

MICHIGAN STATE

UNIVERSITY

Beta Presentation
Predictive Engine for Long-Term
Malware Detonation
The Capstone Experience

Team Proofpoint

Izzy Dove

Sam Gendelman

Alex Kendall

Joshua Wilson

Geoffrey Witherington-Perkins

Department of Computer Science and Engineering
Michigan State University
Spring 2020



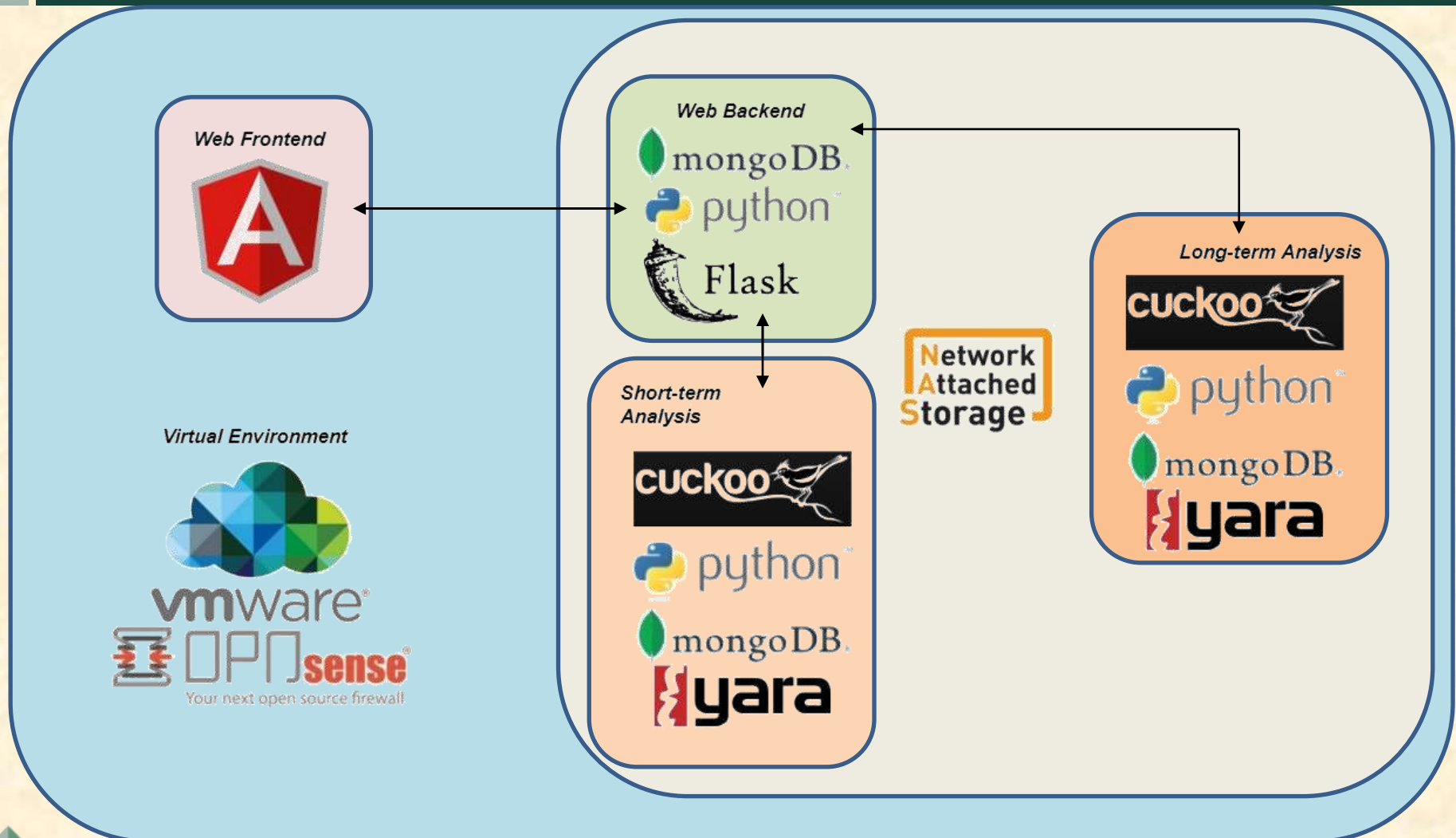
From Students...
