

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



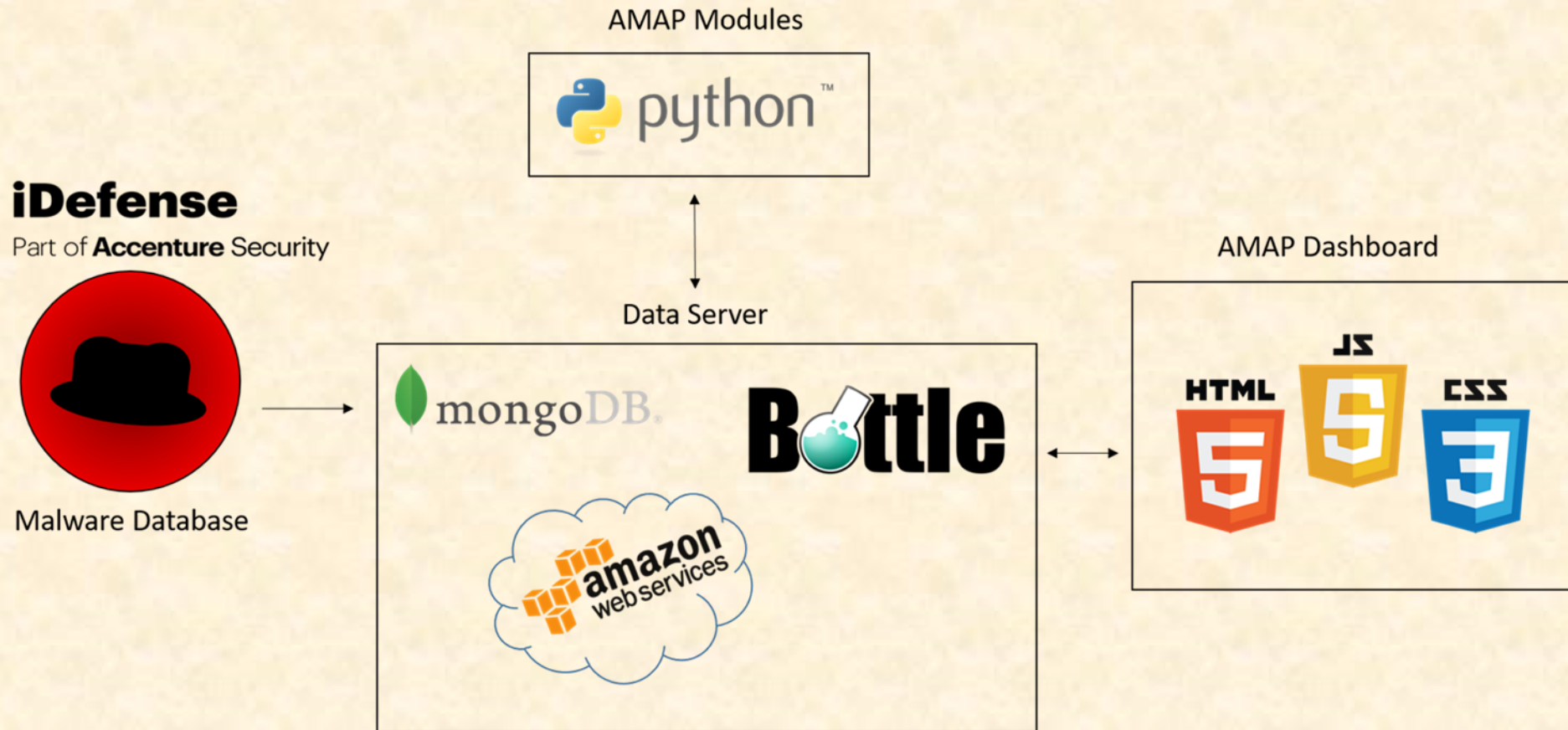
*From Students...
...to Professionals*

Project Overview

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



System Architecture



AMAP Wizard

The screenshot displays the AMAP Wizard web interface in a browser window. The browser's address bar shows the URL `localhost:8080/amap-active`. The interface features a blue sidebar on the left with the Accenture logo and navigation links for Dashboard, File Upload, Module Upload, Processes, and AMAP Wizard. The main content area is titled "AMAP Wizard" and displays the status "AMAP Is Currently Running". Under "Config Options", the settings are: "Time between each pull from database: 10 seconds" and "Files retrieved during each pull: 1". Under "Active Modules", the listed modules are: ratdecoder, file-type, SHA256, sha1, and Cuckoo. At the bottom of the main area, there are two buttons: "Return to Dashboard" and "Quit AMAP".



