MICHIGAN STATE
UNIVERSITY

Beta Presentation
AMAP

The Capstone Experience

Team Accenture

Andrew Mitchell
Teng Xu
Griffin Metevia
Julian Ellis
Sam Kling

Department of Computer Science and Engineering
Michigan State University

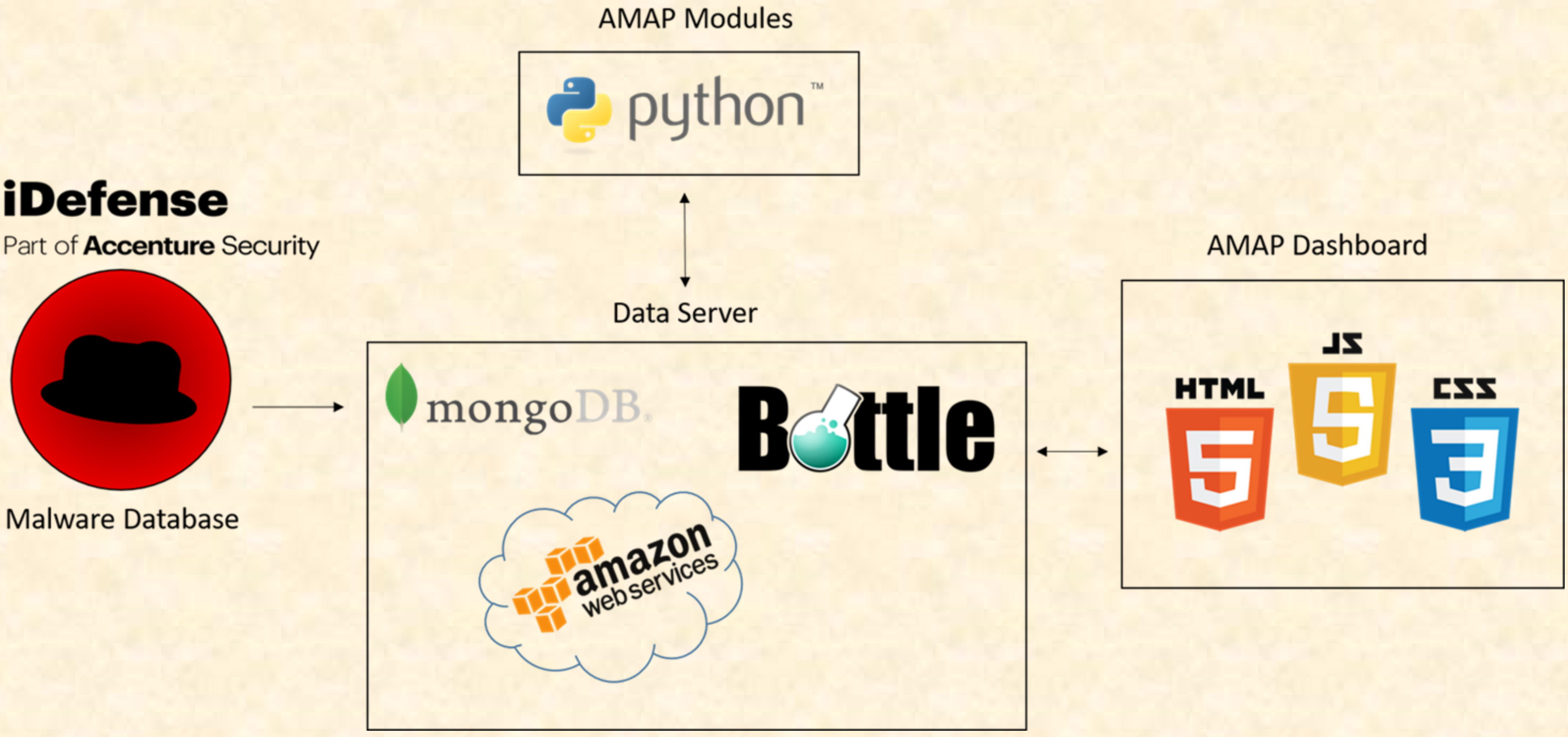