...to Professionals

Project Overview

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



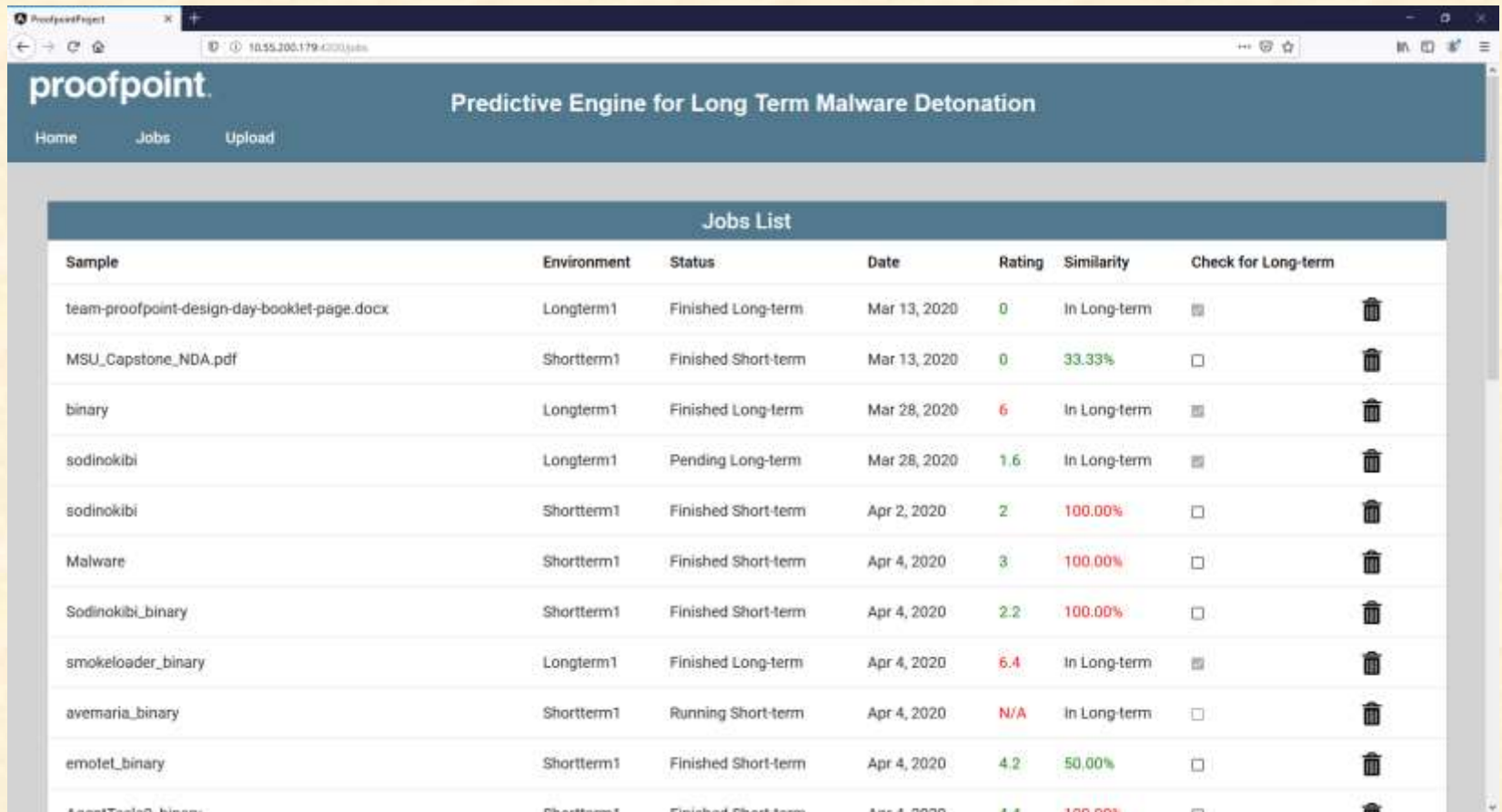
System Architecture



Dashboard



Jobs List

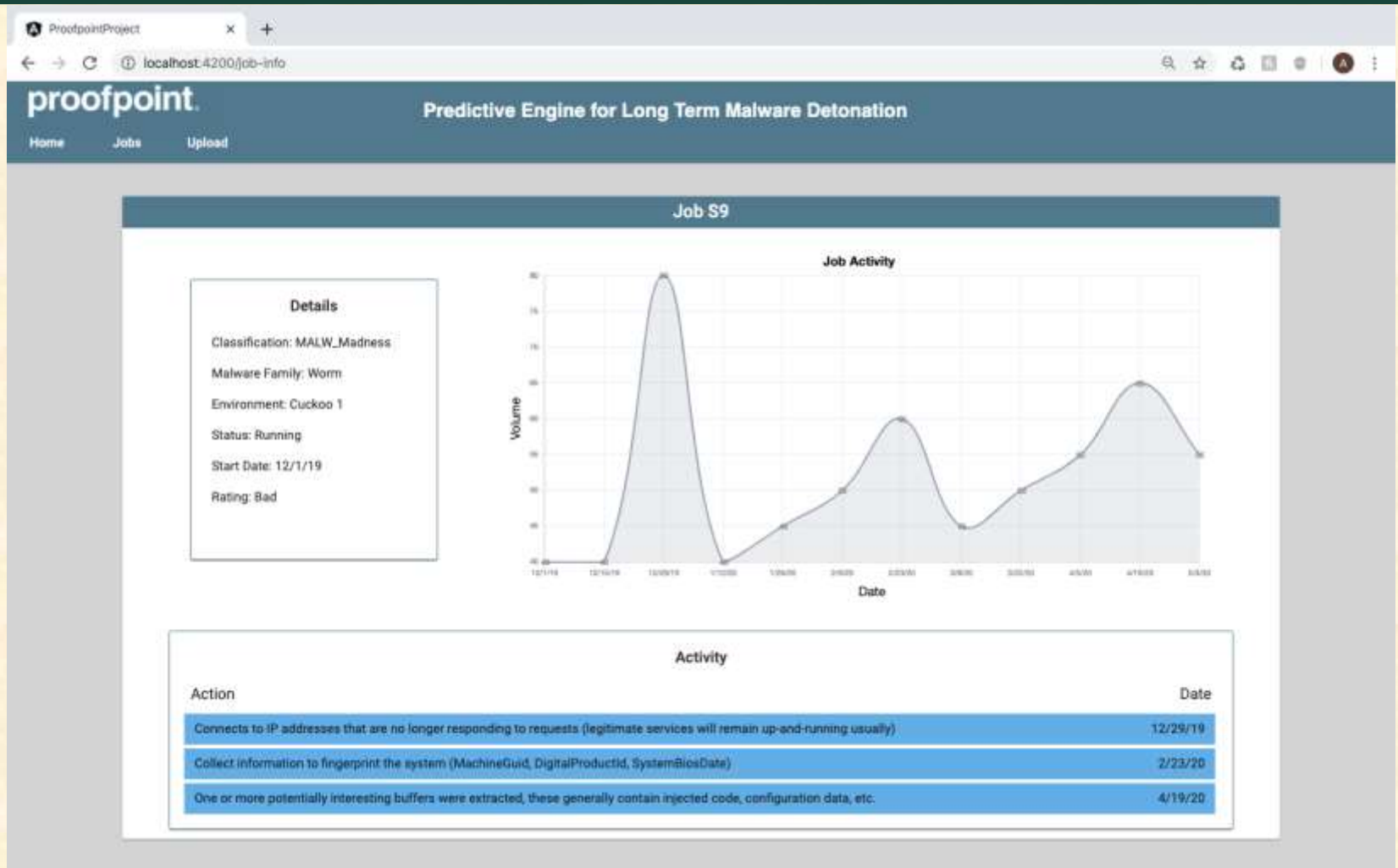


The screenshot shows a web browser window with the URL 10.55.200.179:4200/jobs. The page title is "proofpoint Predictive Engine for Long Term Malware Detonation". The navigation menu includes "Home", "Jobs", and "Upload". The main content area is titled "Jobs List" and contains a table with the following columns: Sample, Environment, Status, Date, Rating, Similarity, and Check for Long-term. The table lists various samples with their corresponding environments, statuses, dates, ratings, and similarity percentages.

