

**MICHIGAN STATE**  
**UNIVERSITY**

# Alpha Presentation

## Cloud Security Event Processing And Alerting Platform The Capstone Experience

Team Rook

Brian Jones

Bradley Baker

Jake Fenton

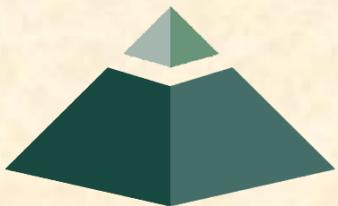
Kaushik Sridasyam

Alex Fall

Department of Computer Science and Engineering

Michigan State University

Fall 2017



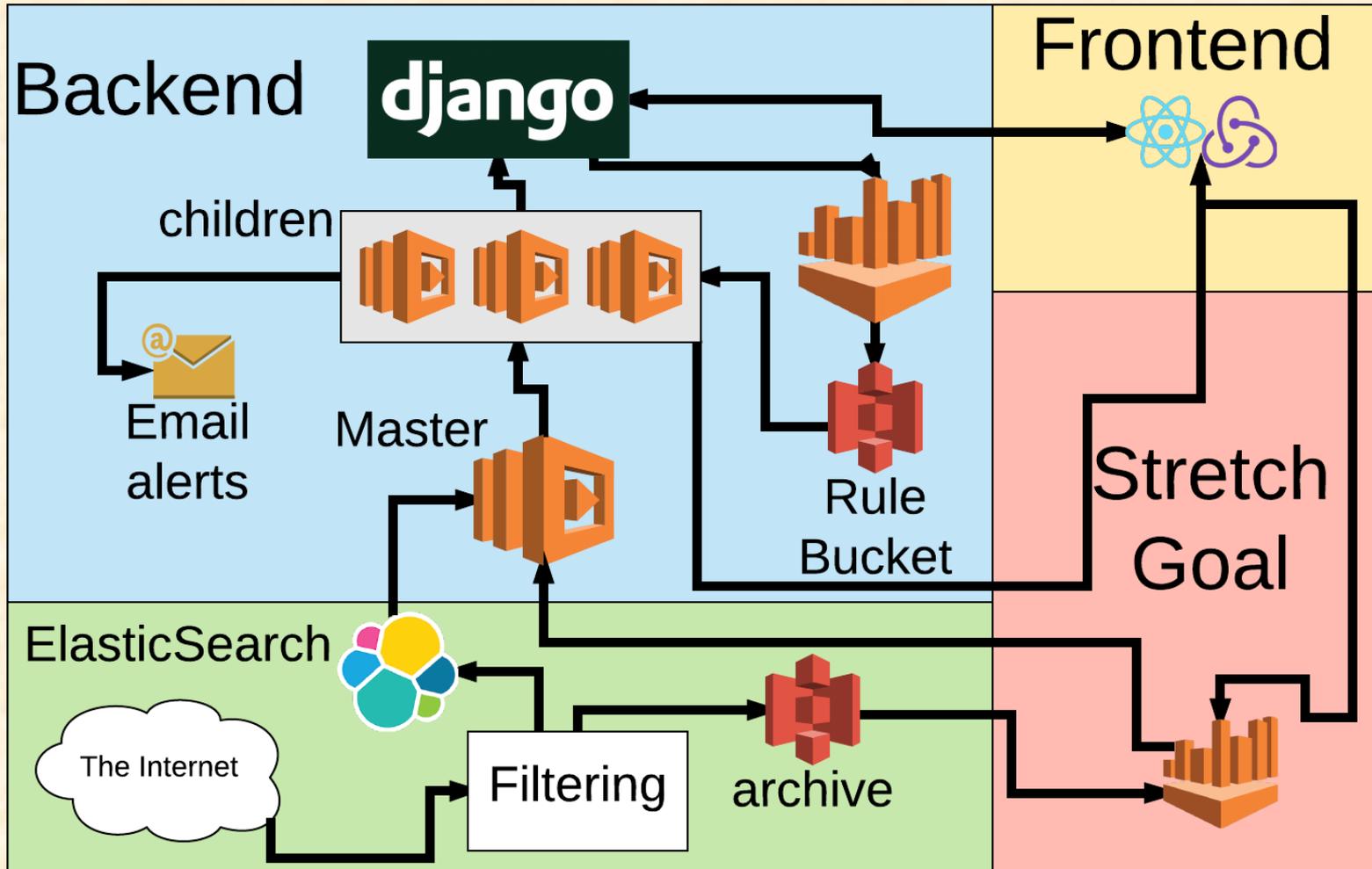
*From Students...  
...to Professionals*

# 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

# System Architecture



# User Interface – Client Profile View

## CUSTOMER SETTINGS

Customer Name:  
Example Inc.

Email:  
contact@example.org

Index Date Format:  
YY:MM:DD

Local DB Name:  
local.db

Whitelist by IP or domain

Add

- notathreat.org Remove
- 11.22.33.44 Remove

CANCEL SAVE CHANGES



# User Interface – Rule View

The screenshot displays the Rook Security web application interface. The browser address bar shows the URL <https://www.rooksecurity.com>. The navigation menu includes 'ROOK SECURITY', 'WORKSPACE', 'CONSOLE', 'SETTINGS', and 'CORRELATION'. The 'CORRELATION' menu item is highlighted with a yellow gear icon. A 'SEND FEEDBACK' button and a user profile icon 'TG' are visible in the top right. Below the navigation, the 'Rules' tab is selected, and a dropdown menu shows 'vulnerability exploit detection'. Three action buttons are present: 'ADD RULE', 'DELETE RULE', and 'EDIT RULE'. A table with columns 'COMPONENT' and 'DETAILS' lists the following data:

COMPONENT	DETAILS
type	threat
threatid	30000,44999
severity	informational,low
action	!deny
from	Untrusted
event_count	10
event_ttl	900
track_by	src

At the bottom, there is a pagination control showing '10' items per page and a page number '1'.



# 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?

---

?

?

?

?

?

?

?

?

?

