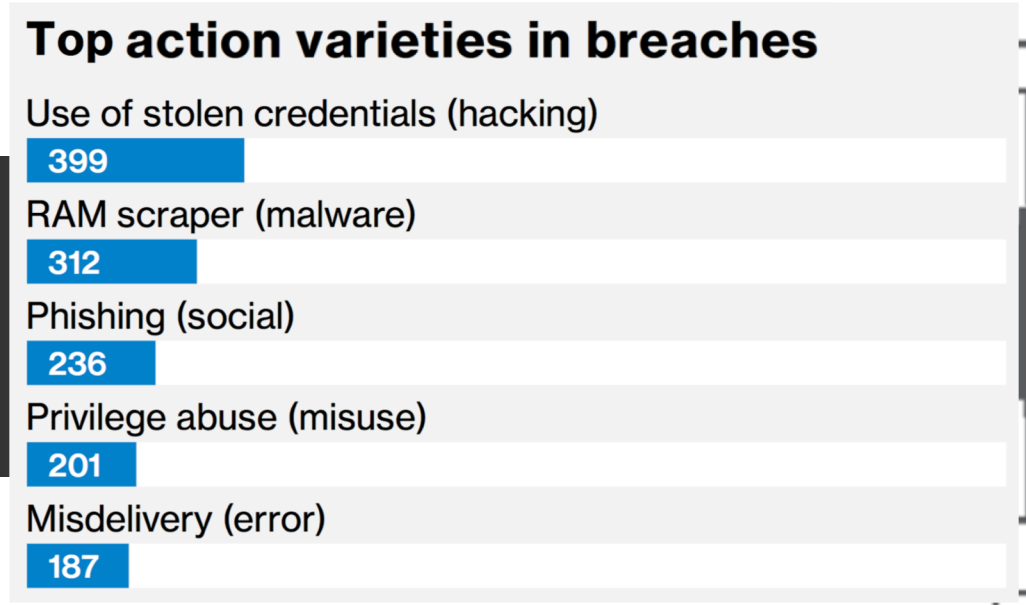


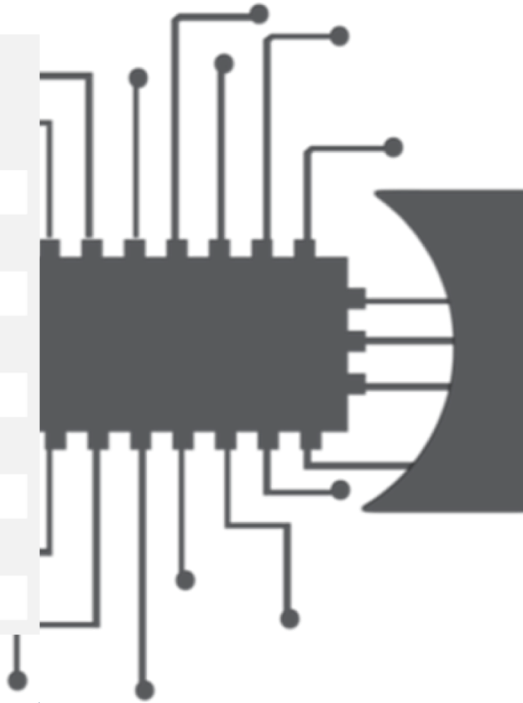
AWS CISO Stephen Schmidt, at re:Invent 2017: “It's people who make mistakes, it's people who have good intentions but get phished, it's people who use the same credentials in multiple locations and don't use a hardware token for a multi-factor authentication… Get the humans away from the data.”

