

MICHIGAN STATE

U N I V E R S I T Y

Project Plan

Endpoint Data Monitoring and Analysis Agent

The Capstone Experience

Team Rook

Bohao Gao

Andrew Gilbertson

Jeremy Specht

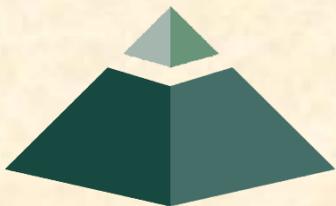
Vikram Thakur

Jared Clark

Department of Computer Science and Engineering

Michigan State University

Spring 2018



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

Functional Specifications

- Endpoint Agent Log Collection
 - Cross Platform Compatible
- Communication Channels for data
 - Configurable
- Web Application to Analyze Agent
 - Configuration
 - Log paths, storage location
 - Health Analysis
 - Alert priorities



Design Specifications

- Agent
 - Background Process
 - Limited client interaction
- Web Application
 - Extends Current Force Platform
 - Display Log History
 - Current Client Host Health Status
 - Configuration



Screen Mockup: System Health

Force Platform

ROOK SECURITY

Agent Dashboard

Select Client

- Client 1
- Client 2
- Client 3
- Client 4

Select Agent

- Agent 1
- Agent 2
- Agent 3
- Agent 4
- Agent 5
- Agent 6

Change Default Data Storage Location

Configure Agent | **System Health**

LOG HISTORY

From: 1/29/2018 8:45 am

To: 1/29/2018 5:16 pm

- Log 1
- Log 2
- Log 3
- Log 4
- Log 5
- Log 6
- Log 7
- Log 8
- Log 9
- Log 10
- Log 11
- Log 12
- Log 13

Messages

1-23-2018-1:24:
Warning, irregular behavior detected.
log: Log2
src: /var/log/syslog

