MICHIGAN STATE
UNIVERSITY

Project Plan
Enhanced Network Anomaly Detection Suite

The Capstone Experience

Team Rook Security

Cam Gibson
Brian Harazim
Grant Levene
Zach Rosenthal
Andrew Werner

Department of Computer Science and Engineering
Michigan State University

Fall 2016

From Students…
…to Professionals

Functional Specifications

Monitors highly-virtualized networks to detect behavior-based attacks

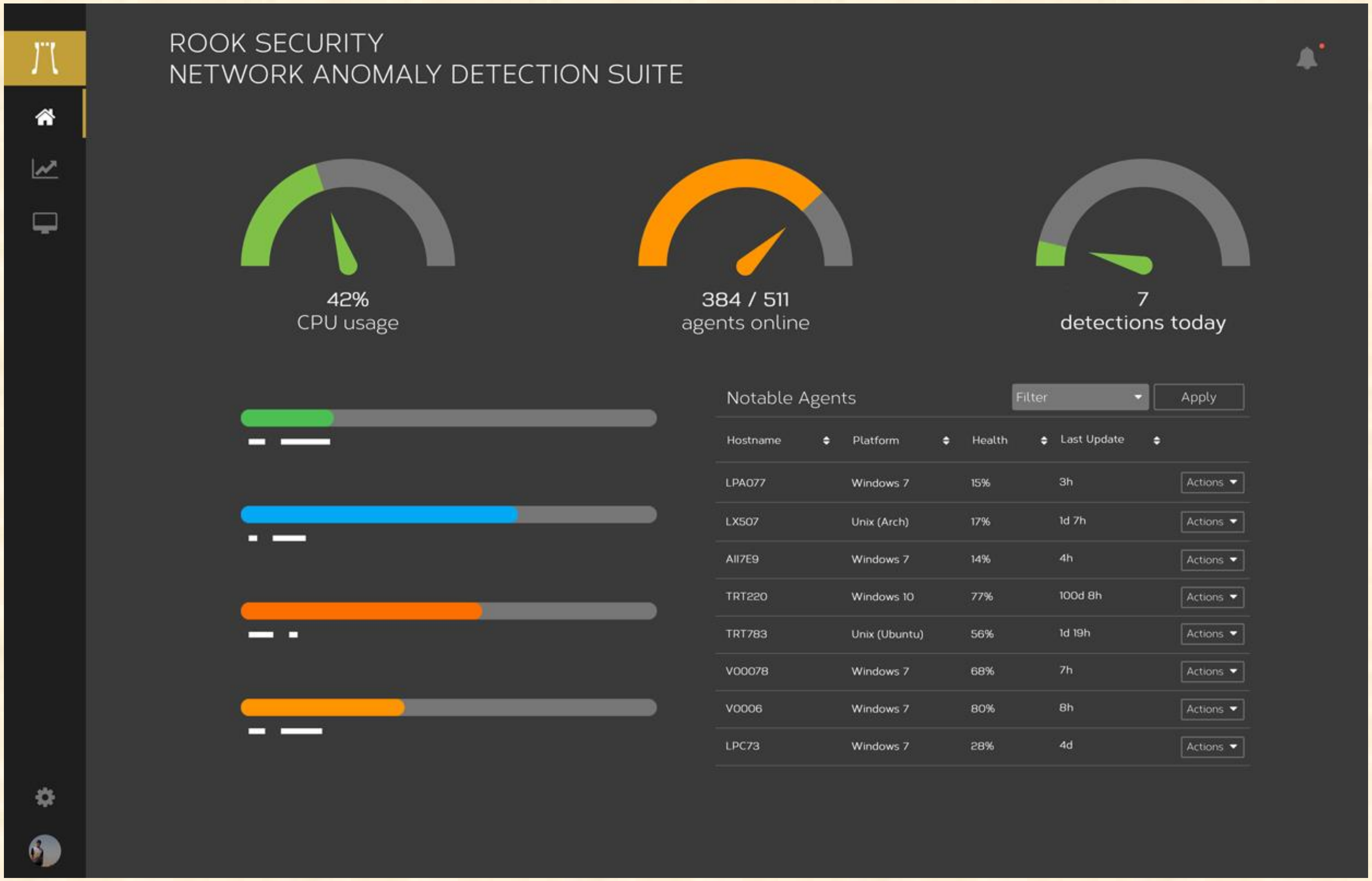
- Optimize Windows agent performance
- Improve analysis engine with machine learning
- Develop agent management console GUI
- Create Linux and OS X agent versions
- Add encryption for all communications
- Add encrypted local database to the agents