aws

Get humans away from the data and analysis





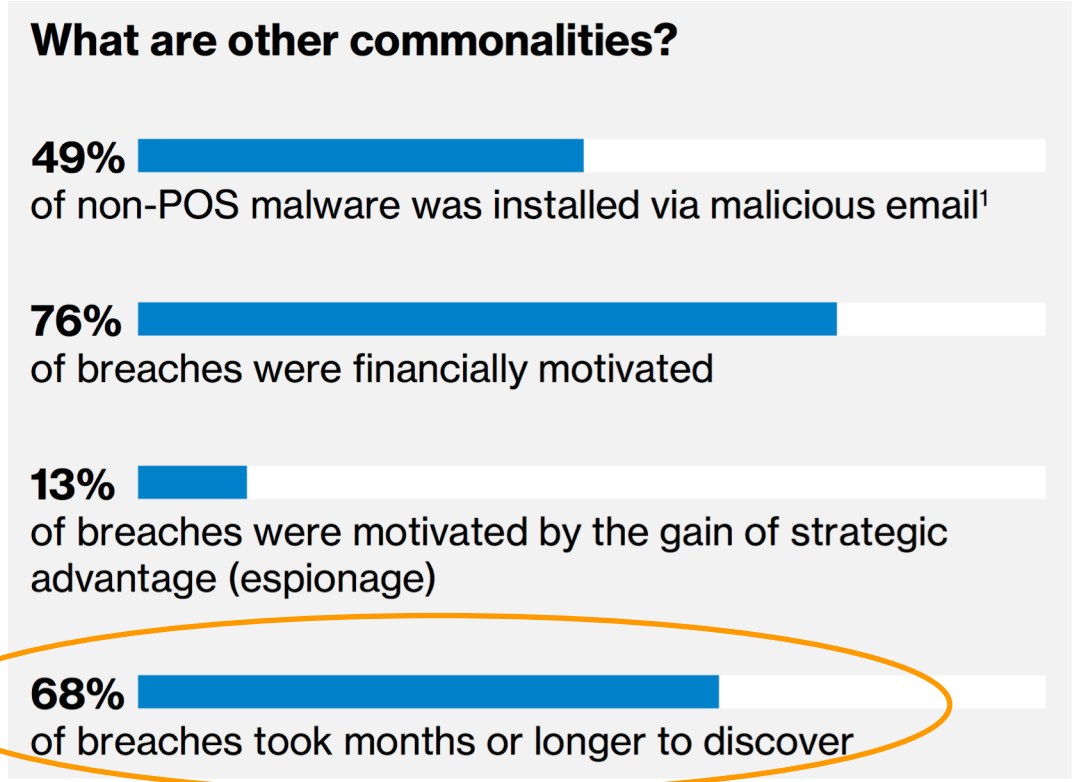


2018 Verizon Data Breach Investigations Report

https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

aws

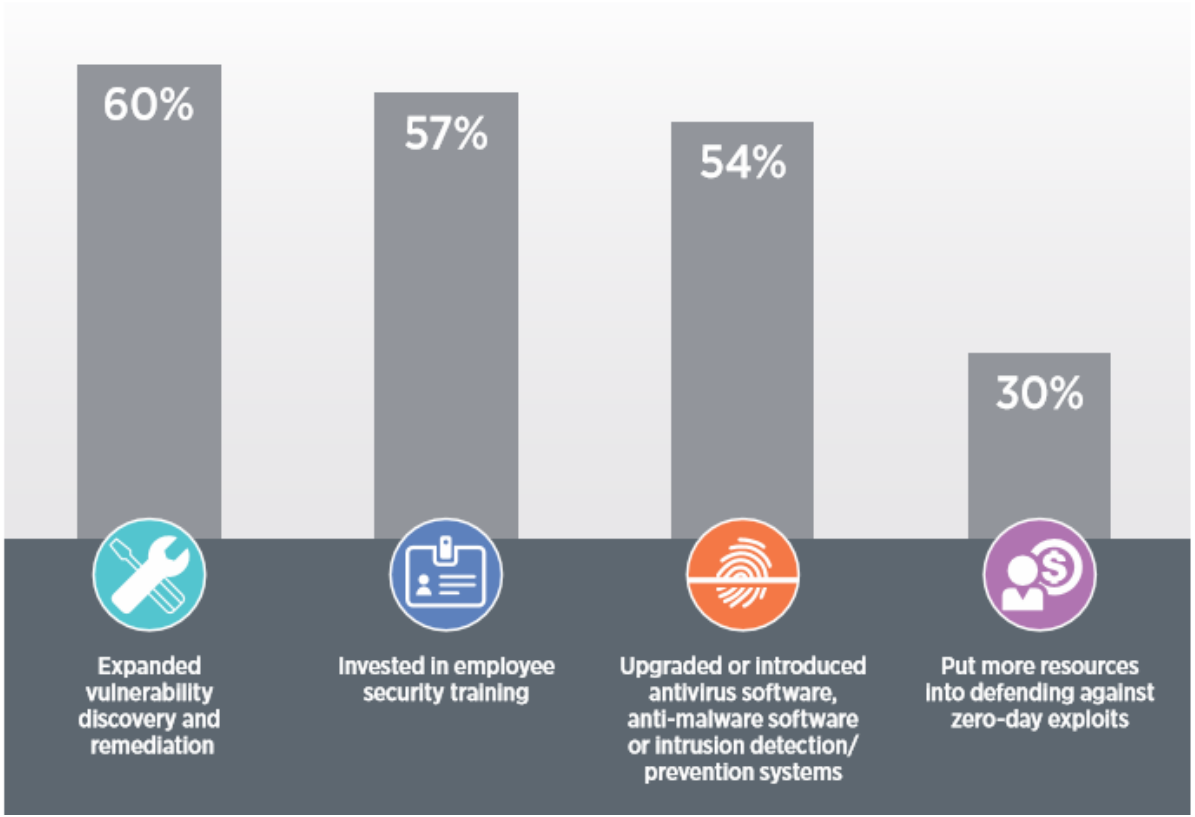
Detecting breaches



https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

aws

Top Actions Taken to Address Security Issues



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

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

AWS Security Solutions

https://www.nist.gov/cyberframework

Identify

AWS
