

MICHIGAN STATE

U N I V E R S I T Y

Beta 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*

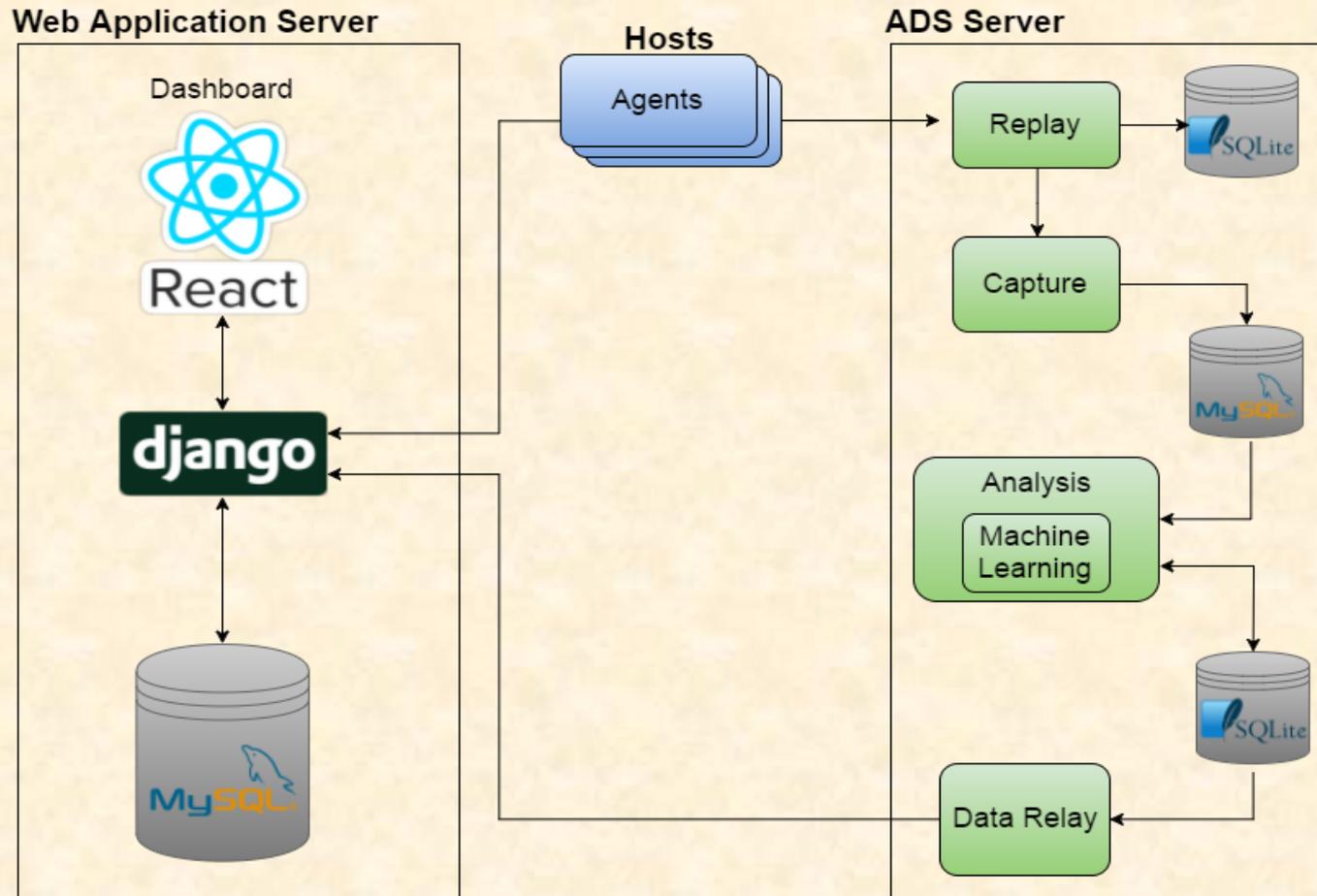
Project Overview

Monitors highly-virtualized networks to detect cybersecurity threats

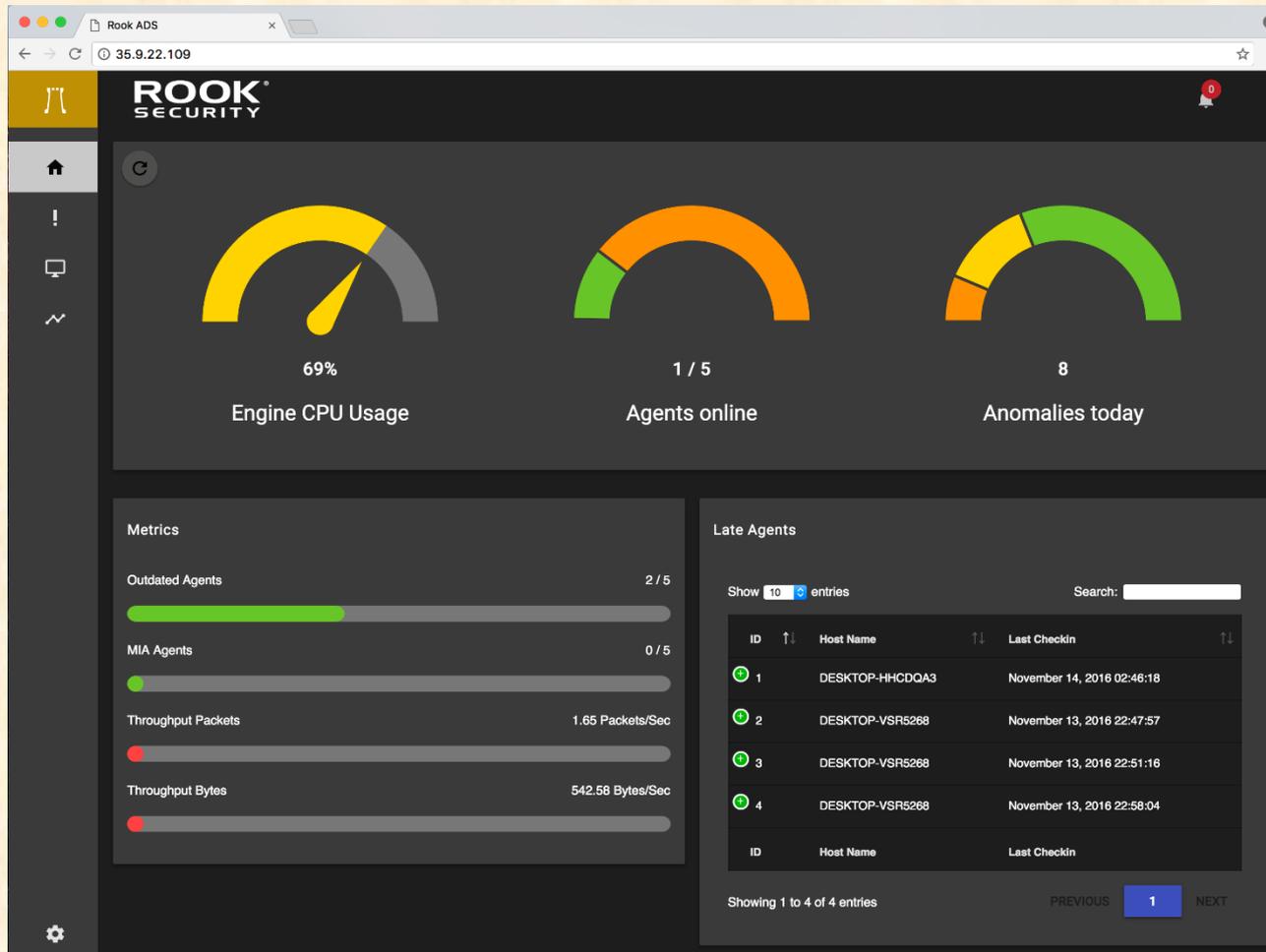
- Develop agent management dashboard
- Optimize agent and engine performance
- Improve analysis engine with machine learning
- Create Linux based agent



System Architecture



Dashboard: Home Page



Dashboard: Alert Table

The screenshot shows a web browser window with the URL `35.9.22.109/events`. The page title is "Rook ADS". The dashboard header includes the Rook Security logo and a notification bell icon with a red circle containing the number "0". The main content area is titled "Network Anomalies" and features a "Show 10 entries" dropdown menu and a search input field. Below this is a table of network anomalies with columns for IP Source, IP Destination, Time, Type, Name, and Score. The table contains three entries, all of which are BLACKLIST events with a score of 22. The table is paginated, showing "Showing 1 to 3 of 3 entries" and navigation buttons for "PREVIOUS", "1", and "NEXT".

IP Source	IP Destination	Time	Type	Name	Score
128.49.16.172	20.20.9.35	Nov 12, 2016 19:30:40	BLACKLIST	"35.9.20.20"	22
128.49.16.172	20.20.9.35	Nov 12, 2016 19:30:40	BLACKLIST	"35.9.20.20"	22
128.49.16.172	20.20.9.35	Nov 13, 2016 17:50:12	BLACKLIST	"35.9.20.20"	22



