

**MICHIGAN STATE**  

---

**U N I V E R S I T Y**

# Alpha Presentation

## Anomaly Detection Suite v2.0

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*

# Project Overview

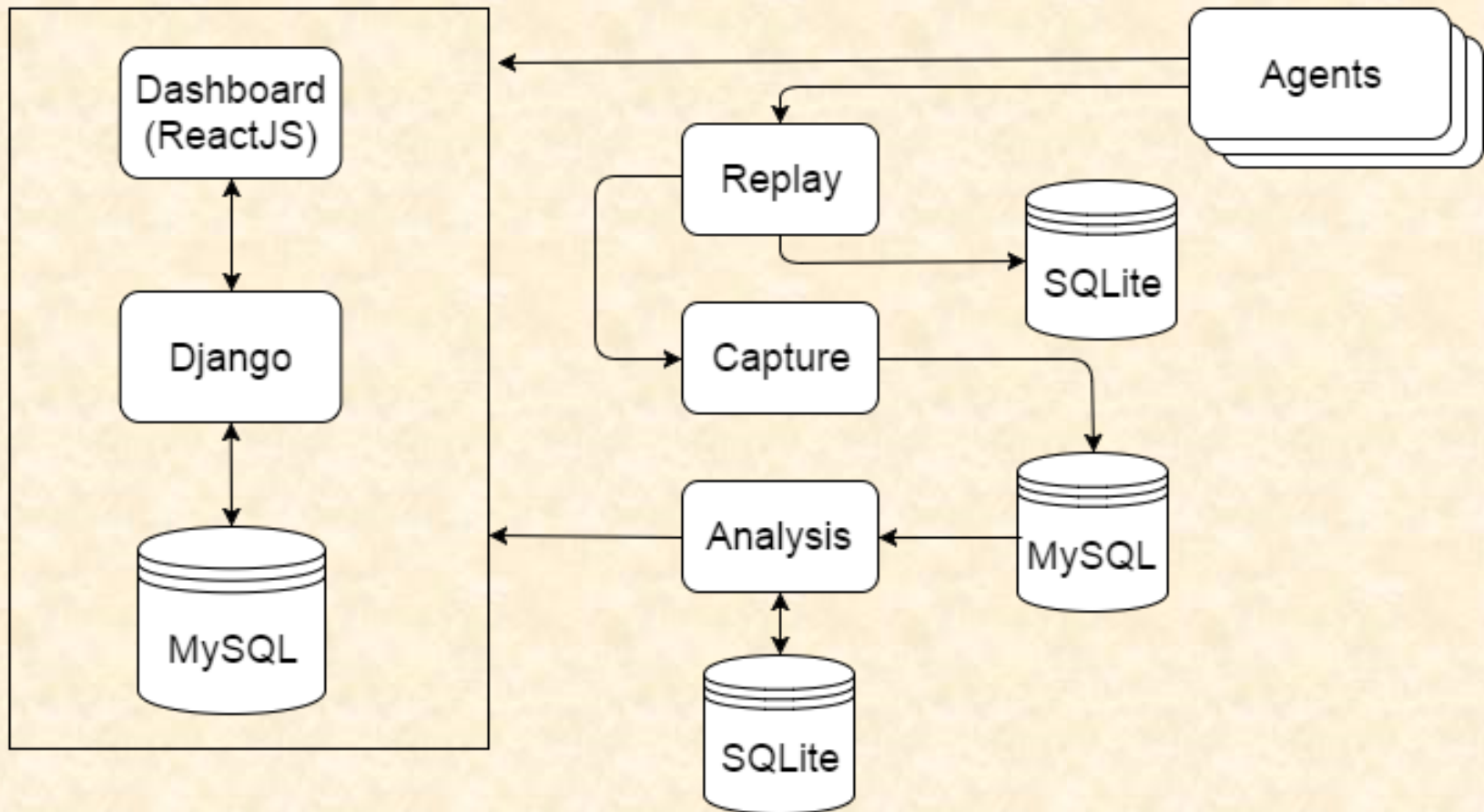
---

Monitors highly-virtualized networks to detect cybersecurity threats