Systems Manager

AWS Config

Protect

AWS
Systems Manager

Amazon Inspector

VPC

KMS

AWS CloudHSM

IAM

AWS Organizations

AWS Cognito

AWS Directory Service

AWS Single Sign-On

Certificate Manager

Amazon Inspector

Amazon Macie

Detect

AWS CloudTrail

AWS Config Rules

**Amazon
CloudWatch Logs**

Amazon GuardDuty

VPC Flow Logs

Amazon Macie

AWS Shield

AWS WAF

Respond

AWS Config Rules

AWS Lambda

**AWS
Systems Manager**

**Amazon
CloudWatch Events**

Recover

AWS Config Rules

AWS Lambda

aws

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: Evocations/Triggers

AWS Config rules

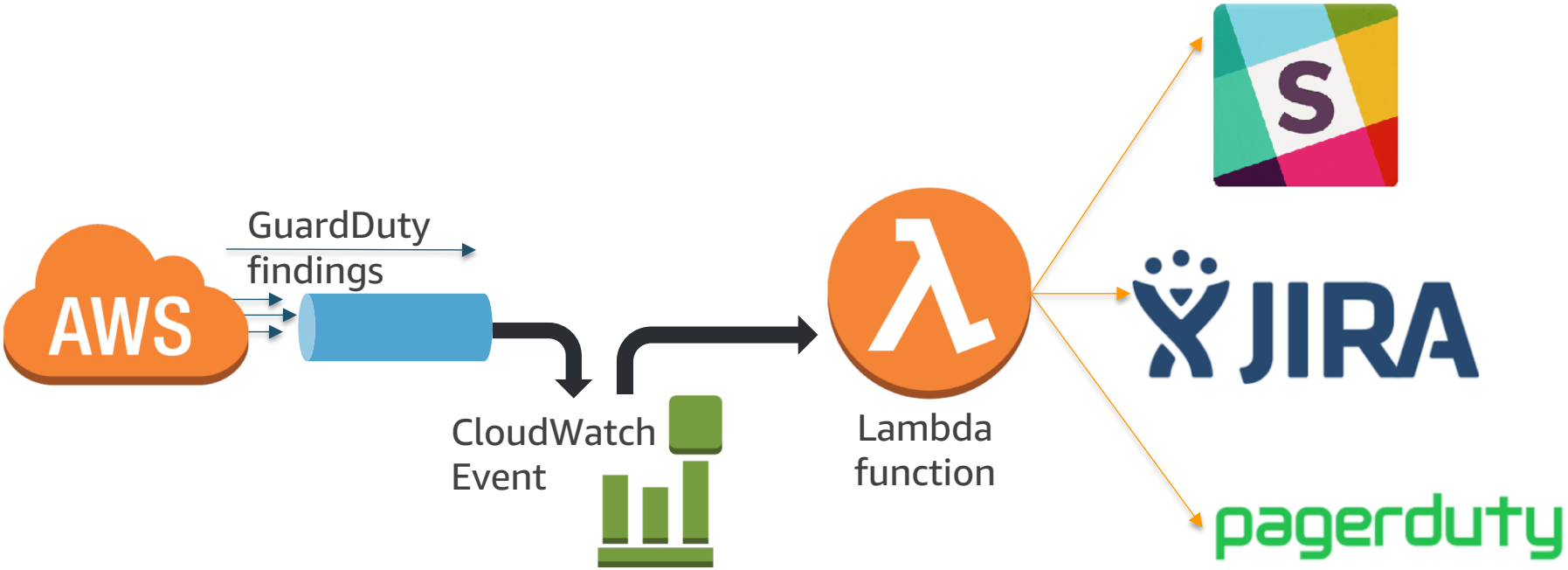
Continuously tracks your resource configuration changes and if they violate any of the conditions in your rules

Amazon CloudWatch Events

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

aws

Amazon CloudWatch Events

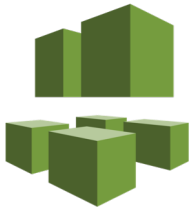


Threat Remediation Services

Threat Remediation Services

AWS Lambda

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



AWS Systems Manager

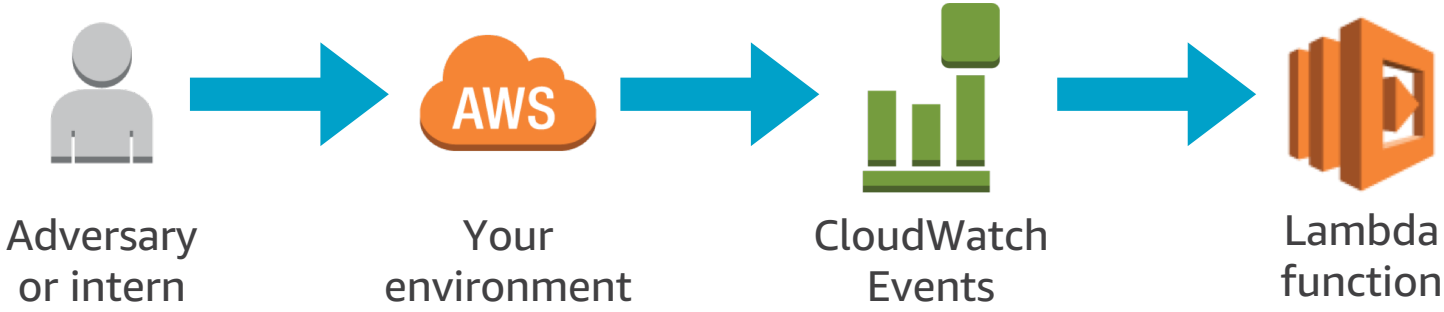
Gain operational insights and take action on AWS resources

