MICHIGAN STATE UNIVERSITY

Alpha Presentation

AMAP

The Capstone Experience

Accenture

Andrew Mitchell
Teng Xu
Griffin Metevia
Julian Ellis
Sam Kling

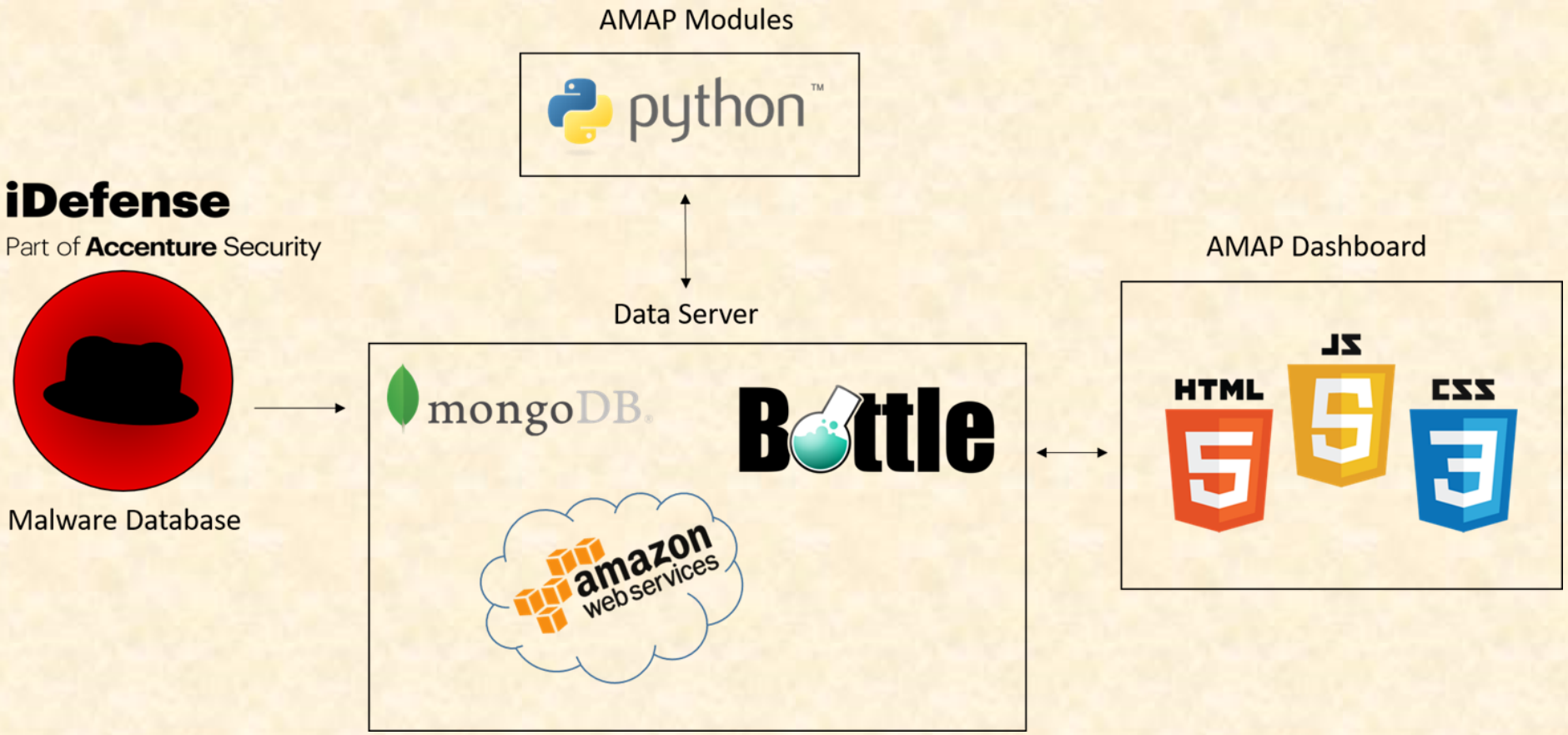
From Students…
…to Professionals

Department of Computer Science and Engineering
Michigan State University
Spring 2018