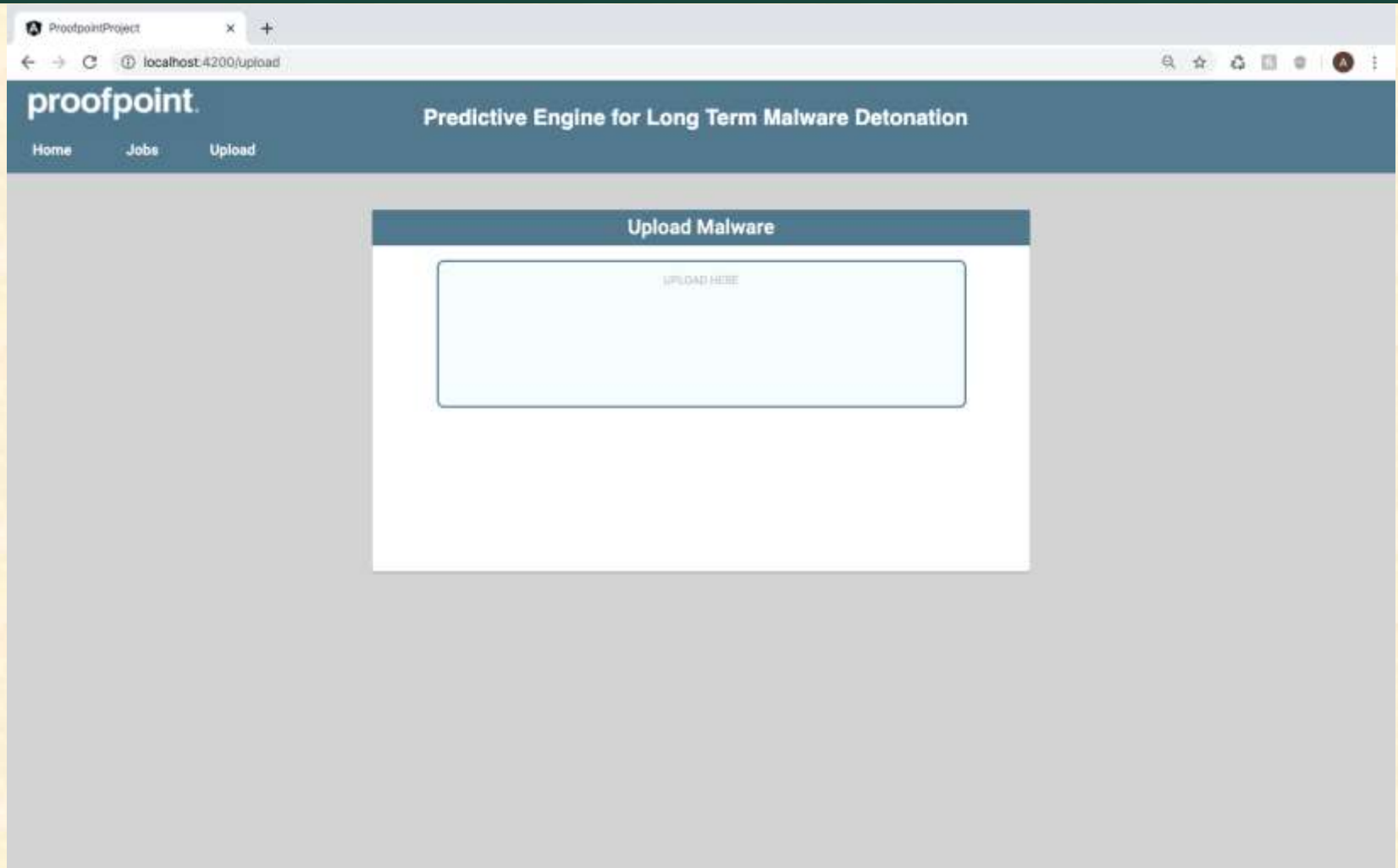
Sample	Environment	Status	Date	Rating	Similarity	Check for Long-term
team-proofpoint-design-day-booklet-page.docx	Longterm1	Finished Long-term	Mar 13, 2020	0	In Long-term	<input checked="" type="checkbox"/>
MSU_Capstone_NDA.pdf	Shortterm1	Finished Short-term	Mar 13, 2020	0	33.33%	<input type="checkbox"/>
binary	Longterm1	Finished Long-term	Mar 28, 2020	6	In Long-term	<input checked="" type="checkbox"/>
sodinokibi	Longterm1	Pending Long-term	Mar 28, 2020	1.6	In Long-term	<input checked="" type="checkbox"/>
sodinokibi	Shortterm1	Finished Short-term	Apr 2, 2020	2	100.00%	<input type="checkbox"/>
Malware	Shortterm1	Finished Short-term	Apr 4, 2020	3	100.00%	<input type="checkbox"/>
Sodinokibi_binary	Shortterm1	Finished Short-term	Apr 4, 2020	2.2	100.00%	<input type="checkbox"/>
smokeloader_binary	Longterm1	Finished Long-term	Apr 4, 2020	6.4	In Long-term	<input checked="" type="checkbox"/>
avemaria_binary	Shortterm1	Running Short-term	Apr 4, 2020	N/A	In Long-term	<input type="checkbox"/>
emotel_binary	Shortterm1	Finished Short-term	Apr 4, 2020	4.2	50.00%	<input type="checkbox"/>
AvastTool0_binary	Shortterm1	Finished Short-term	Apr 4, 2020	4.4	100.00%	<input type="checkbox"/>



Individual Job



Individual Job



What's left to do?

- Fine-tune similarity checking algorithm
- Bug fixes
- Improvements to front end
- Wrap-up live updating
- Finish implementing our own malware queue



Questions?

?

?

?

?

?

?

?

?

?