Amazon Inspector

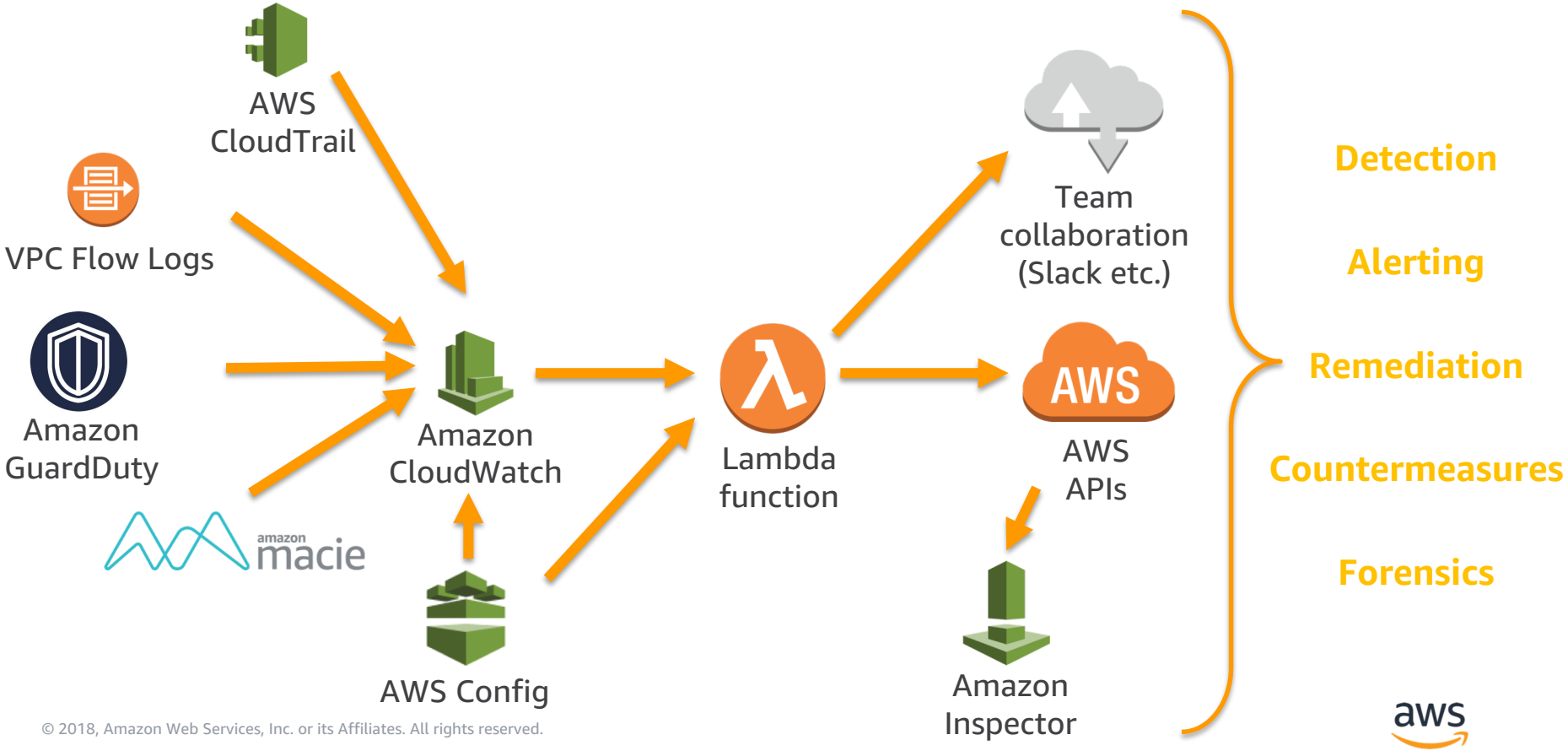
Automate security assessments of EC2 instances