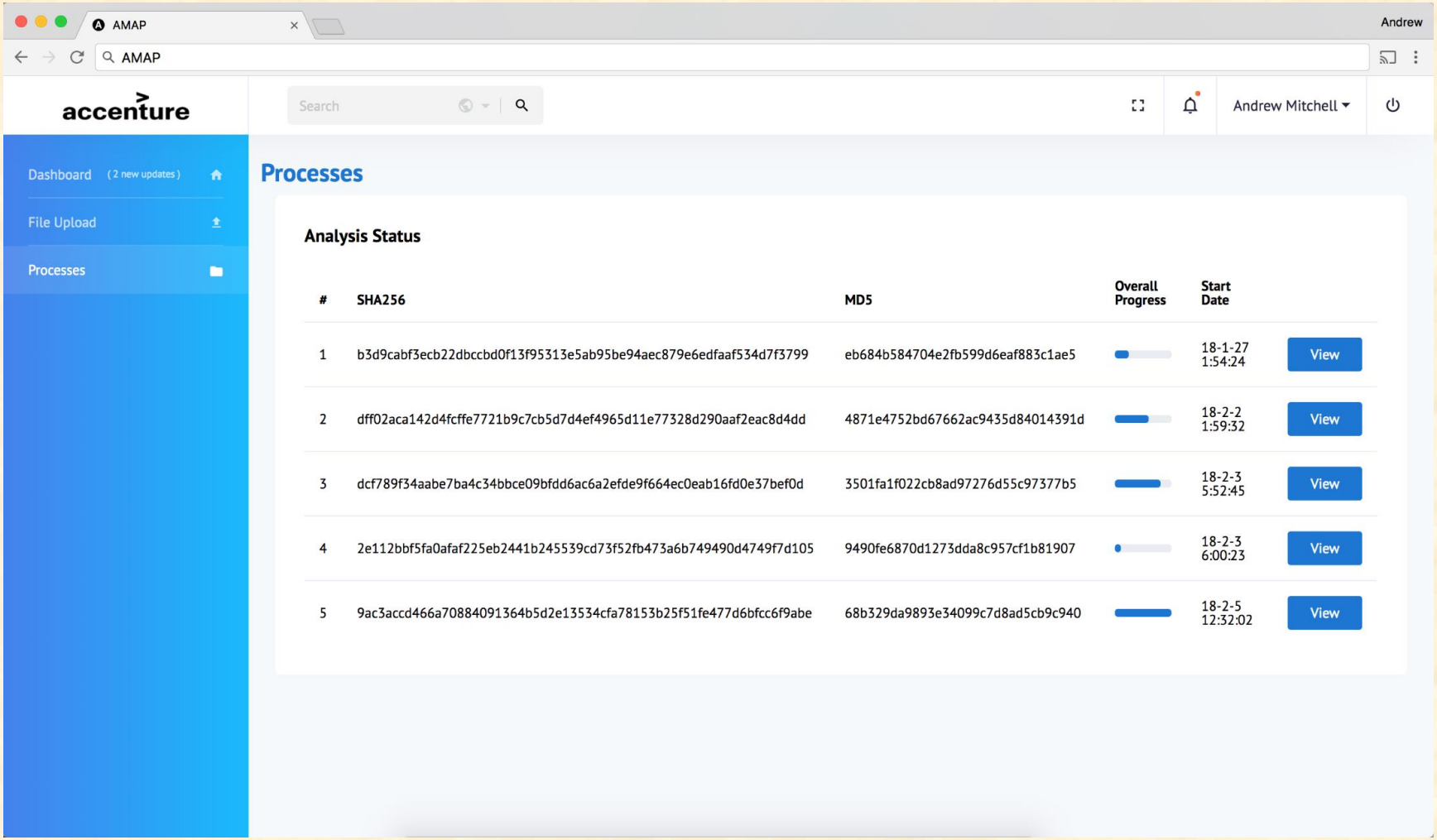
Project Overview

- Automated Malware Analysis
- Wizard Style UI
- High Volume Testing in Multithreaded Environment