Design Specifications

Web Management Console Features

- Agent health and directory
- Host health and directory
- Anomaly alerts via email, dashboard, and push notifications
- Network statistics
- Remote agent management

Screen Mockup: Home Page



ROOK SECURITY
NETWORK ANOMALY DETECTION SUITE

42%
CPU usage

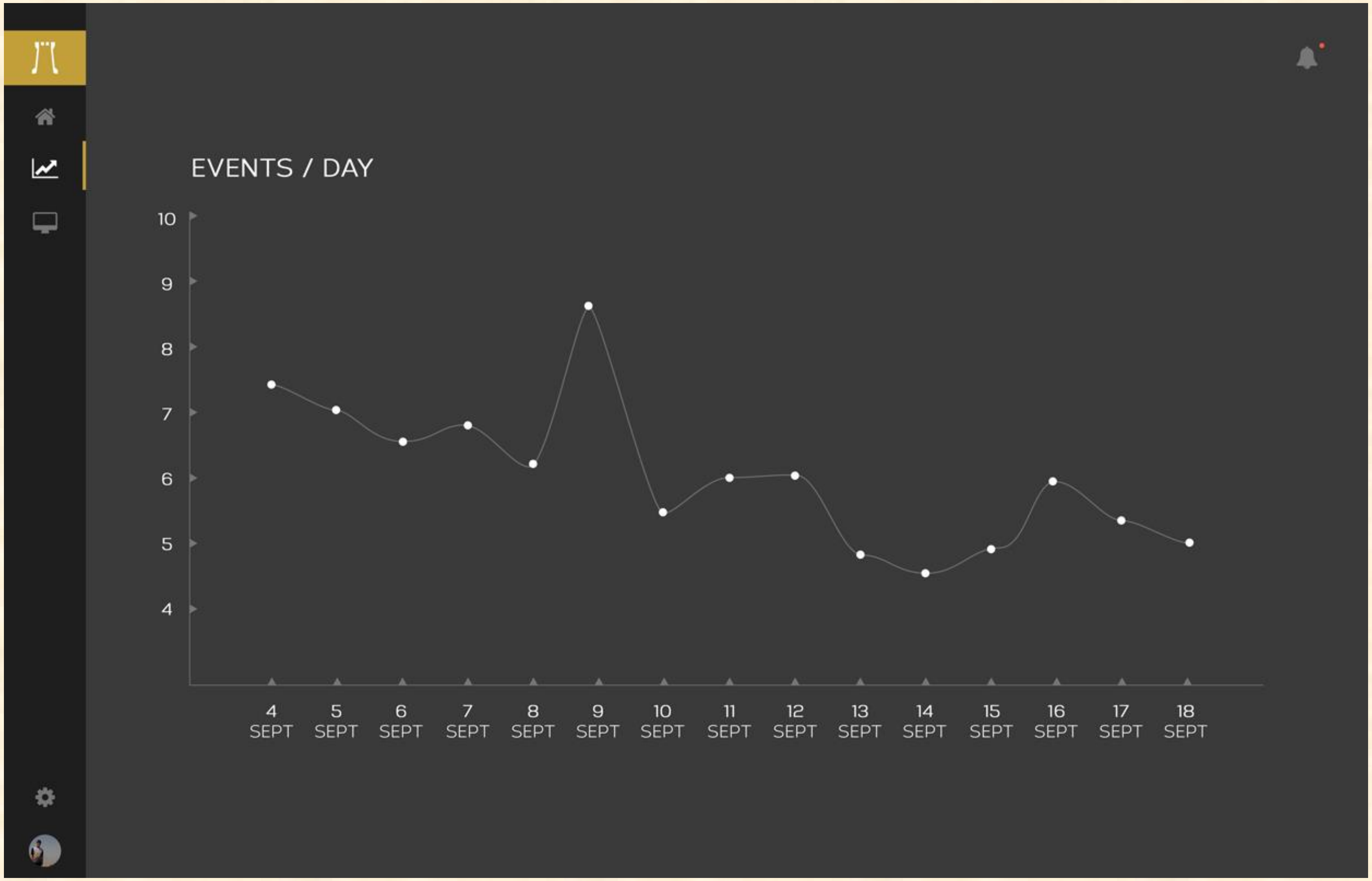
384 / 511
agents online

7
