

**MICHIGAN STATE**  
**UNIVERSITY**

# Project Plan

## Predictive Engine for Long Term Malware Detonation

### The Capstone Experience

#### Team Proofpoint

Izzy Dove

Samuel Gendelman

Alexander Kendall

Joshua Wilson

Geoffrey Witherington-Perkins

Department of Computer Science and Engineering

Michigan State University

Spring 2020



*From Students...*  
*...to Professionals*

# Functional Specifications

---

- Long-term malware detonation & analysis
- Automatic categorization of malware
- Display analysis data on web application



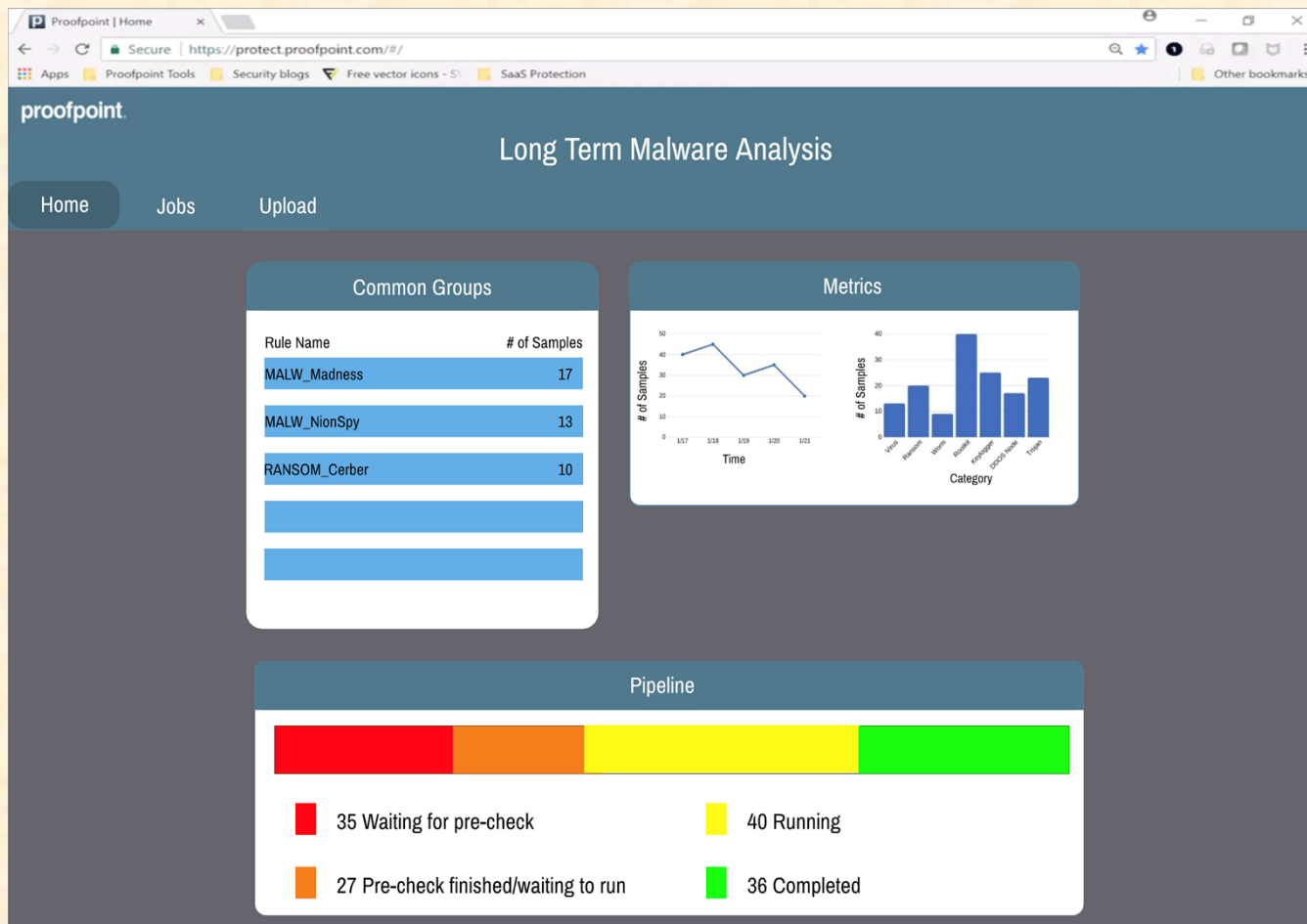
# Design Specifications

---

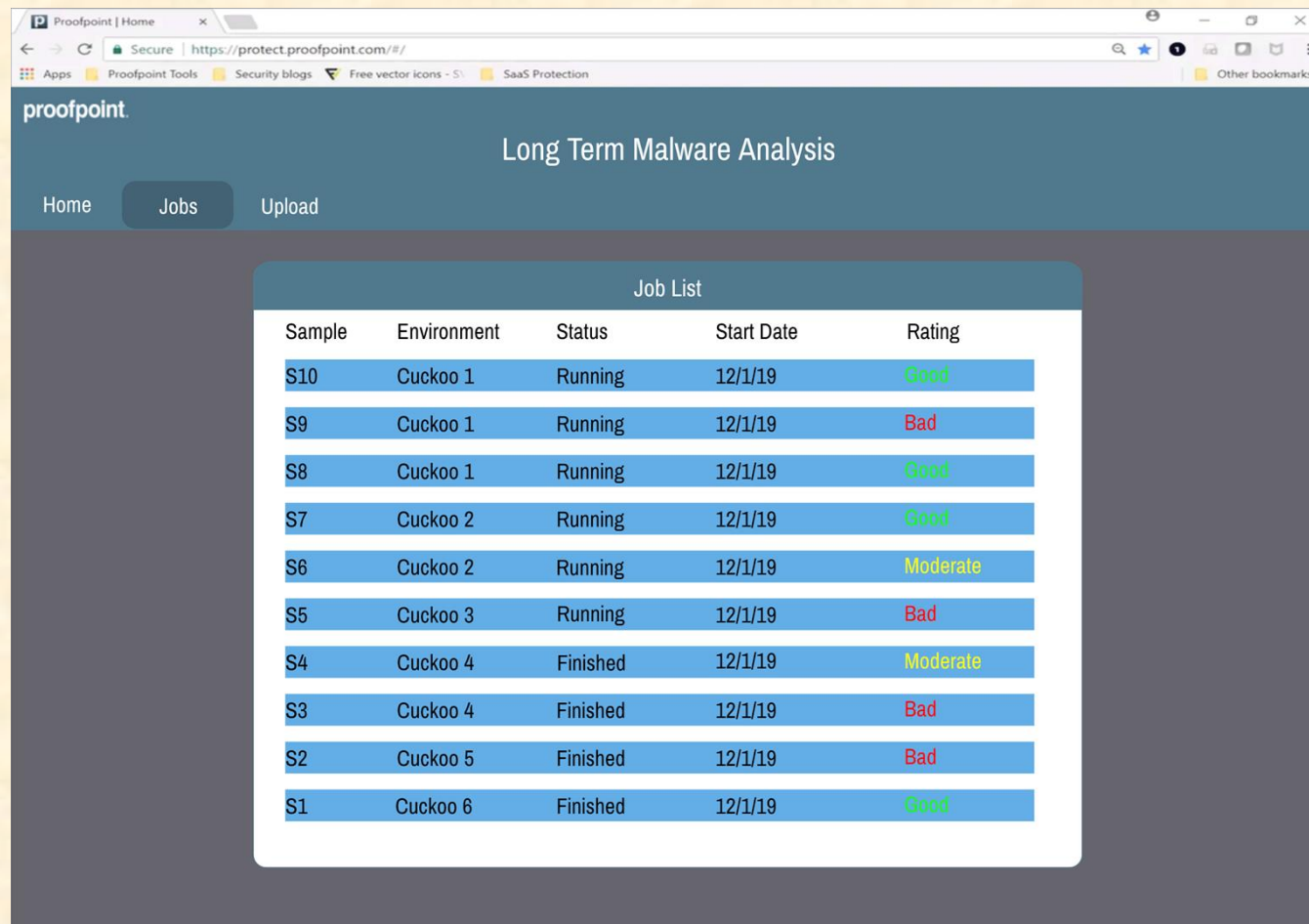
- Home Dashboard with summary of overall data
- Jobs Page with a list of all running jobs
- Individual Sample Page with sample information
- Upload Page used to upload malware samples



# Screen Mockup: Home Page



# Screen Mockup: Jobs Page



proofpoint.