aws

High-Level Playbook



High-Level Playbook



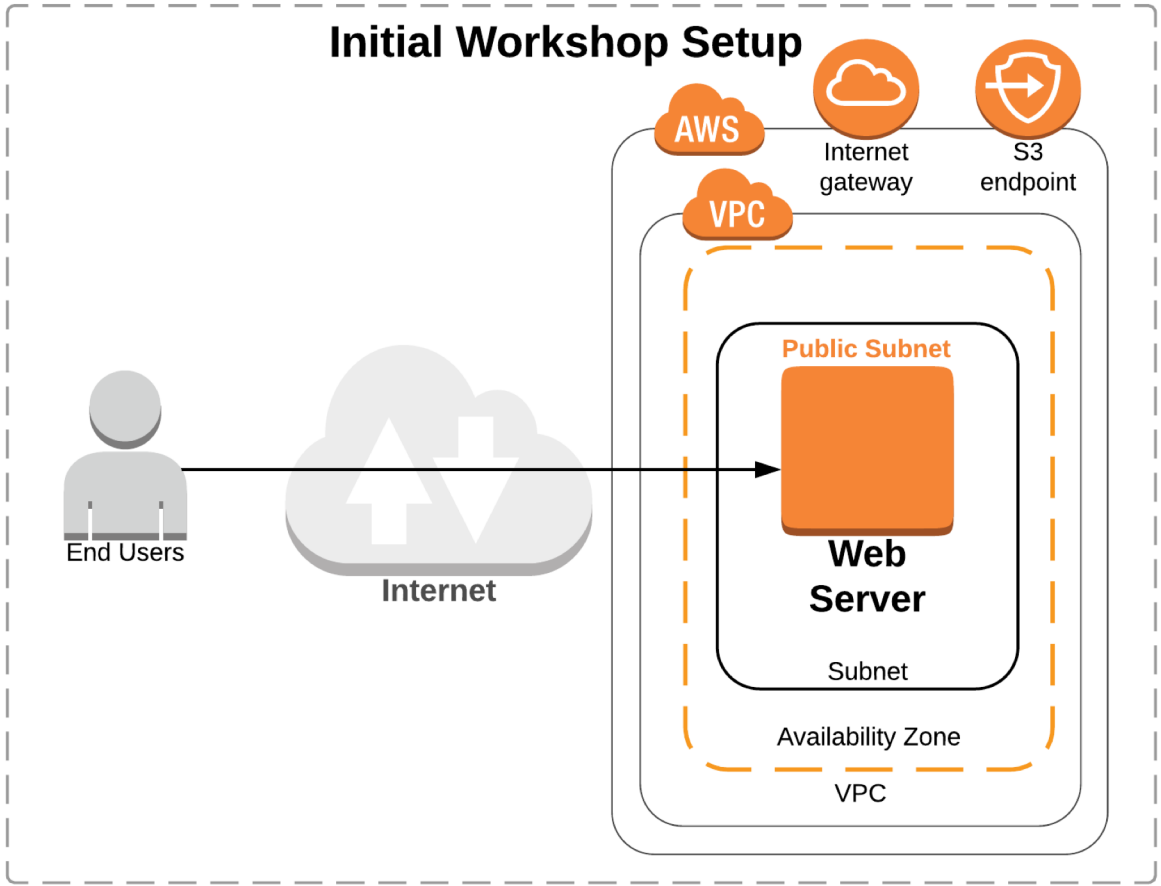
Review Questions

- How can you create custom rules for Config?
- How do GuardDuty and Macie differ?
- What services are important for automation of remediations?
- What performance impact does GuardDuty have on your account if you have more then 100 VPCs?
- Which of the services discussed have direct access to your EC2 Instances?