detections today

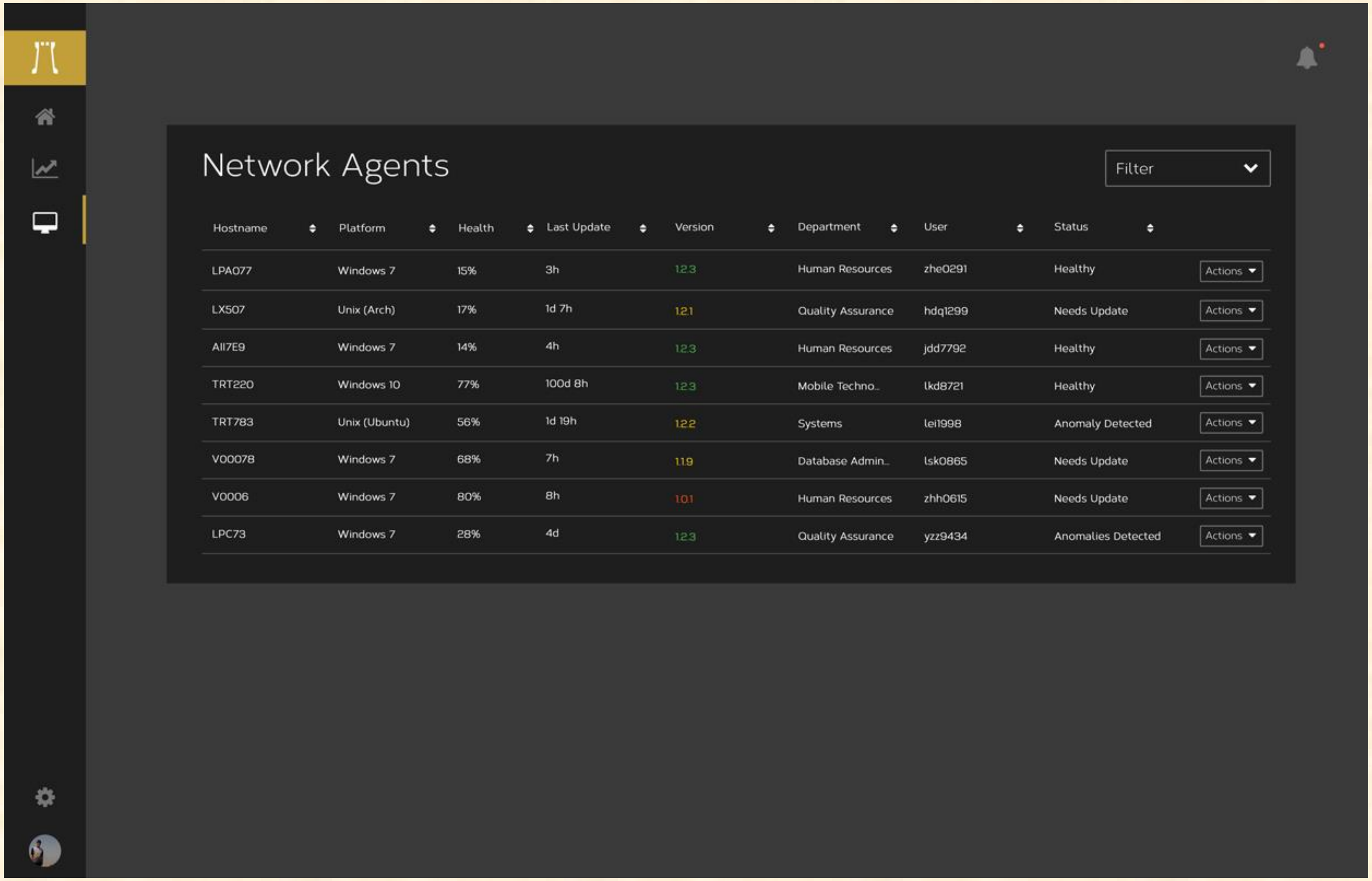
Notable Agents

Hostname	Platform	Health	Last Update	
LPA077	Windows 7	15%	3h	Actions
LX507	Unix (Arch)	17%	1d 7h	Actions
AII7E9	Windows 7	14%	4h	Actions
TRT220	Windows 10	77%	100d 8h	Actions
TRT783	Unix (Ubuntu)	56%	1d 19h	Actions
V00078	Windows 7	68%	7h	Actions
V0006	Windows 7	80%	8h	Actions
LPC73	Windows 7	28%	4d	Actions