Dashboard: Agent Management

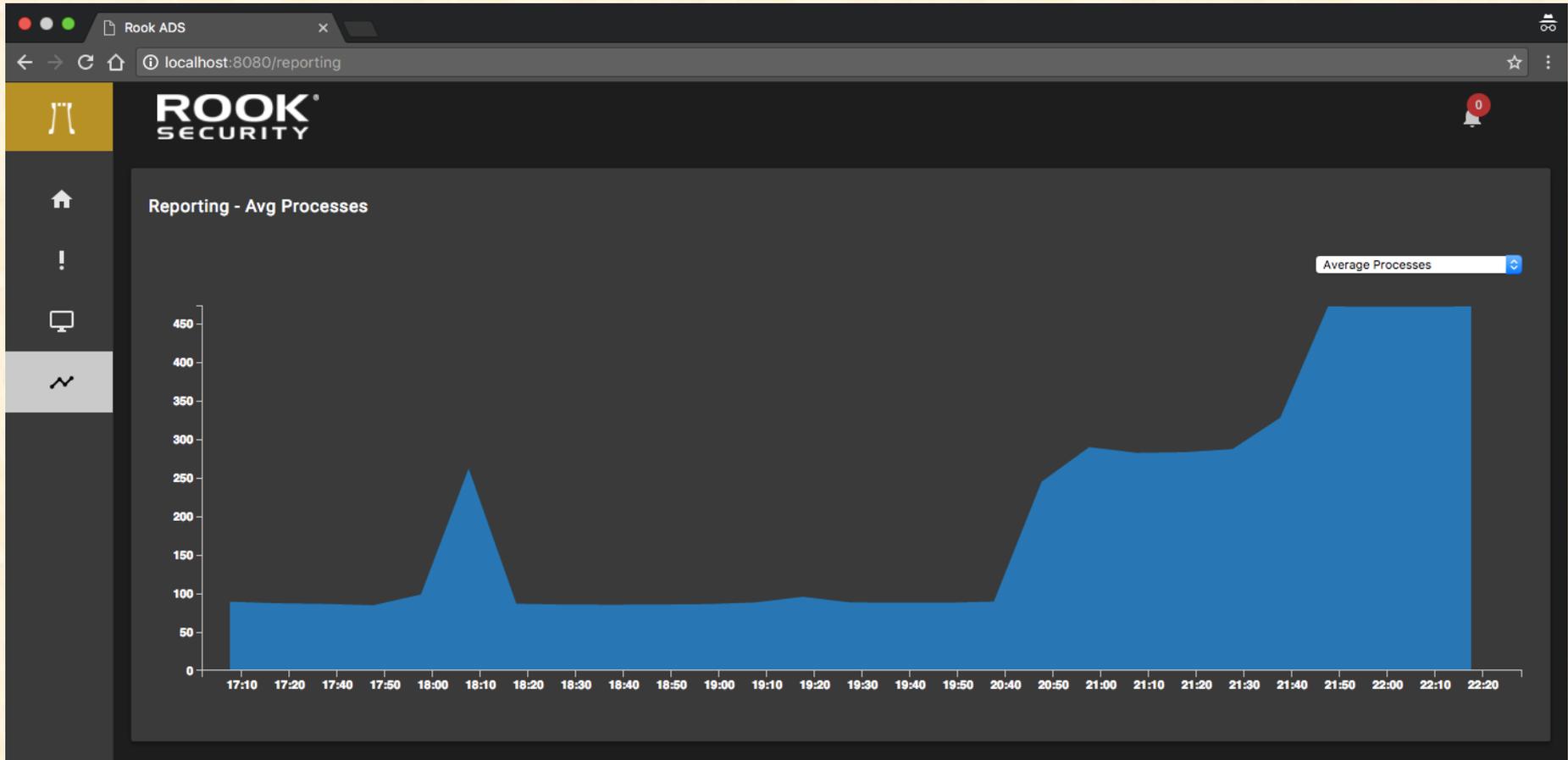
The screenshot shows the Rook Security dashboard for Agent Management. The browser address bar indicates the URL is 35.9.22.109/agents. The dashboard features a dark theme with a sidebar on the left containing navigation icons for home, alerts, devices, and settings. The main content area is titled "Network Agents" and includes a search bar and a "Show 10 entries" dropdown. A table displays the following data:

ID	Host Name	OS	CPU	MEM	Num. Processes	Disk Space	MAC	Current Version	Select Update
1	DESKTOP-HHCDQA3	Windows 10.0.14393	100%	55.1%	89	29.84%	00:0C:29:74:E1:62	1.0.0	1.0.0
2	DESKTOP-VSR5268	Windows 10.0.14393	62.61%	32.52%	77	47.49%	00:0C:29:E3:70:D5	1.2.1	1.2.1
3	DESKTOP-VSR5268	Windows 10.0.14393	73.98%	47.02%	83	47.49%	00:0C:29:F4:B6:78	1.2.1	1.2.1
4	DESKTOP-VSR5268	Windows 10.0.14393	100%	44.65%	80	47.49%	00:0C:29:D4:70:D1	1.2.1	1.2.1
5	ubuntu	Ubuntu 16.04.1 LTS	8.21%	90.32%	472	27.29%	00:0C:29:61:4F:D4	1.0.0	1.0.0

At the bottom of the table, there is a pagination bar showing "Showing 1 to 5 of 5 entries" and navigation buttons for "PREVIOUS", "1" (selected), and "NEXT".



Dashboard: Reporting



What's left to do?

- Project Video
- Enhance operation of machine learning component
- Integration testing of all features
- Performance testing
- Add further support for Windows and Linux based agents on server



Questions?

?

?

?

?

?

?

?

?

?

