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

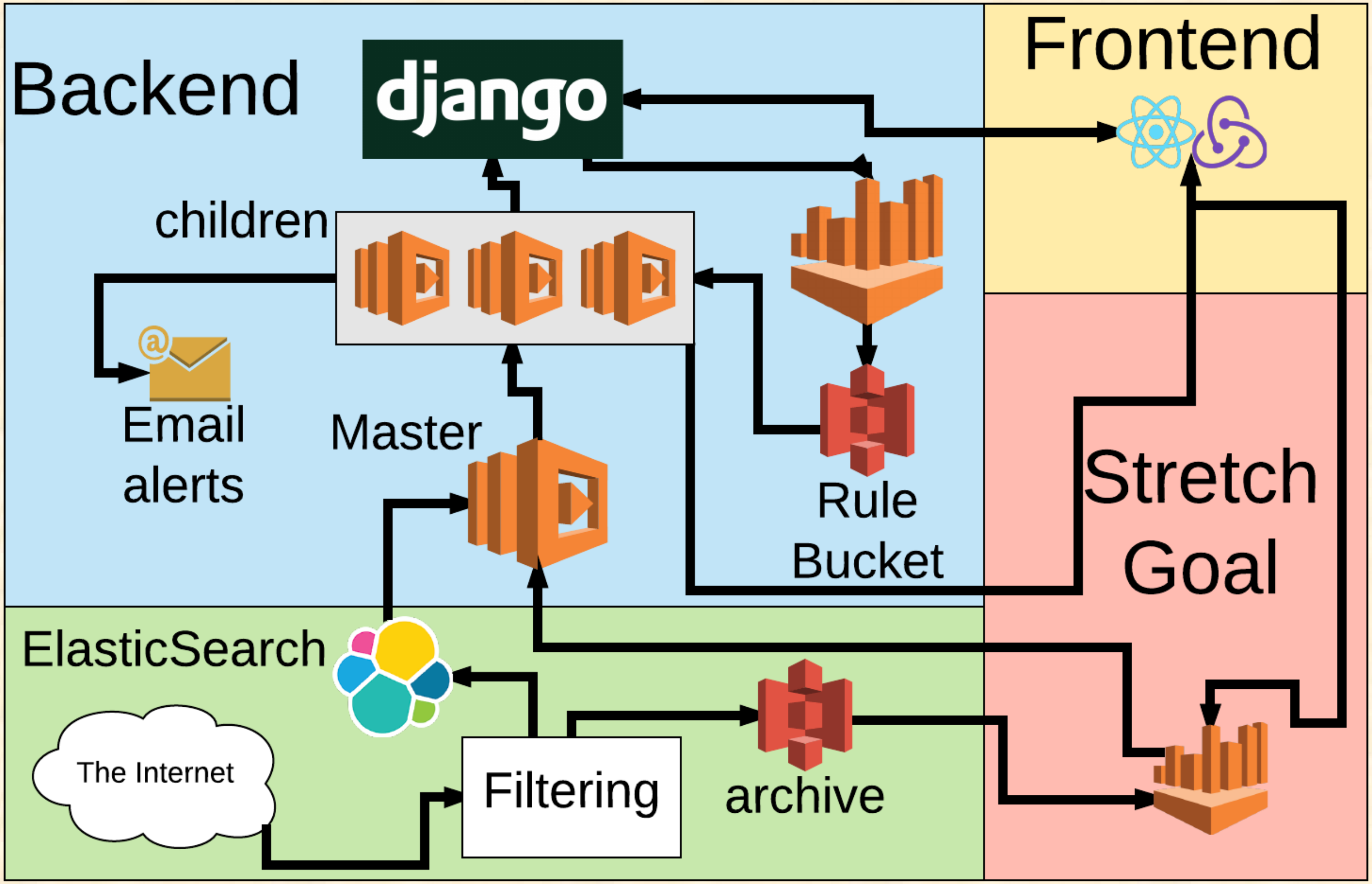
Fall 2017

From Students…