STATUS

Overall health: **Good**

Log Source: [/var/log/syslog](#)
Source health: **Warning**

Alerts

1-23-2018-1:24:
Alert Threshold reached, type: 2,
src: Log2

Total Log Volume: 17 Logs, 200 KB

Last Checked in: 0 Hours, 37 Minutes ago

Specify range of time

Select individual logs

System Health

Log Source Info

Alerts



Screen Mockup: Configuration

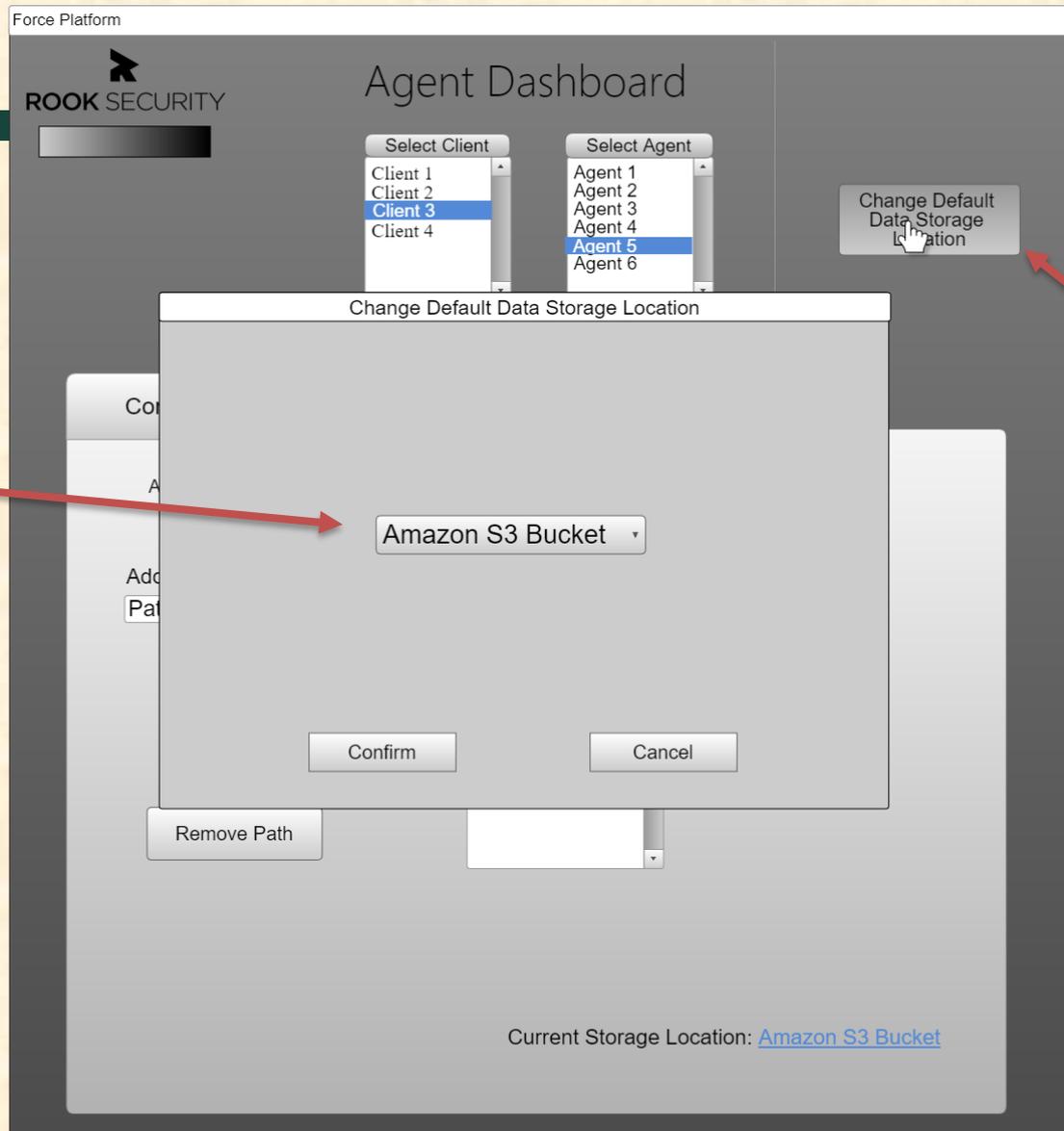
The screenshot shows the 'Agent Dashboard' configuration window. At the top left is the 'ROOK SECURITY' logo. Below it are two dropdown menus: 'Select Client' (with Client 3 selected) and 'Select Agent' (with Agent 5 selected). To the right is a button labeled 'Change Default Data Storage Location'. Below these are two tabs: 'Configure Agent' (active) and 'System Health'. The 'Configure Agent' tab shows 'Agent Version: 1.02.07'. On the left, there is an 'Add Path' section with a text input containing 'Path 9' and an 'Add' button, and a 'Remove Path' button below it. In the center is a 'Current Paths' list containing Path 1 through Path 8. On the right, there is a checked checkbox for 'Custom Data Storage Location' and a dropdown menu currently set to 'Amazon S3 Bucket'. At the bottom, it displays 'Current Storage Location: Amazon S3 Bucket'.