Spring 2018

From Students…
…to Professionals

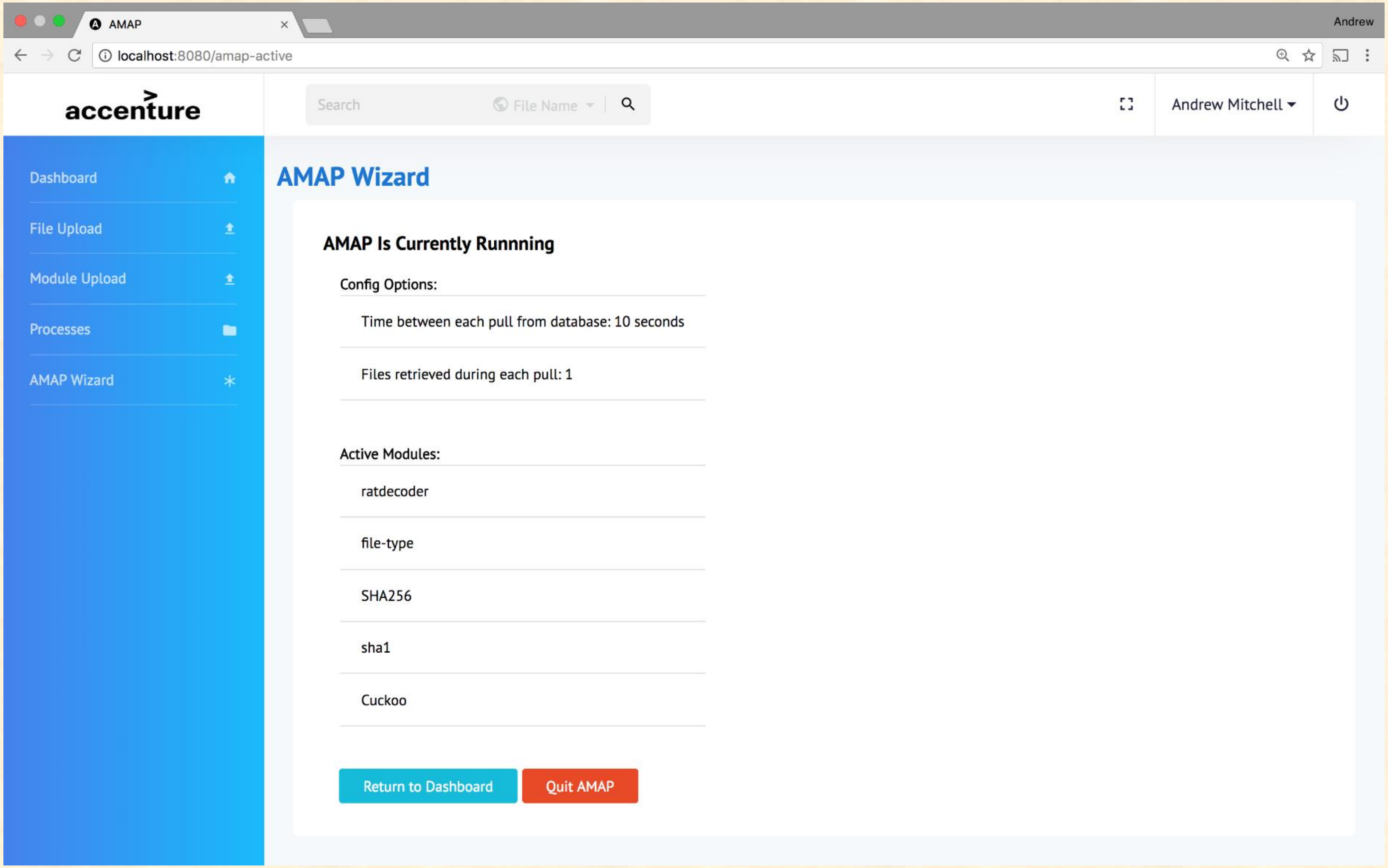
Project Overview

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

System Architecture



AMAP Wizard



AMAP Wizard

AMAP Is Currently Runnning

Config Options:

