Threat Detection and Remediation Workshop

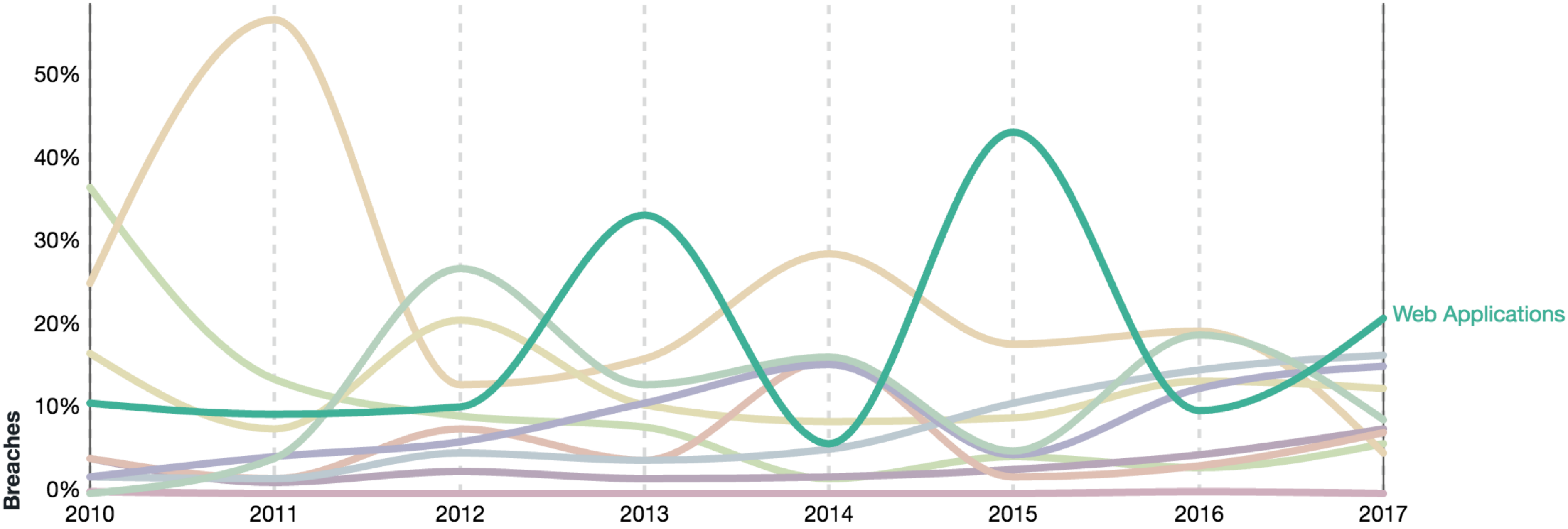
Module 1

Workshop agenda

- Quick introduction to the workshop
- **Module 1:** environment build and configuration (15 min)
  - Run CloudFormation template and some setup
- **Module 2:** attack simulation (and presentation) (40 min)
  - Run CloudFormation template
  - Presentation and Live Demo Exercise
- **Module 3:** detection and remediation (50 min)
  - Investigate the attack
- **Module 4:** review and discussion (15 min)
  - Presentation / group Q&A
  - Cleanup

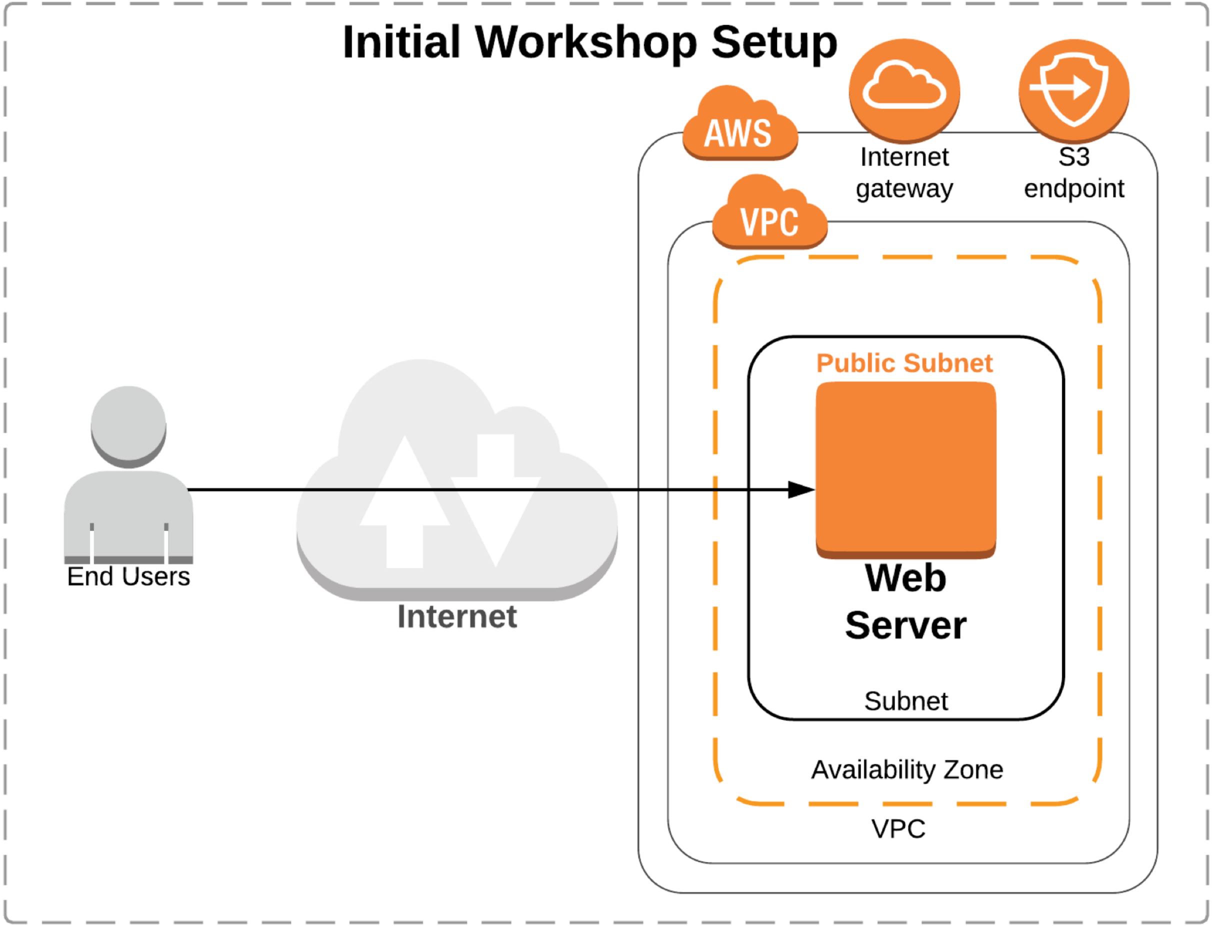
Verizon Report

Verizon - 2018 Data Breach Investigations Report



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

Initial setup



Workshop GitHub Repo Link – Start Module 1

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
- Read through the lab scenario
- In the Modules section at the end of the page, click on **Environment Build and Configuration**
- Run through this module (~15 min) then stop (we will then start Module 2 and do a presentation)