Add/Remove Source Paths

Select New Storage Location



Screen Mockup: Storage Location



Change Default Storage Option

Button to bring up window

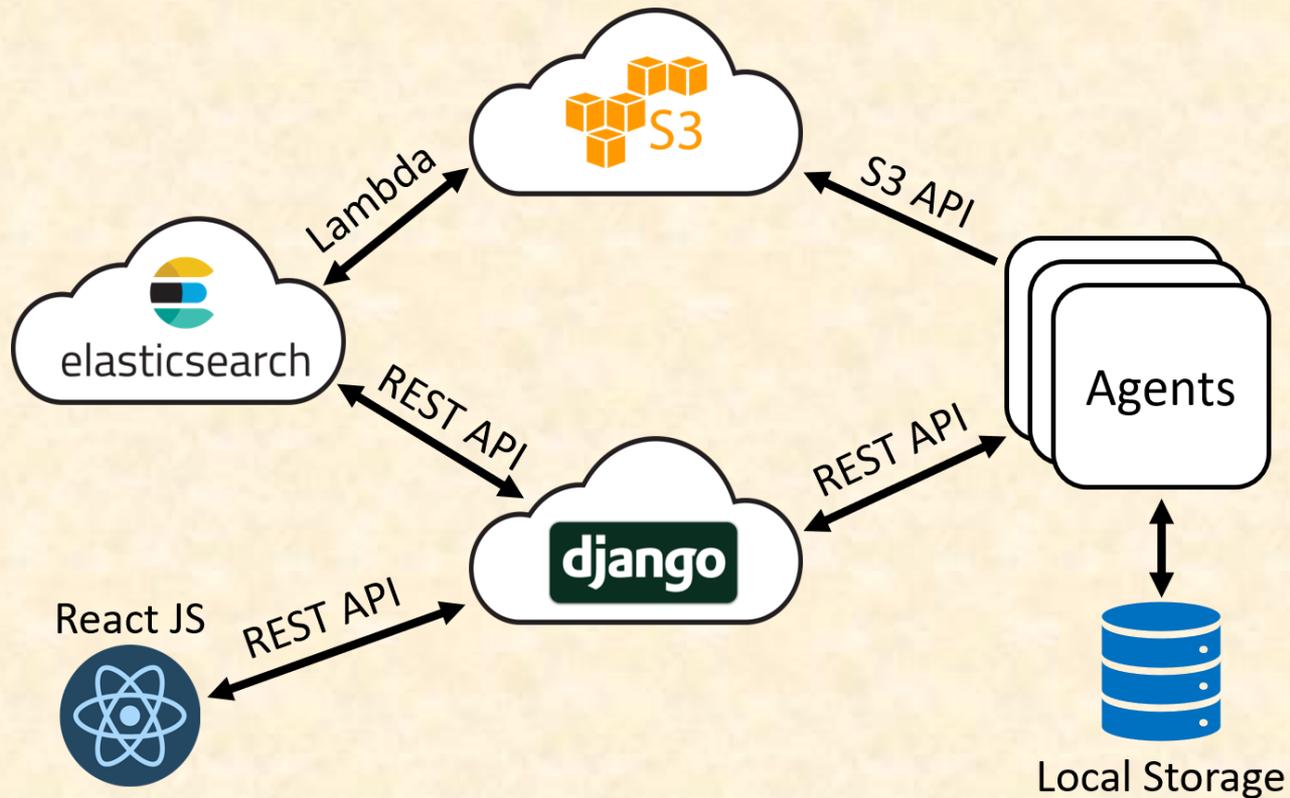


Technical Specifications

- Storage System
 - AWS S3, Django RESTful endpoint, Elastic Search
- Log Collection Agents using Go
 - Easy Cross Platform Design
 - Local storage capability
- Web Interface
 - ReactJS, Redux, HTML, CSS
 - Backend leverages Django



System Architecture



System Components

- Hardware Platforms
 - Ubuntu Django Server
 - AWS S3 Buckets
 - AWS Elastic Search
- Software Platforms / Technologies
 - GoLand IDE
 - Django REST Framework
 - OS Specific Log Collection Interaction
 - AWS API for Go



Risks

- Developing Cross Platform Software
 - Streamlining Log Collection Process for all OS
 - Collect in each OS and build overarching process
- Health Metrics
 - Making sure what is being analyzed is useful
 - Constant communication with Rook
- Integration of Current Platform
 - Cannot compromise integrity of existing platform
 - Iterative Process including Rook Analysts' Feedback
- Effective Testing
 - Replicate realistic traffic on agent and web application
 - Use mock data provided by rook and bench testing



Questions?

?

?

?

?

?

?

?

?

?

