From Students…
...to Professionals

Michigan State University

Alpha Presentation

Endpoint Data Monitoring and Analysis Agent

The Capstone Experience

Team Rook

Jared Clark
Drew Gilbertson
Bohao Gao
Jeremy Specht
Vikram Thakur

Department of Computer Science and Engineering
Michigan State University
Spring 2018
Project Overview

• Endpoint Agent Log Collection
  ▪ Cross Platform Compatible

• Communication Channels for Data
  ▪ Configurable

• Web Application to Analyze Agent
  ▪ Configuration
    o Log Paths, Storage Location
  ▪ Health Analysis
    o Alert Priorities
System Architecture

- **Lambda**
- **S3**
- **elasticsearch**
- **Django**
- **React JS**
- **Force Platform**
- **Agents**
- **Local Storage**

REST API connections between services.
Force Platform

Agent Management Console

Change Interval:
Current interval: 15 Minutes
New Interval:

Log File Paths:
- corecaptured.log
- deploypolicyd.stdout
- fits_convert.log
- install.log
- system.log

Select Unique Location:
AMAZON S3 BUCKET

Add Path:
Remove Path:
Force Platform

The Agent Management Console displays various sections:

- **Log Volume (Last Hour):** The logs include:
  - var/files/log: 85
  - var/rev.log: 3
  - var/secret.log: 8
  - var/log/rel: 3

- **Agent Info:**
  - **Client:** Meijer
  - **Agent ID:** MeijerAgent001
  - **Operating System:** Mac OS
  - **Storage Location:** Amazon S3 Bucket
  - **Time Zone:** EST

- **Health Status:**
  - **Agent Health Status:** Good
  - **System Health Status:** Good

- **Agent Config Info:**
  - **Last Config Change:** 2/18/18
  - **Path Change:** added rev/log to log
  - **Interval Change:** 15 mins
  - **Storage Change:** Amazon S3 Bucket
  - **User:** Jeremy Spacht

- **Agent Alerts:**
  - Alert 1
  - Alert 2
  - Alert 3
  - Alert 4
  - Alert 5
  - Alert 6
  - Alert 7
  - Alert 8
  - Alert 9
  - Alert 10
Storage System
What’s left to do?

• Remote Configuration of Agent
• Front-End Development
  ▪ Refine Interface Functionality
• Back-End Development
  ▪ Feature Expansion
• Elasticsearch
  ▪ Integration
Questions?