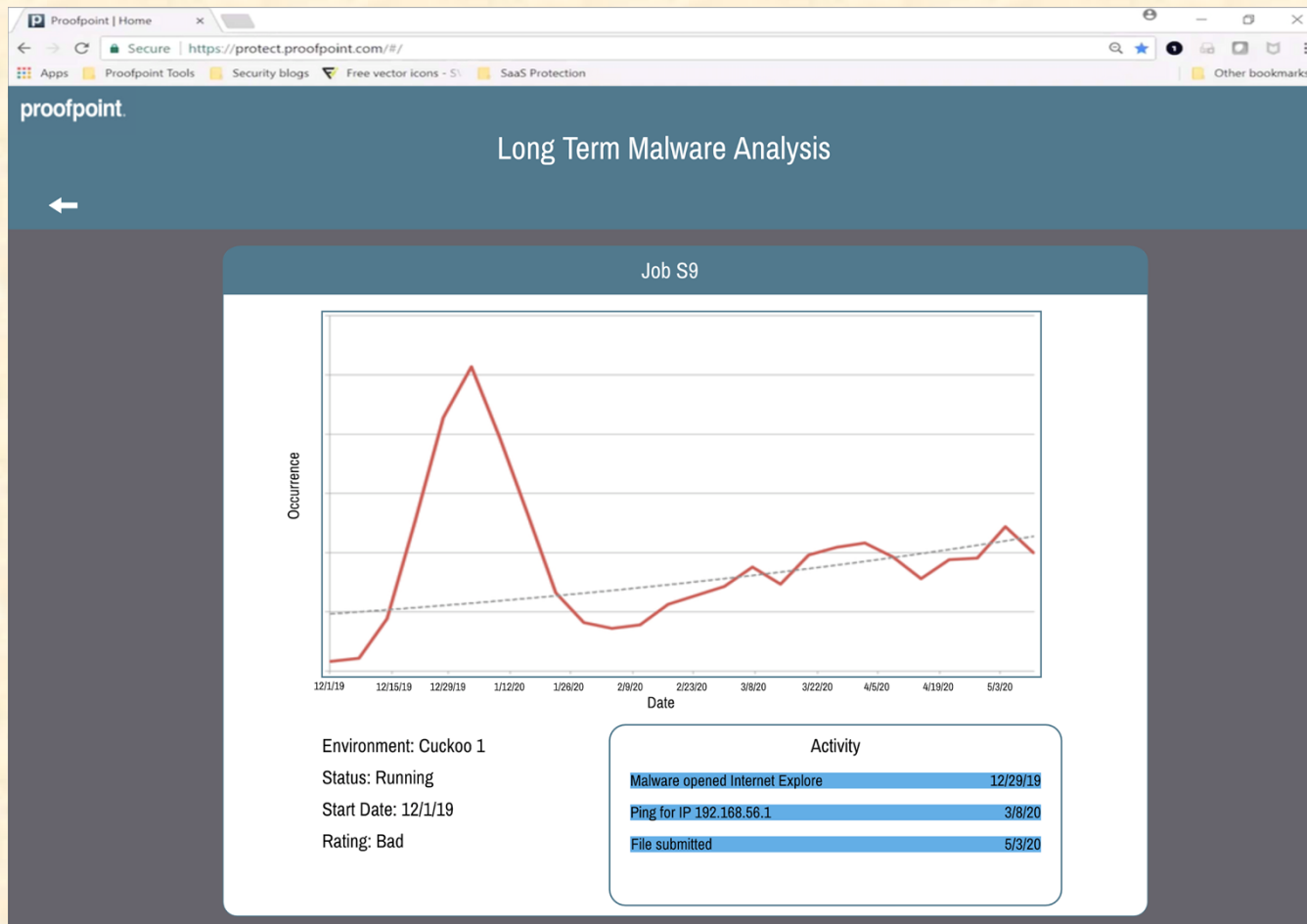
Long Term Malware Analysis

Home Jobs Upload

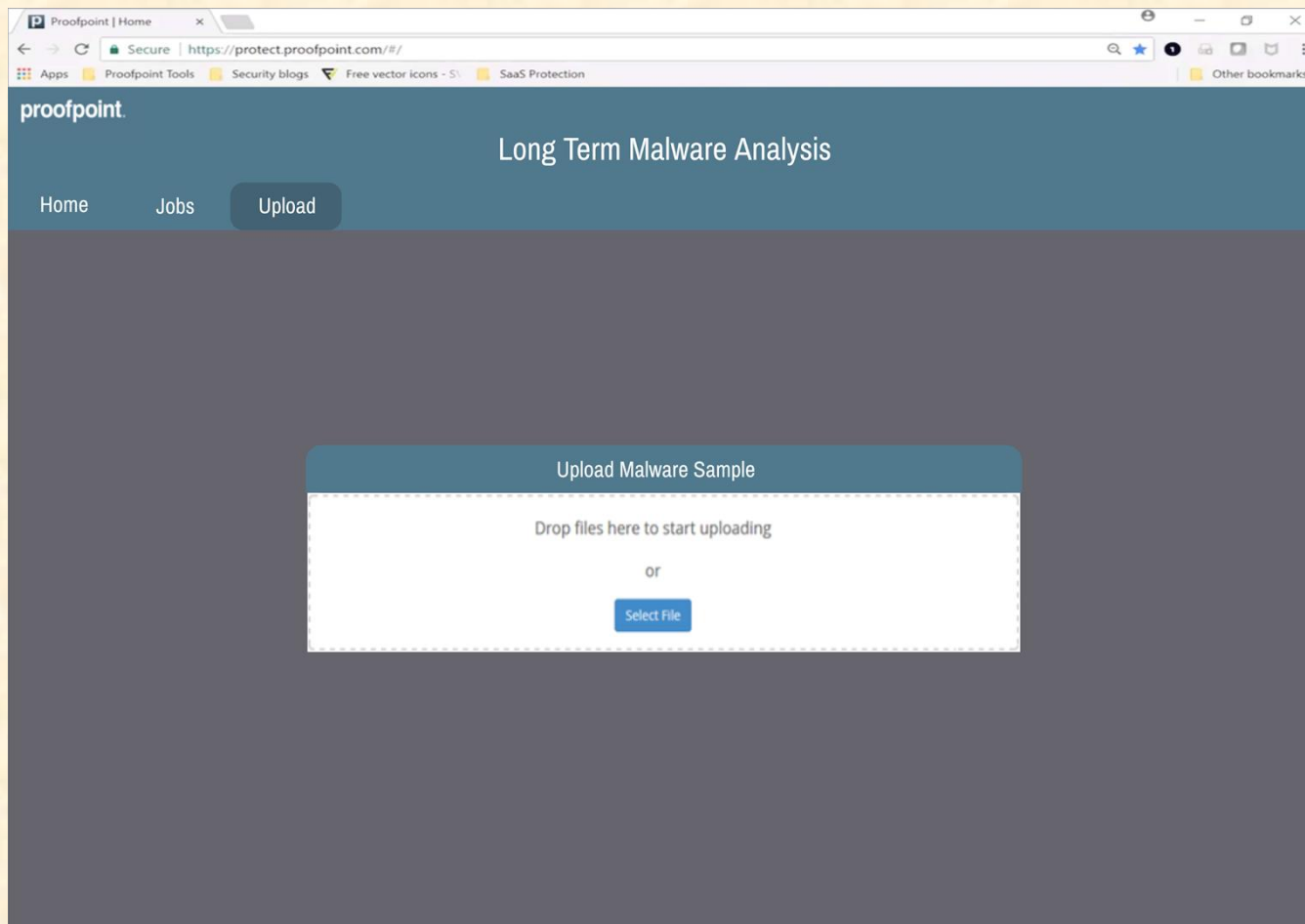
Sample	Environment	Status	Start Date	Rating
S10	Cuckoo 1	Running	12/1/19	Good
S9	Cuckoo 1	Running	12/1/19	Bad
S8	Cuckoo 1	Running	12/1/19	Good
S7	Cuckoo 2	Running	12/1/19	Good
S6	Cuckoo 2	Running	12/1/19	Moderate
S5	Cuckoo 3	Running	12/1/19	Bad
S4	Cuckoo 4	Finished	12/1/19	Moderate
S3	Cuckoo 4	Finished	12/1/19	Bad
S2	Cuckoo 5	Finished	12/1/19	Bad
S1	Cuckoo 6	Finished	12/1/19	Good