Time between each pull from database: 10 seconds

Files retrieved during each pull: 1

Active Modules:

ratdecoder

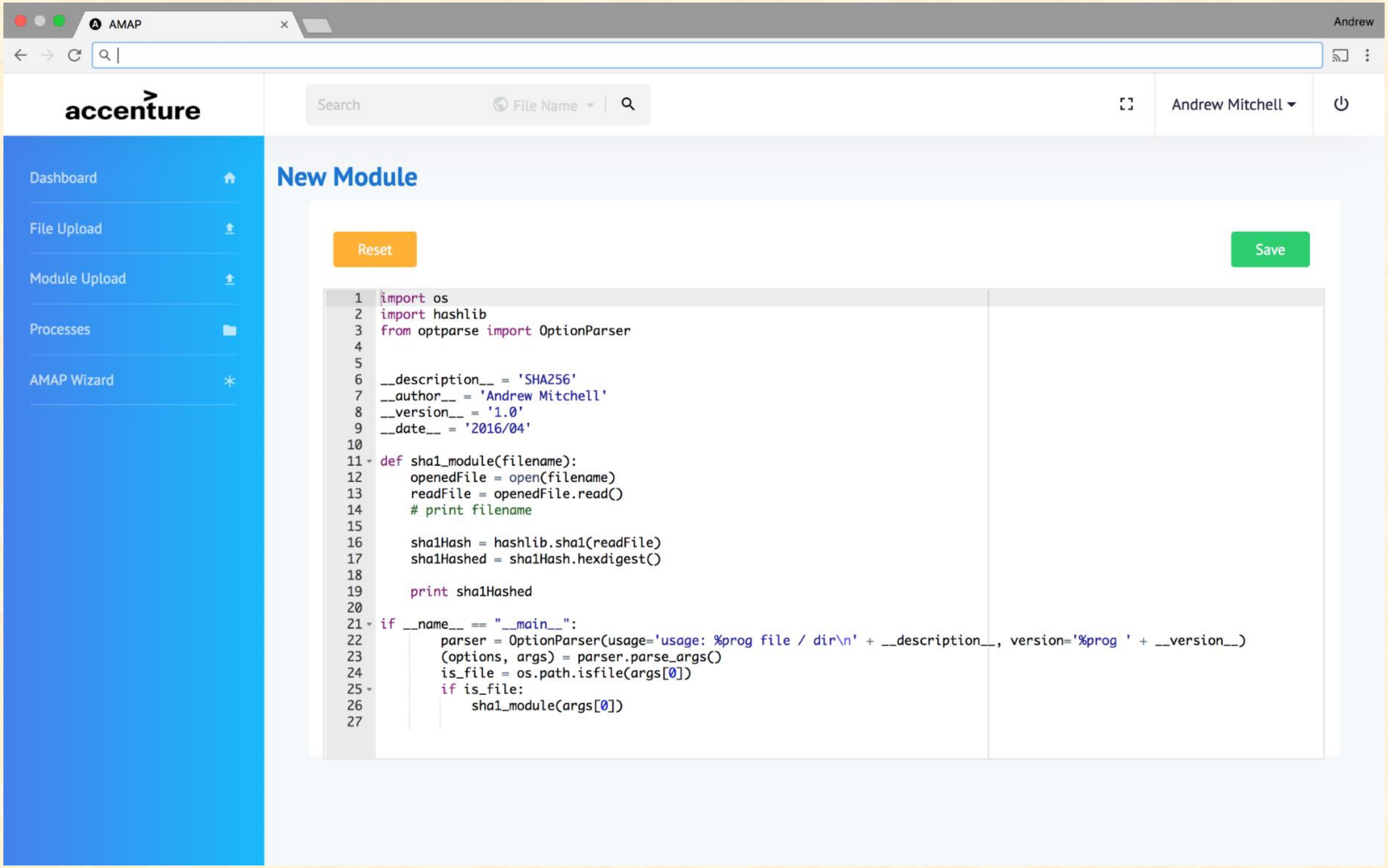
file-type

SHA256

sha1

Cuckoo

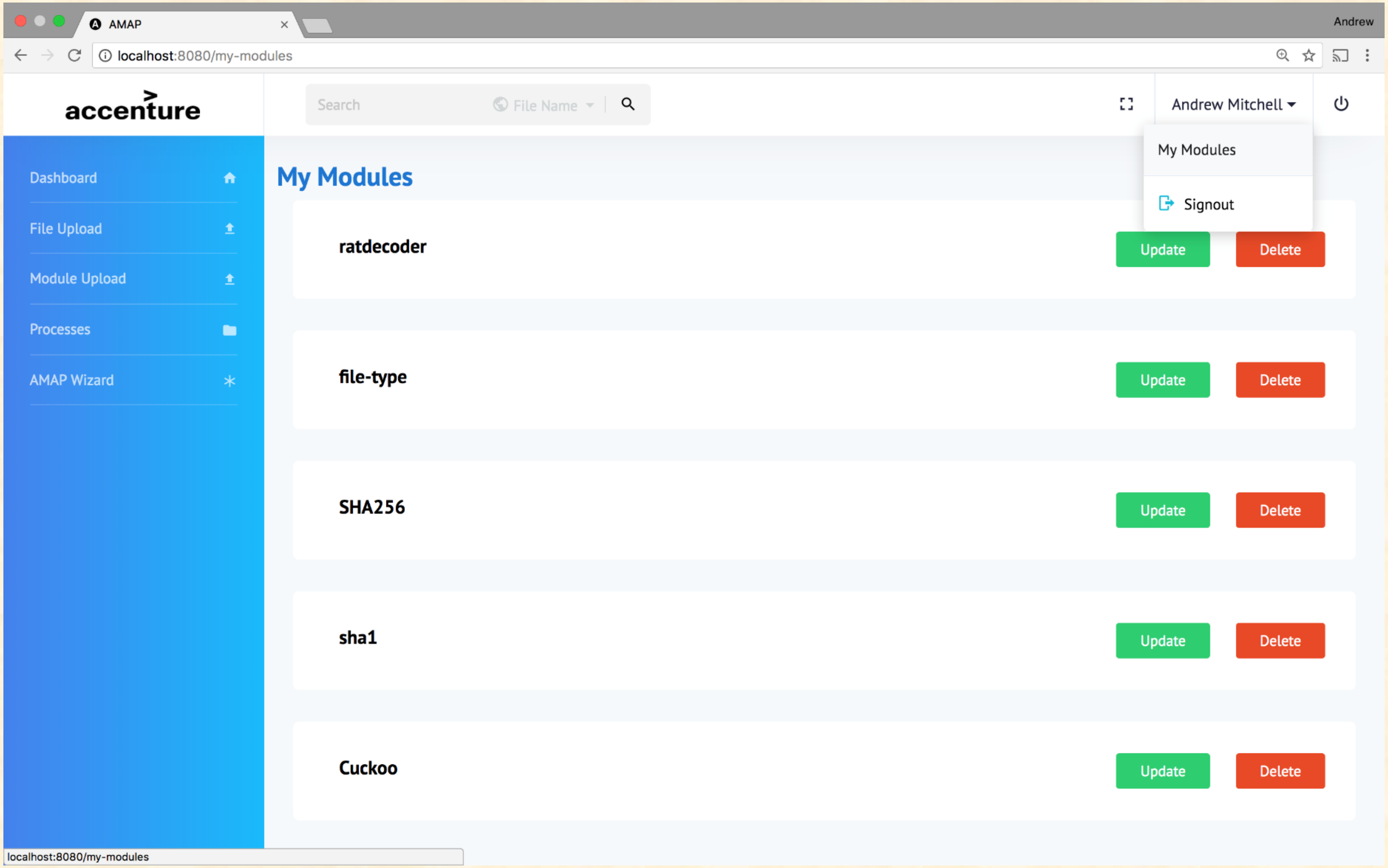
New Module Creator



New Module

```
import os
import hashlib
from optparse import OptionParser


__description__ = 'SHA256'
__author__ = 'Andrew Mitchell'
__version__ = '1.0'
__date__ = '2016/04'

def sha1_module(filename):
    openedFile = open(filename)
    readFile = openedFile.read()
    # print filename

    sha1Hash = hashlib.sha1(readFile)
    sha1Hashed = sha1Hash.hexdigest()

    print sha1Hashed

if __name__ == "__main__":
        parser = OptionParser(usage='usage: %prog file / dir\n' + __description__, version='%prog ' + __version__)
        (options, args) = parser.parse_args()
        is_file = os.path.isfile(args[0])
        if is_file:
            sha1_module(args[0])