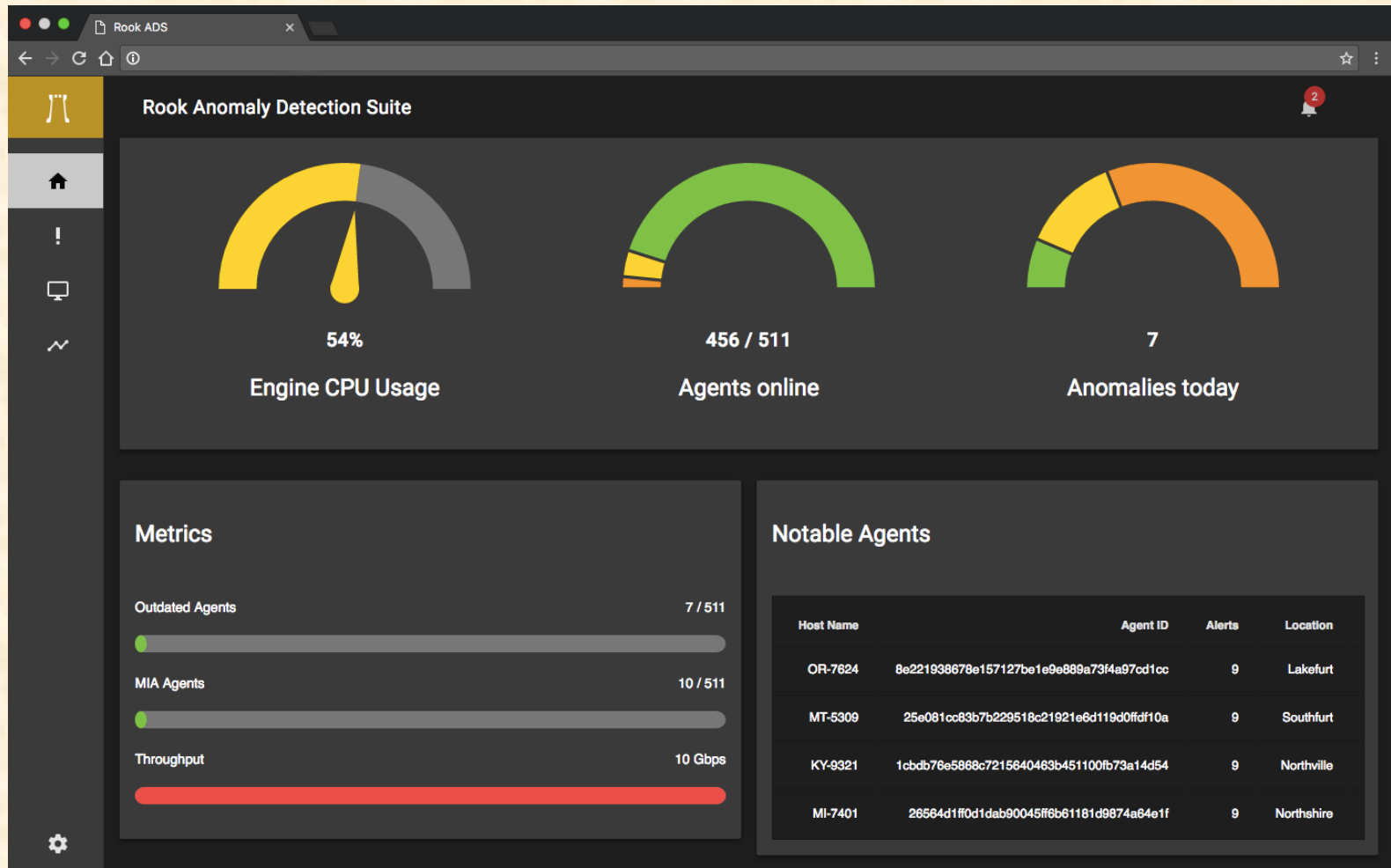
- Develop agent management dashboard
- Optimize agent and engine performance
- Add encrypted local database to the agents
- Add encryption for all communications
- Improve analysis engine with machine learning