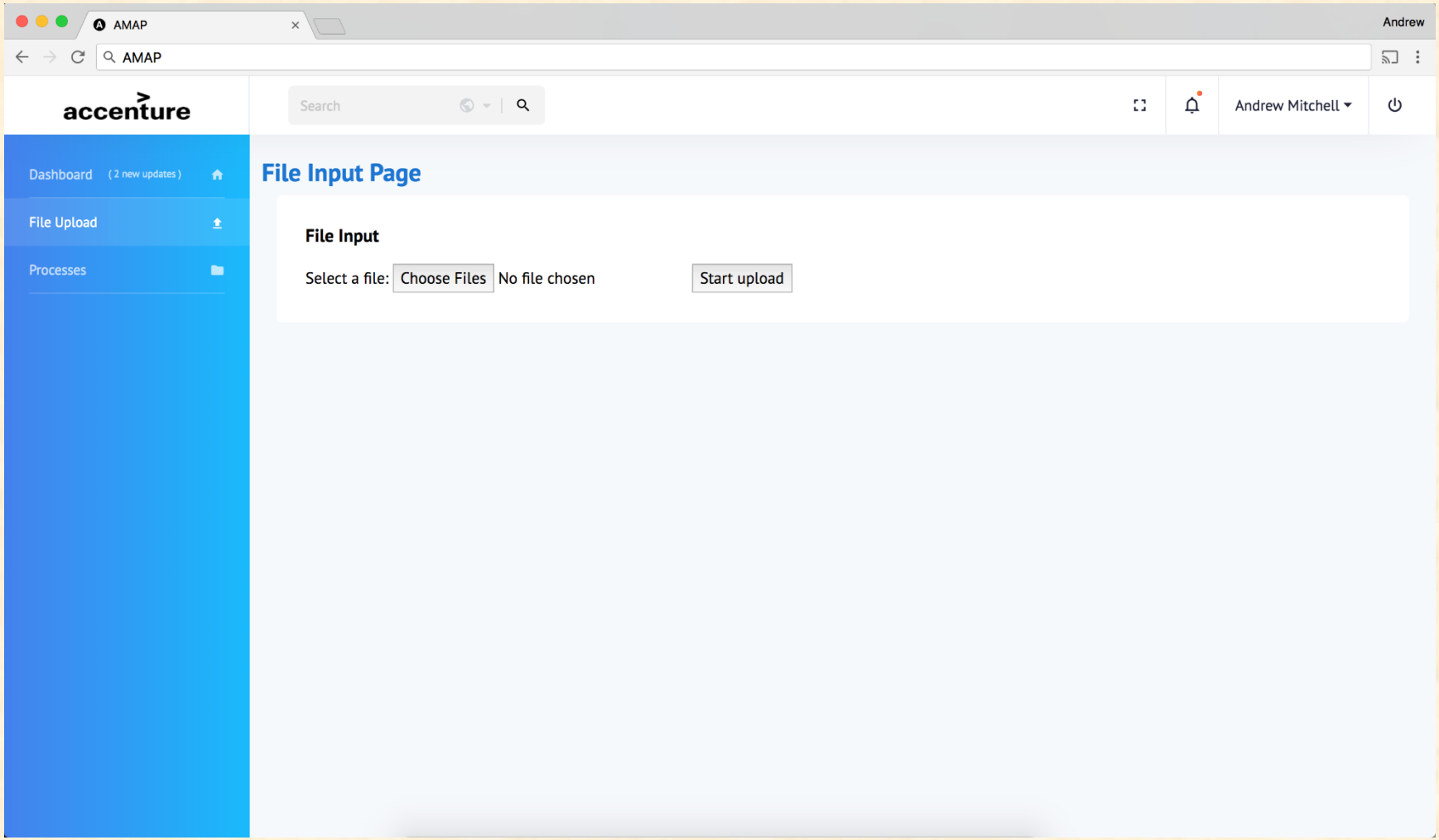
System Architecture



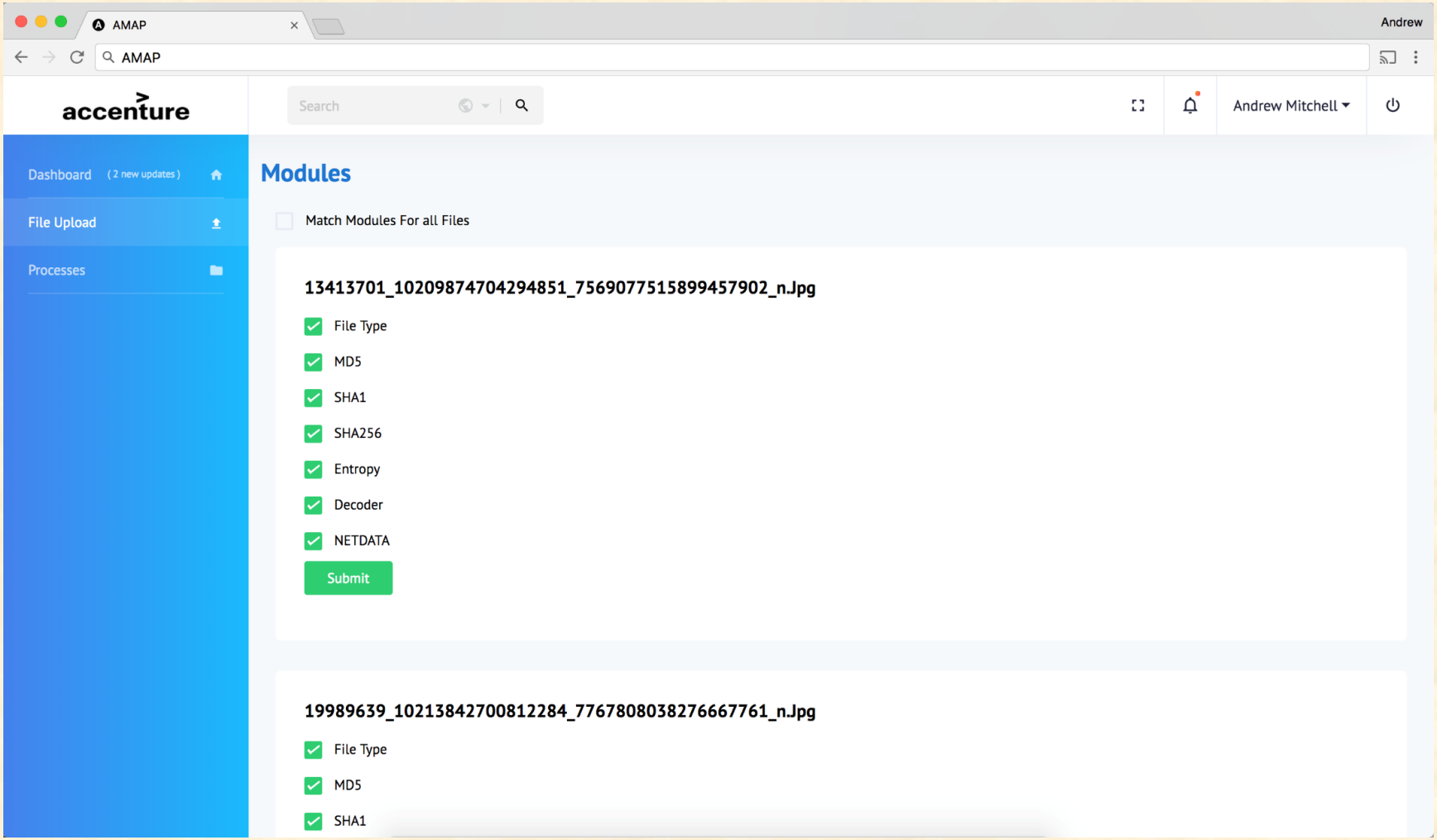
Current Process Status Page



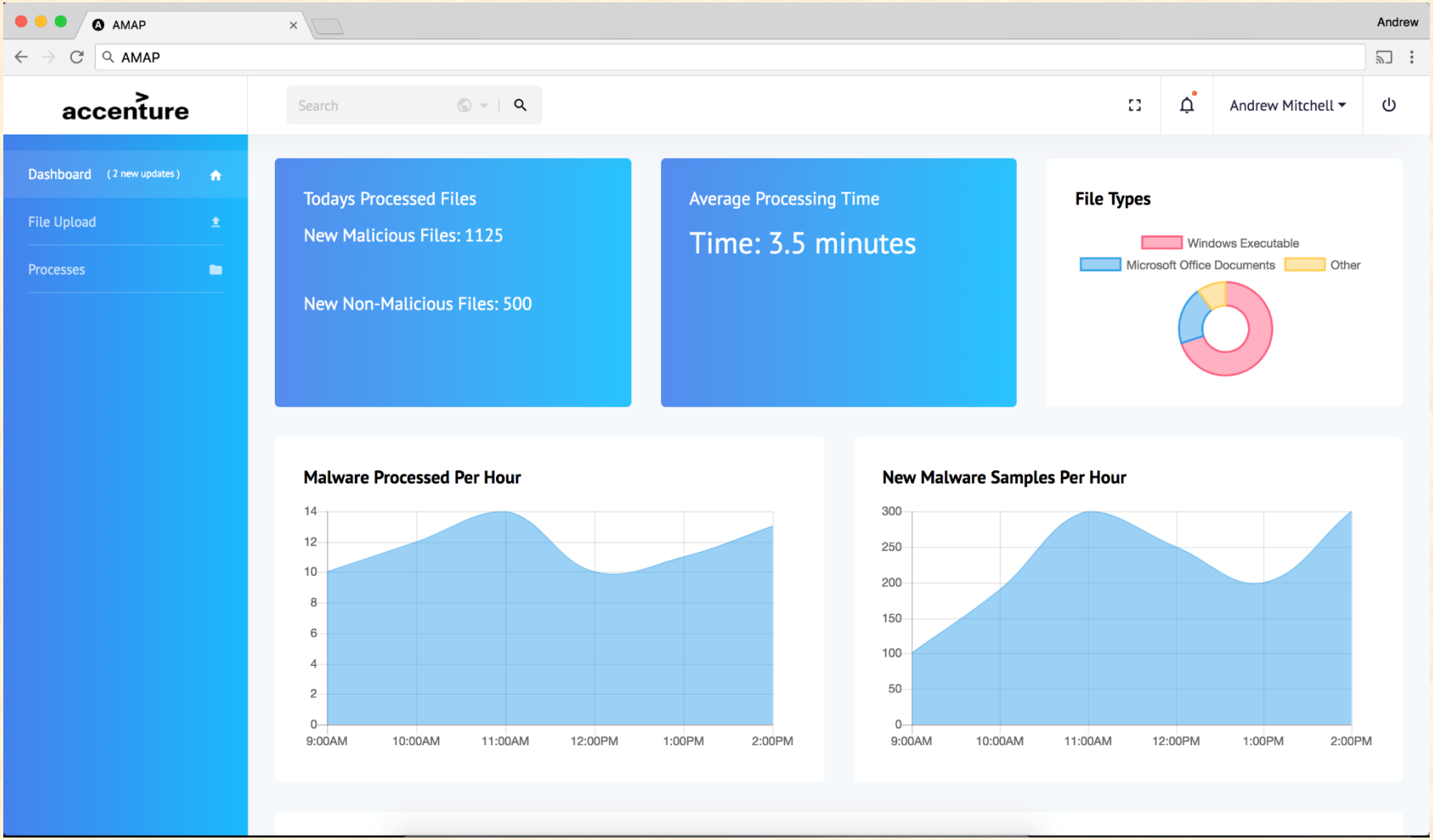
File Upload


AMAP
Andrew
AMAP
accenture
Search
Andrew Mitchell
Dashboard (2 new updates)
File Upload
Processes
File Input Page
File Input
Select a file: Choose Files No file chosen
Start upload

Module Selection Page



Dashboard


AMAP
Andrew
AMAP
accenture
Search
Andrew Mitchell
Dashboard (2 new updates)
File Upload
Processes
Todays Processed Files
New Malicious Files: 1125
New Non-Malicious Files: 500
Average Processing Time
Time: 3.5 minutes
File Types
Windows Executable
Microsoft Office Documents
Other
Malware Processed Per Hour
14
12
10
8
6
4
2
0
9:00AM
10:00AM
11:00AM
12:00PM
1:00PM
2:00PM
New Malware Samples Per Hour
300
250
200
150
100
50
0
9:00AM
10:00AM
11:00AM
12:00PM
1:00PM
2:00PM

What's left to do?

- Add More Dynamic Analysis Modules
- Add More Information to Dashboard Page
- Create Login Page
- Write and Pull Malware Information to/from iDefense Database

Questions?