# Screen Mockup: Individual Job



# Screen Mockup: Upload Page



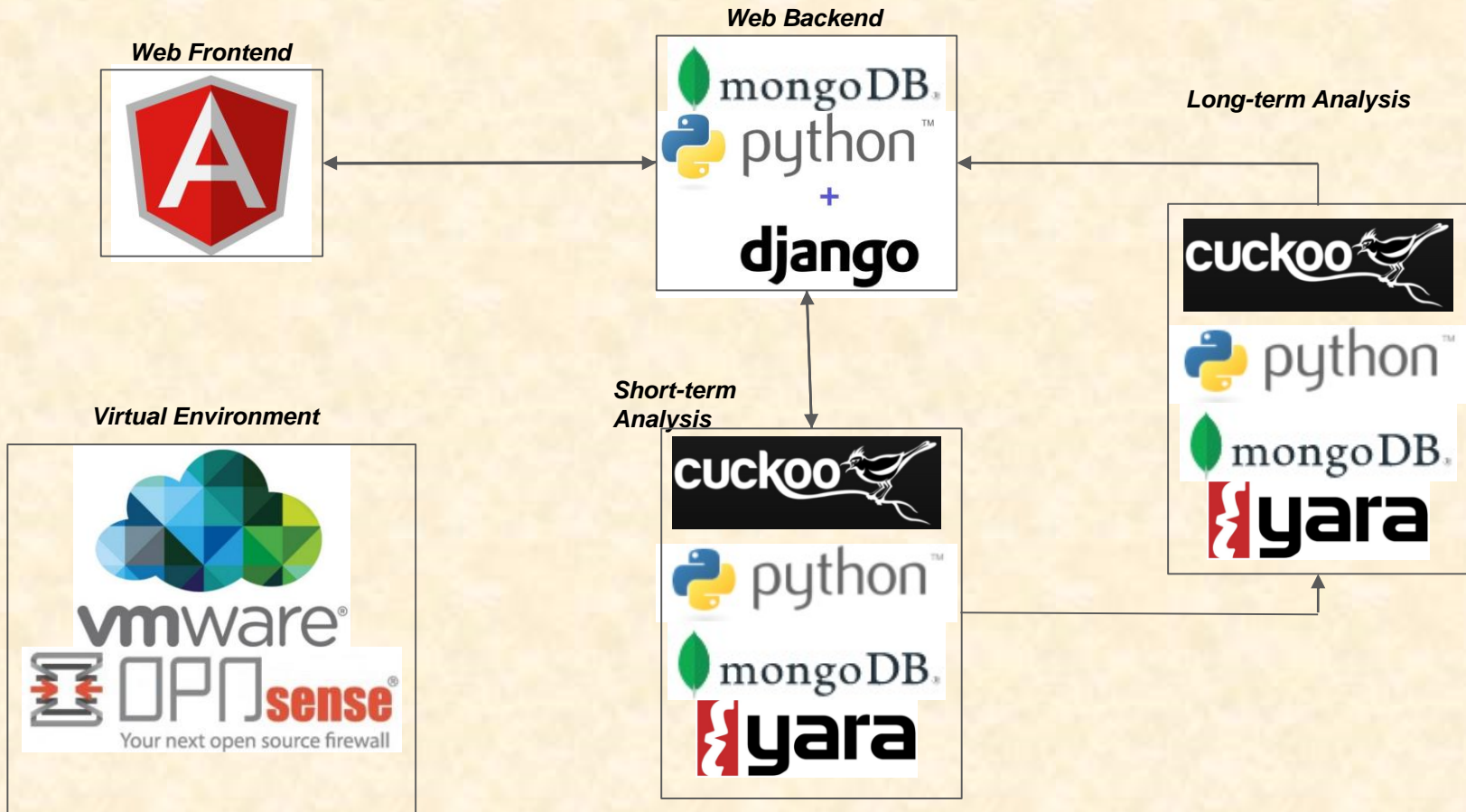
# Technical Specifications

---

- Frontend consists of a dashboard style web app made in Angular 2+. It will use data collected from the Cuckoo sandboxes.
- Web server running on windows virtual machine in VMware ESXi provided by Proofpoint
- Python backend using Django and MongoDB
- Malware classification using Cuckoo and Yara



# System Architecture



# System Components

- Hardware Platforms
  - Proofpoint server system
  - Capstone Macs
  - Windows VMs
- Software Platforms / Technologies
  - Frontend: Angular, Javascript
  - Backend: Cuckoo, MongoDB, OPNsense, Yara, Python
  - Virtualization: VMware ESXi

# Risks

- Mis-categorization Error
  - Mis-categorize as unique and waste analysis resources
  - Implement pre-check system using Yara and Cuckoo
- Cuckoo API Integration
  - Team unfamiliar with Cuckoo API and how Cuckoo logs
  - Will use a practice environment for log parser/automation
- Malware Unpredictability
  - Malware is unpredictable/dangerous with internet access
  - Use OPNsense with Proofpoint rule set
- Rushed Timeline
  - Need to complete project 1 month early to gather data
  - Stick to strict schedule



# Questions?

---

?

?

?

?

?

?

?

?

?