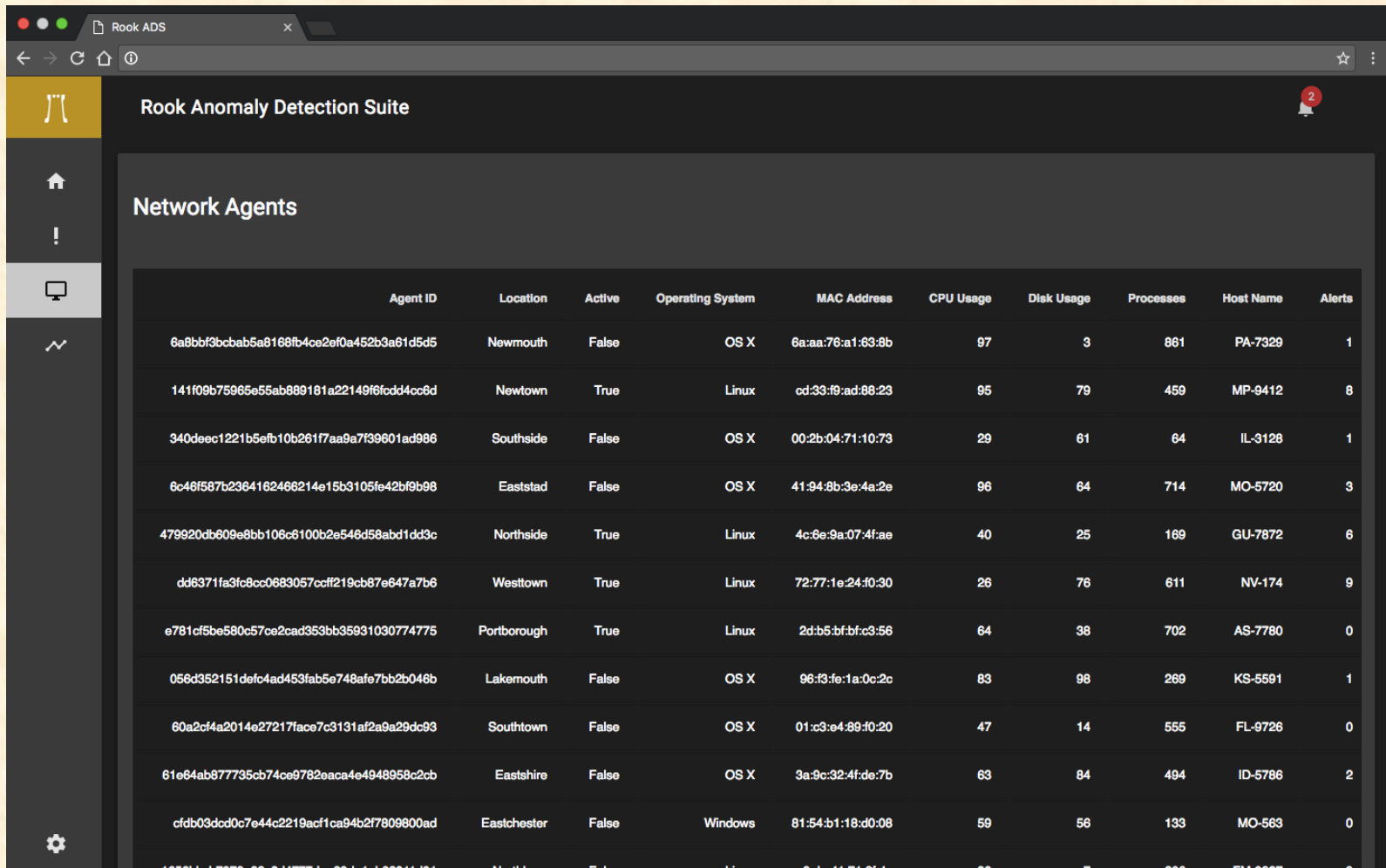
# System Architecture



# Dashboard: Home Page



# Dashboard: Agent Management



The screenshot displays the 'Rook Anomaly Detection Suite' interface. The main content area is titled 'Network Agents' and contains a table with the following columns: Agent ID, Location, Active, Operating System, MAC Address, CPU Usage, Disk Usage, Processes, Host Name, and Alerts. The table lists 12 agents with their respective status and metrics.

