Alpha Presentation
Cloud Security Event Processing And Alerting Platform
The Capstone Experience

Team Rook
Brian Jones
Bradley Baker
Jake Fenton
Kaushik Sridasyam
Alex Fall

Department of Computer Science and Engineering
Michigan State University
Fall 2017
Project Overview

• Rook provides managed security services
• Scans network logs looking for security threats
• We’re upgrading the scanner to add...
  ▪ Scalability
  ▪ Standardized management
  ▪ Unified programs
User Interface – Client Profile View

CUSTOMER SETTINGS

Customer Name:
Example Inc.

Email:
contact@example.org

Index Date Format:
YYYY:MM:DD

Local DB Name:
local.db

Whitelist by IP or domain

- notathreat.org
- 11.22.33.44

Add
Remove

CANCEL
SAVE CHANGES
User Interface – Rule View
What’s left to do?

• Testing
  ▪ Unit testing
  ▪ Rook personal feedback

• Integrate all of the pieces
  ▪ Write to S3 via API
  ▪ Have lambdas trigger email
  ▪ Convert the lambda engines
  ▪ Iterate frontend with Rook
Questions?