MICHIGAN STATE UNIVERSITY

Alpha Presentation

Improved Detonation of Evasive Malware

The Capstone Experience

Team Proofpoint

Ryan Gallant
Jack Mansueti
Ian Murray
Sean Joseph
Tae Park

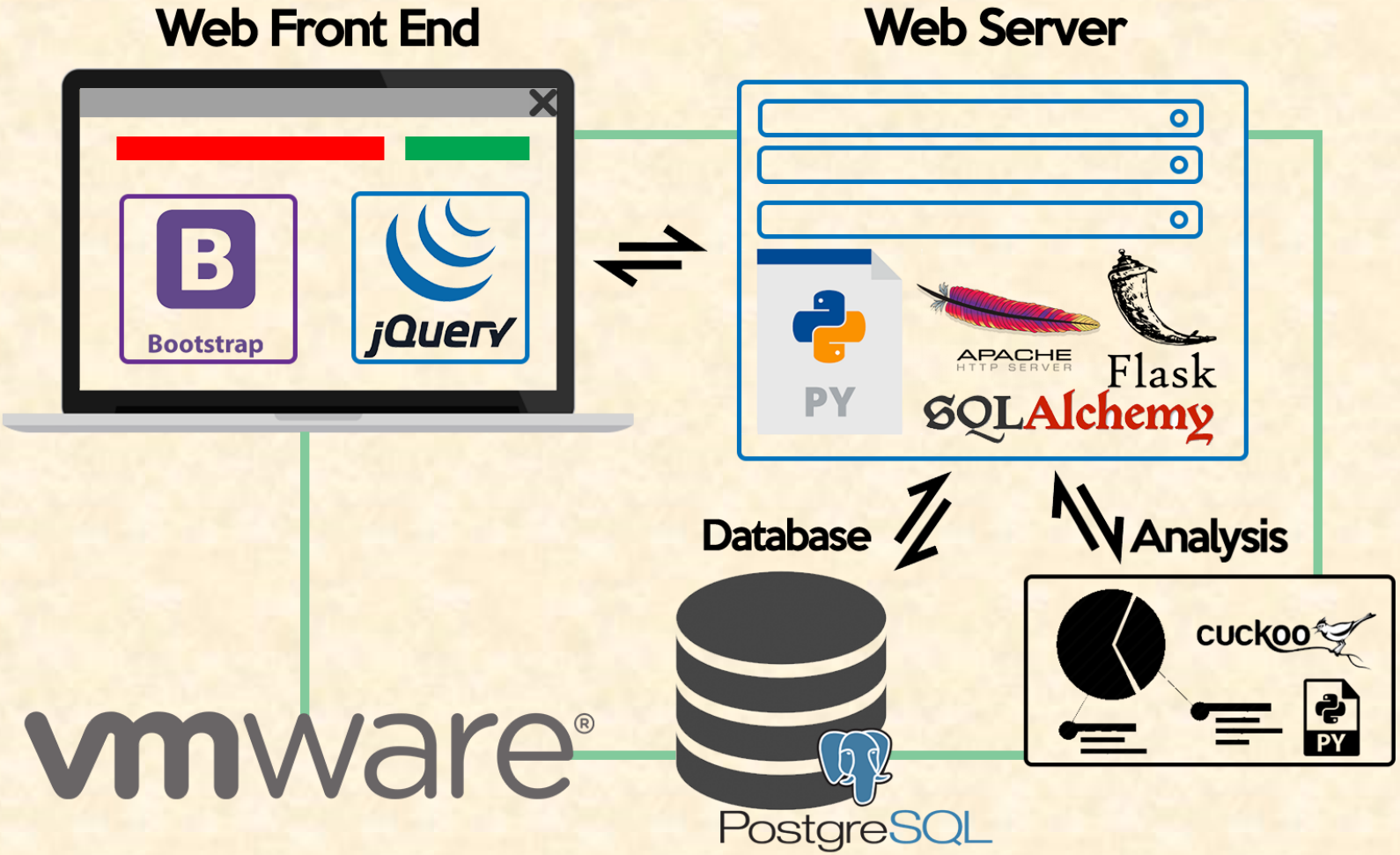
Department of Computer Science and Engineering
Michigan State University
Fall 2018

From Students…
…to Professionals

Project Overview

- System reads in a live feed of malware from Proofpoint
- Cuckoo sandbox detonates malware
- If Cuckoo detects evasive behaviors, it sends the malware to the python script for modification
- After modification, malware is sent back to Cuckoo to execute again
- Results are sent to the dashboard

System Architecture



What's left to do?

- Detection and action on additional evasive behaviors
- Automation
  - Link to Proofpoint's inflow
  - Run any program all the way through without any human interaction
- Work with more Formats of Executable

Questions?