Screen Mockup: Data Visualization



Screen Mockup: Agent Management



Network Agents

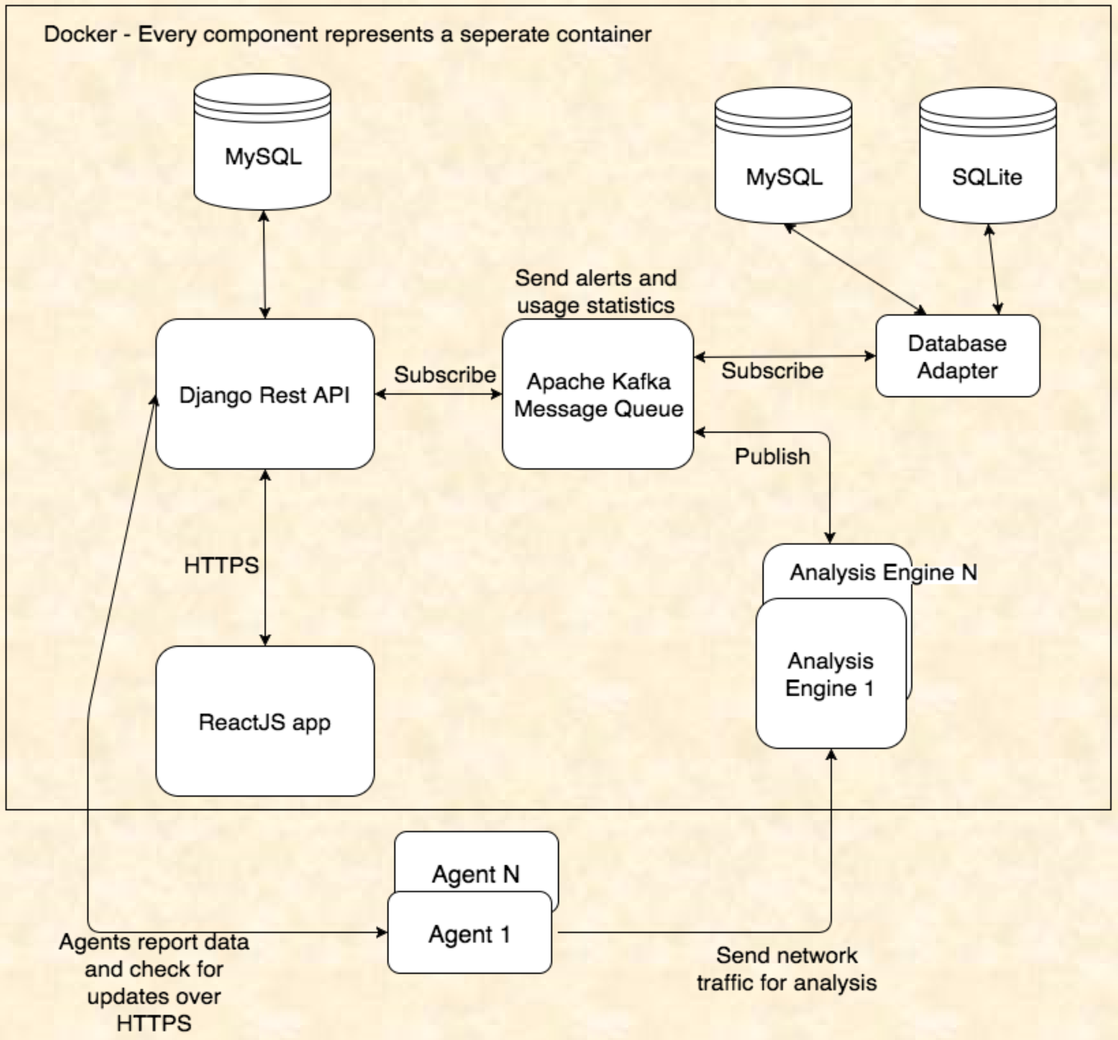
Filter

Hostname	Platform	Health	Last Update	Version	Department	User	Status	
LPA077	Windows 7	15%	3h	1.2.3	Human Resources	zhe0291	Healthy	Actions
LX507	Unix (Arch)	17%	1d 7h	1.2.1	Quality Assurance	hdq1299	Needs Update	Actions
All7E9	Windows 7	14%	4h	1.2.3	Human Resources	jdd7792	Healthy	Actions
TRT220	Windows 10	77%	100d 8h	1.2.3	Mobile Techno...	lkd8721	Healthy	Actions
TRT783	Unix (Ubuntu)	56%	1d 19h	1.2.2	Systems	lei1998	Anomaly Detected	Actions
V00078	Windows 7	68%	7h	1.1.9	Database Admin...	lsk0865	Needs Update	Actions
V0006	Windows 7	80%	8h	1.0.1	Human Resources	zhh0615	Needs Update	Actions
LPC73	Windows 7	28%	4d	1.2.3	Quality Assurance	yzz9434	Anomalies Detected	Actions

Technical Specifications

- Management Console
  - Frontend: ReactJS
  - Backend: Django Rest Framework
  - Message Queue: Apache Kafka
- Machine Learning
  - Octave
  - Clustering Libraries: Graphlab-create, HDBScan
  - NumPy
- Environment
  - Containerization with Docker Compose

System Architecture Diagram



Docker - Every component represents a seperate container
MySQL
MySQL
SQLite
Send alerts and usage statistics
Database Adapter
Django Rest API
Subscribe