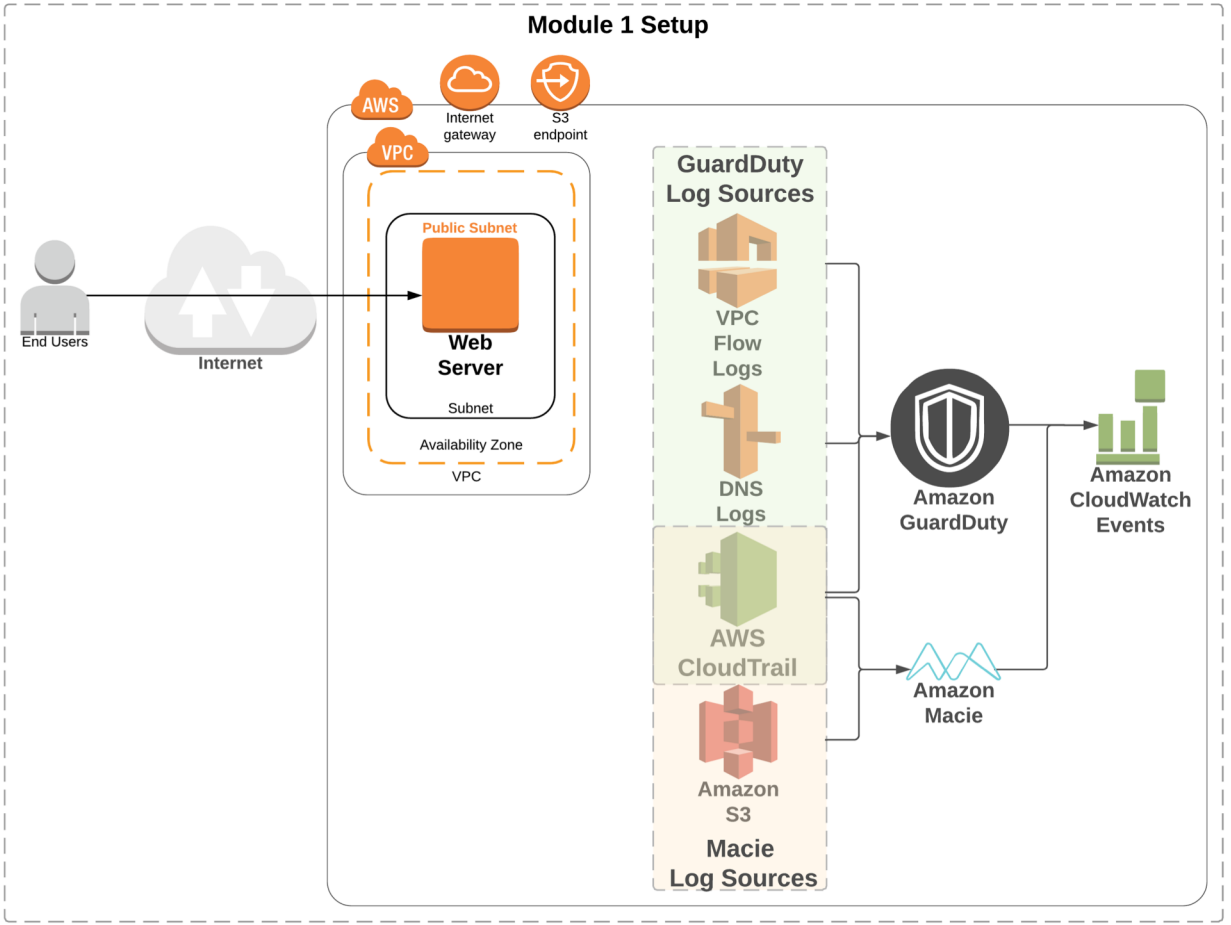
aws

Workshop walkthrough

The initial setup



Module 1 setup



Start module 3

use
us-west-2

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

Directions:

- Browse to **https://tinyurl.com/y84cc3pj**
- Click on **Detection & Remediation** at the end
- Run through this module (~45 min)
- We will then finish up with module 4 and cleanup

aws