New Module Creator

The screenshot displays the AMAP (Accenture Module Automation Platform) interface. The top navigation bar includes the Accenture logo, a search bar, a "File Name" dropdown, and a user profile for "Andrew Mitchell". The left sidebar contains navigation options: Dashboard, File Upload, Module Upload, Processes, and AMAP Wizard. The main content area is titled "New Module" and features a "Reset" button and a "Save" button. The central code editor contains the following Python code:

```
1 import os
2 import hashlib
3 from optparse import OptionParser
4
5
6 __description__ = 'SHA256'
7 __author__ = 'Andrew Mitchell'
8 __version__ = '1.0'
9 __date__ = '2016/04'
10
11 def sha1_module(filename):
12     openedFile = open(filename)
13     readfile = openedFile.read()
14     # print filename
15
16     sha1Hash = hashlib.sha1(readfile)
17     sha1Hashed = sha1Hash.hexdigest()
18
19     print sha1Hashed
20
21 if __name__ == "__main__":
22     parser = OptionParser(usage='usage: %prog file / dir\n' + __description__, version='%prog ' + __version__)
23     (options, args) = parser.parse_args()
24     is_file = os.path.isfile(args[0])
25     if is_file:
26         sha1_module(args[0])
27
```



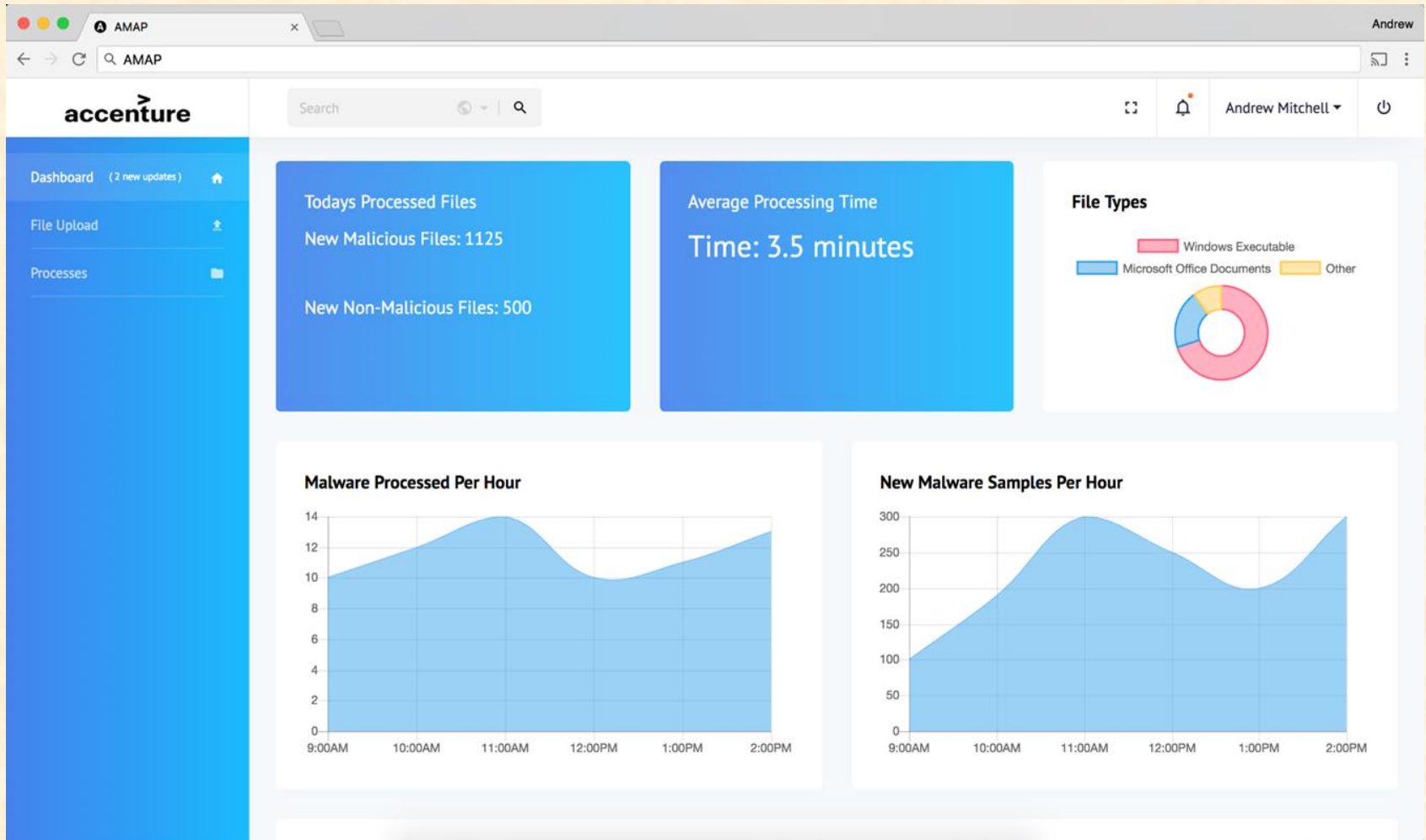
My Modules Page

The screenshot displays the 'My Modules' page in the AMAP application. The page features a sidebar with navigation options: Dashboard, File Upload, Module Upload, Processes, and AMAP Wizard. The main content area is titled 'My Modules' and contains a list of modules. Each module entry includes the module name and two action buttons: 'Update' (green) and 'Delete' (red). A user profile dropdown menu is open, showing the user's name 'Andrew Mitchell' and two options: 'My Modules' and 'Signout'.

Module Name	Update	Delete
ratdecoder	Update	Delete
file-type	Update	Delete
SHA256	Update	Delete
sha1	Update	Delete
Cuckoo	Update	Delete



AMAP Dashboard



What's left to do?

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



Questions?

?

?

?

?

?

?

?

?

?