Apache Kafka Message Queue
Subscribe
Publish
HTTPS
Analysis Engine N
Analysis Engine 1
ReactJS app
Agent N
Agent 1
Agents report data and check for updates over HTTPS
Send network traffic for analysis

System Components

- Hardware Platforms
  - Rack Servers
  - Network Clients
- Software Platforms
  - Windows
  - Linux / Unix
  - OS X

Software Technologies

- Docker / Docker Compose
- C
- Python (Django)
- Daphne
- Apache Kafka
- ReactJS
- HTML / CSS
- MaterialUI
- OpenSSL
- Graphlab-create
- HDBScan
- NumPy

Testing

- Frontend: Jest.js
- Backend: Django Test Framework
- API Endpoints: Postman
- Unit and Integration tests

Risks

- Limited knowledge of technologies
  - Django, Apache Kafka, Daphne, and Windows development
  - Write simple prototypes using these technologies
- Getting enough traffic to do testing
  - Software requires a high volume of traffic to gather data
  - Simulate different attacks to try and catch
- Secure code and keeping software secure
  - Writing secure code and protecting the company’s software
  - Learn what secure code is, and locking our computers
- Machine learning getting baseline dataset
  - Realistic dataset for machine learning algorithms to “learn” from
  - Understand machine learning and simulate normal network traffic