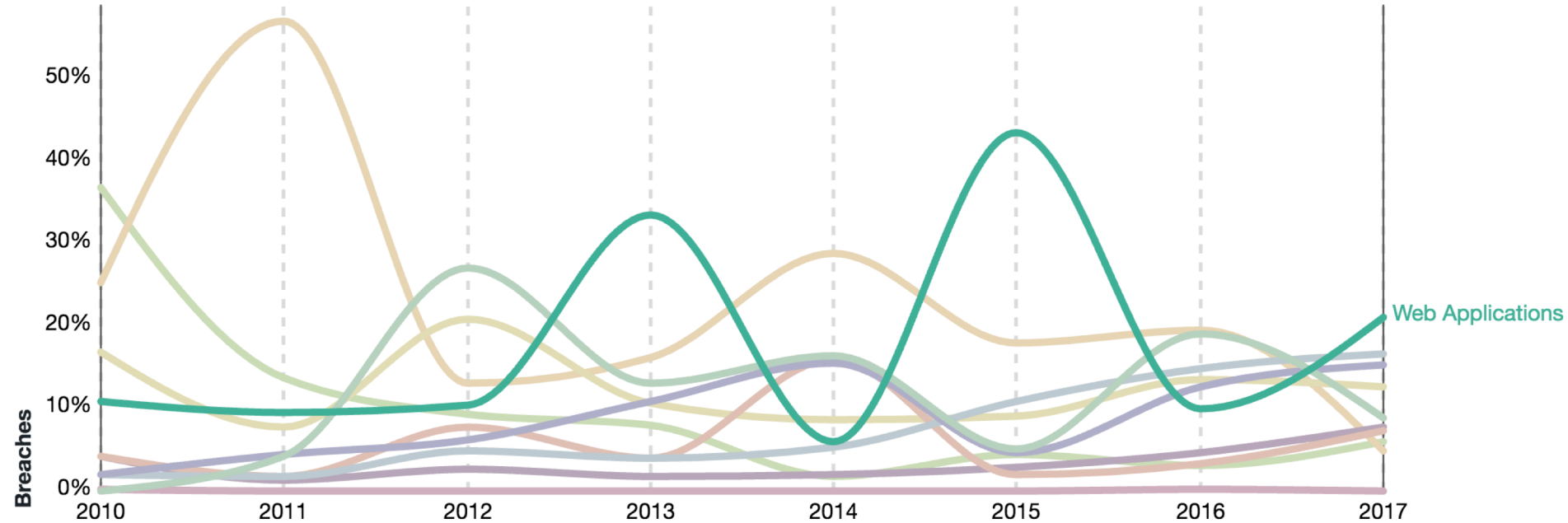


Threat Detection and Remediation Workshop

Module 1

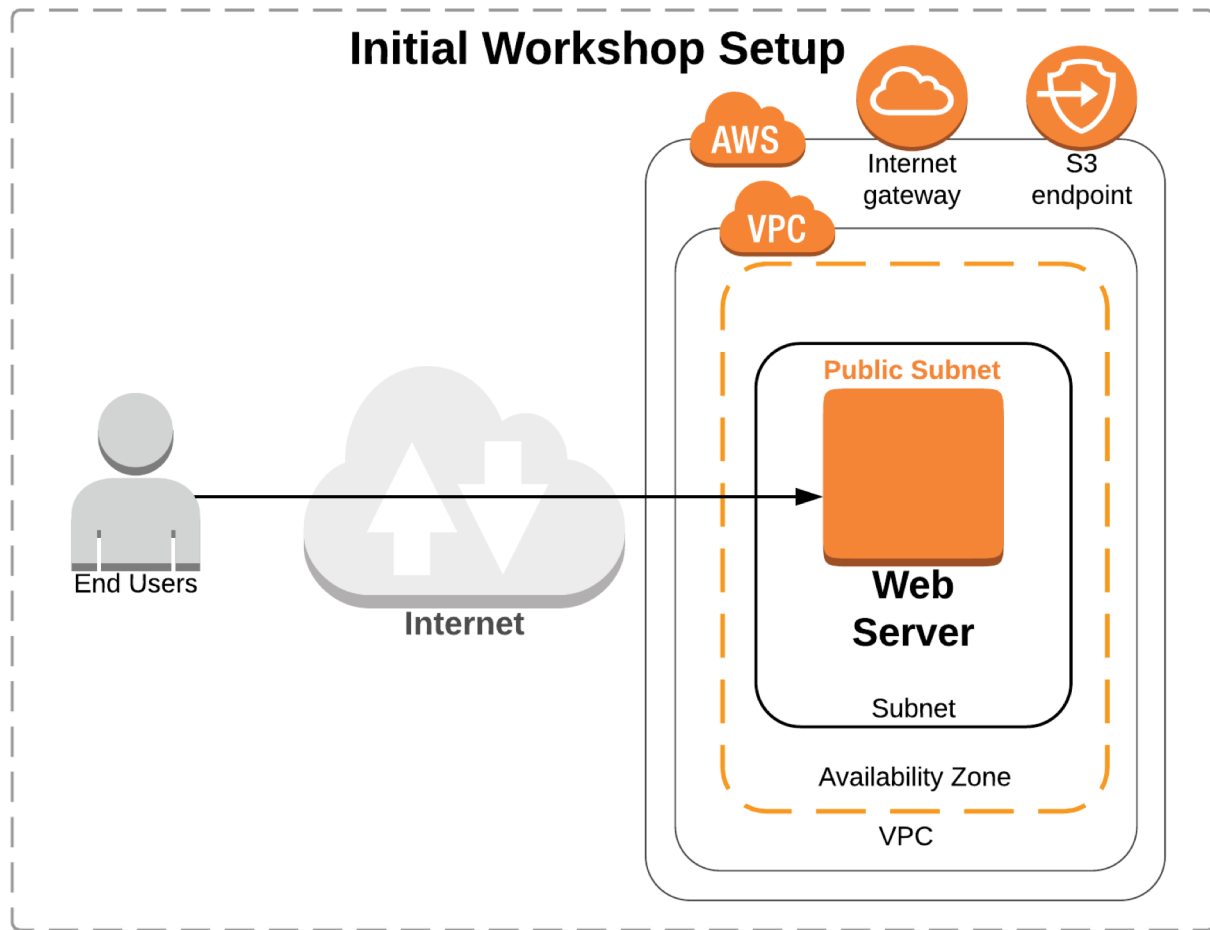
Verizon Report

Verizon - 2018 Data Breach Investigations Report
Data Breach Patterns



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

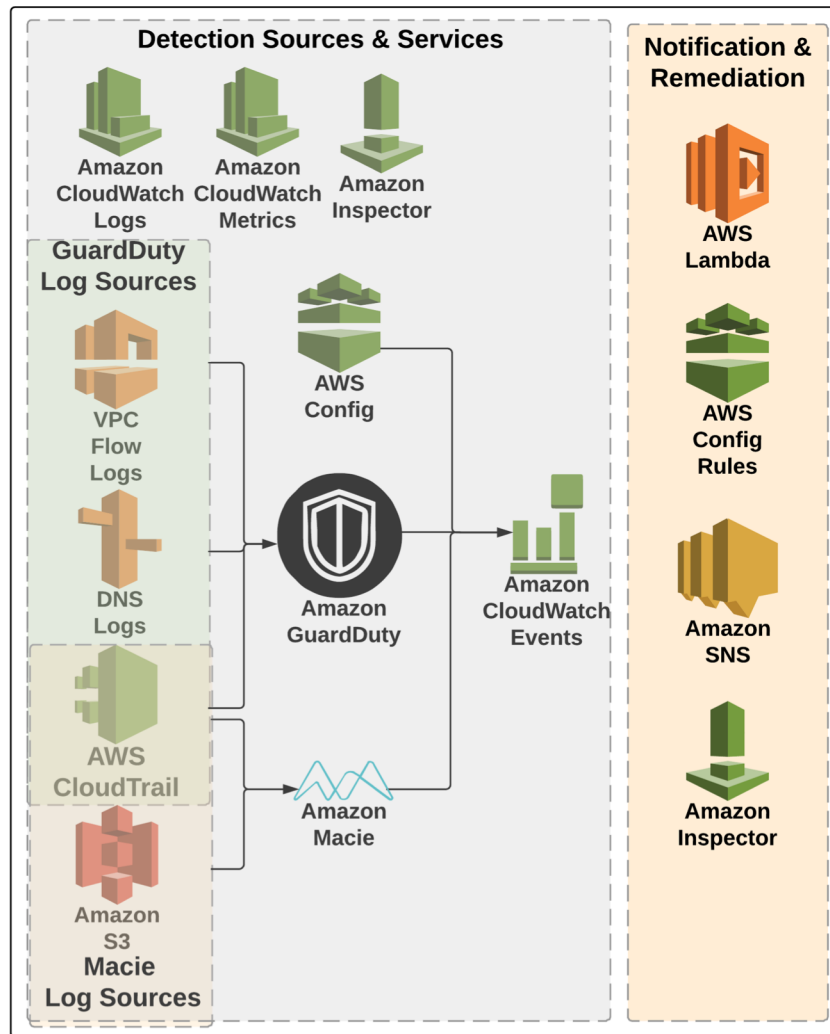
Initial setup



Workshop agenda

- Quick introduction to the workshop
- **Module 1: Environment build and configuration** (20 min)
 - Run CloudFormation template and some setup
- **Module 2: Attack simulation (and presentation)** (40 min)
 - Run CloudFormation template
 - Presentation and live role playing exercise
- **Module 3: Detection and remediation** (45 min)
 - Investigate the attack
- **Module 4: Review and discussion** (15 min)
 - Presentation / group Q&A
 - Cleanup

Threat detection and remediation services



Start module 1

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>
- Read through the workshop scenario
- Click on **Environment Build and Configuration** at the end
- Complete module (~15 min) then stop
- We will later start module 2 and do a presentation

Start module 1

<https://tinyurl.com/y84cc3pj>

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

use
us-west-2

Parameters

Resource and Notification Configuration

Resource Prefix

threat-detection-wksp

Prefix of Resources created for this workshop.

Email Address

example@example.com

Enter a valid email address for receiving alerts.

Security Services Configuration

AWS Config

No

Is AWS Config already enabled in this region?

Amazon Macie Roles

No

Have the Amazon Macie IAM Roles been created for this account?

AWS Inspector Role

No

Has the Inspector Service-Linked Role been created for this account?