Agent ID	Location	Active	Operating System	MAC Address	CPU Usage	Disk Usage	Processes	Host Name	Alerts
6a8bf3bcbab5a8168fb4ce2ef0a452b3a61d5d5	Newmouth	False	OS X	6a:aa:76:a1:63:8b	97	3	861	PA-7329	1
141f09b75985e55ab889181a22149f6fcd4cc8d	Newtown	True	Linux	cd:33:f9:ad:88:23	95	79	459	MP-9412	8
340deec1221b5efb10b261f7aa9a7f39801ad986	Southside	False	OS X	00:2b:04:71:10:73	29	61	64	IL-3128	1
6c46f587b2364162466214e15b3105fe42bf9b98	Eaststad	False	OS X	41:94:8b:3e:4a:2e	96	64	714	MO-5720	3
479920db609e8bb106c6100b2e546d58abd1dd3c	Northside	True	Linux	4c:6e:9a:07:4f:ae	40	25	169	GU-7872	6
dd6371fa3fc8cc0683057cff219cb87e647a7b6	Westtown	True	Linux	72:77:1e:24:f0:30	26	76	611	NV-174	9
e781cf5be580c57ce2cad353bb35931030774775	Portborough	True	Linux	2d:b5:bf:bf:c3:56	64	38	702	AS-7780	0
056d352151defc4ad453fab5e748afe7bb2b046b	Lakemouth	False	OS X	96:f3:fe:1a:0c:2c	83	98	269	KS-5591	1
60a2cf4a2014e27217face7c3131af2a9a29dc93	Southtown	False	OS X	01:c3:e4:89:f0:20	47	14	555	FL-9726	0
61e64ab877735cb74ce9782eaca4e4948958c2cb	Eastshire	False	OS X	3a:9c:32:4f:de:7b	63	84	494	ID-5786	2
cfdb03dcd0c7e44c2219acf1ca94b2f7809800ad	Eastchester	False	Windows	81:54:b1:18:d0:08	59	56	133	MO-563	0
1658bcb7072e89c9145774e09d1cb09811d91	Northbury	False	Linux	c9:dc:41:31:06:1e	88	7	908	EM-8807	0



# Performance Statistics

%	image name	app name
81.7770	libsqlite3.so.0.8.6	analyze
100.000	libsqlite3.so.0.8.6	analyze

```

CPU: Intel Core/i7 speed 2792.93 Mhz (estimated)
Counted CPU CLK_UNHALTED_events (Clock cycles when not halted) with a unit mask of 0x00 (No unit mask) count 100000
-----
samples % image name app name symbol name
-----
435595 81.7770 libsqlite3.so.0.8.6 analyze /usr/lib/x86_64-linux-gnu/libsqlite3.so.0.8.6
435595 100.000 libsqlite3.so.0.8.6 analyze /usr/lib/x86_64-linux-gnu/libsqlite3.so.0.8.6 [self]
-----
65420 12.2817 libc-2.19.so analyze /lib/x86_64-linux-gnu/libc-2.19.so
65420 100.000 libc-2.19.so analyze /lib/x86_64-linux-gnu/libc-2.19.so [self]
-----
7589 1.4247 libpthread-2.19.so analyze pthread_mutex_unlock
7589 100.000 libpthread-2.19.so analyze pthread_mutex_unlock
-----
7209 1.3534 libmysqclient.so.18.0.0 analyze /usr/lib/x86_64-linux-gnu/libmysqclient.so.18.0.0
7209 100.000 libmysqclient.so.18.0.0 analyze /usr/lib/x86_64-linux-gnu/libmysqclient.so.18.0.0
-----
7013 1.3166 libpthread-2.19.so analyze pthread_mutex_lock
7013 100.000 libpthread-2.19.so analyze pthread_mutex_lock
    
```

%	self	total	name
time	us/call	us/call	
66.67	32.37	32.37	Many SQLite Query

```

Each sample counts as 0.01 seconds.
-----
% cumulative self self total
time seconds seconds calls us/call us/call name
-----
66.67 0.02 0.02 618 32.37 32.37
33.34 0.03 0.01 50195 0.00 0.00
0.00 0.03 0.00 12360 0.00 0.00
0.00 0.03 0.00 3974 0.00 0.00
0.00 0.03 0.00 3703 0.00 0.00 check_ip
0.00 0.03 0.00 3471 0.00 0.00
0.00 0.03 0.00 3315 0.00 0.00
0.00 0.03 0.00 3020 0.00 0.00
0.00 0.03 0.00 2016 0.00 0.00 socket_tcp_open
0.00 0.03 0.00 1486 0.00 0.00
0.00 0.03 0.00 919 0.00 0.00
0.00 0.03 0.00 618 0.00 0.00
0.00 0.03 0.00 618 0.00 0.00
    
```



# What's left to do?

- Connect agents to management dashboard
- Implement data visualization
- Remote agent updating
- Optimize SQL queries
- Make agents more self-analyzing
- Improve anomaly detection algorithm with machine learning



# Questions?

---

?

?

?

?

?

?

?

?

?