```

My Modules Page



My Modules

ratdecoder Update Delete

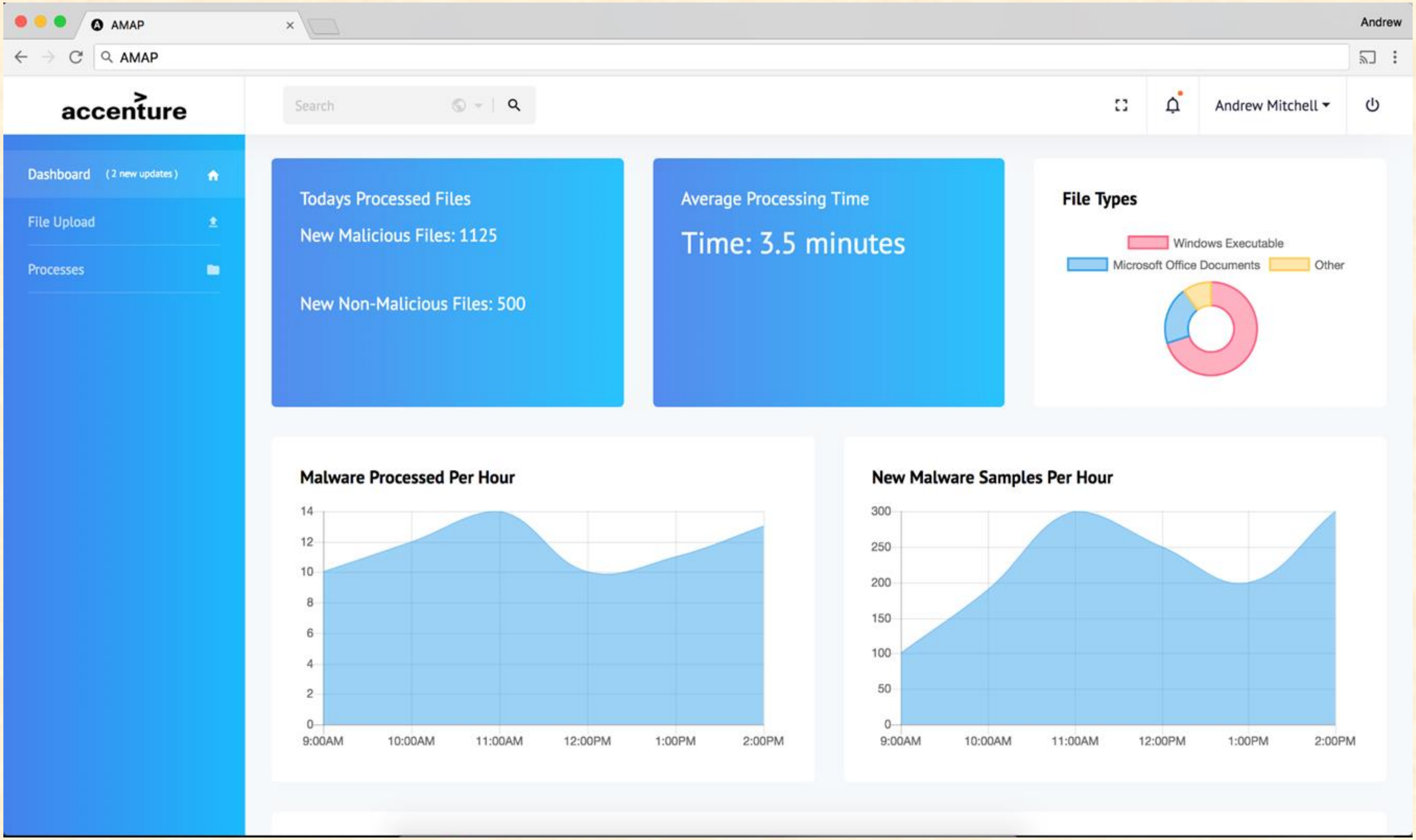
file-type Update Delete

SHA256 Update Delete

sha1 Update Delete

Cuckoo Update Delete

AMAP Dashboard



Todays Processed Files

New Malicious Files: 1125

New Non-Malicious Files: 500

Average Processing Time

Time: 3.5 minutes

File Types

Malware Processed Per Hour

New Malware Samples Per Hour

What’s left to do?

- Polish UI
- Test Compatibility with Other Modules
- Project Video

Questions?

? ? ? ?

? ?

? ? ?