…to Professionals

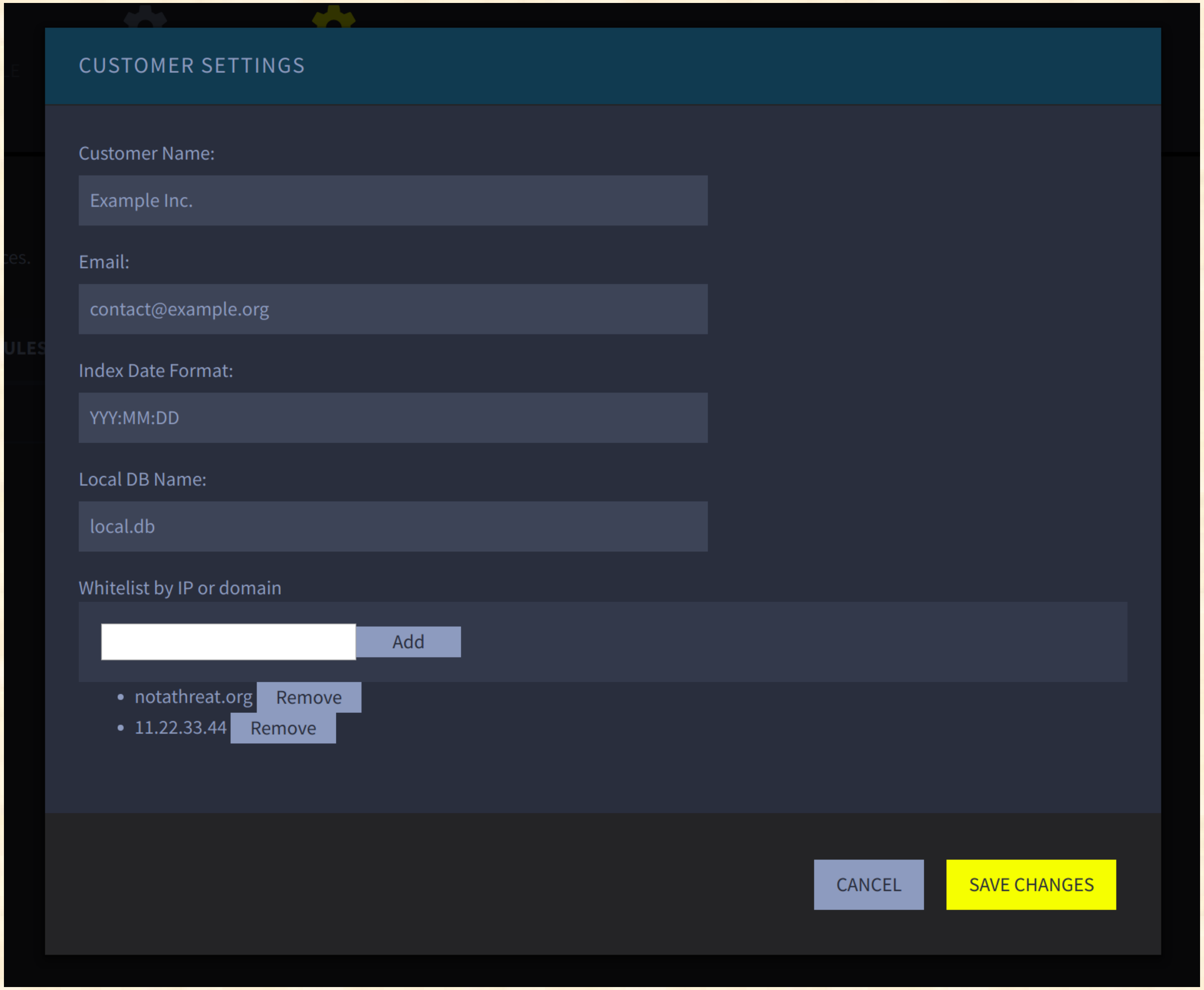
Project Overview

- 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

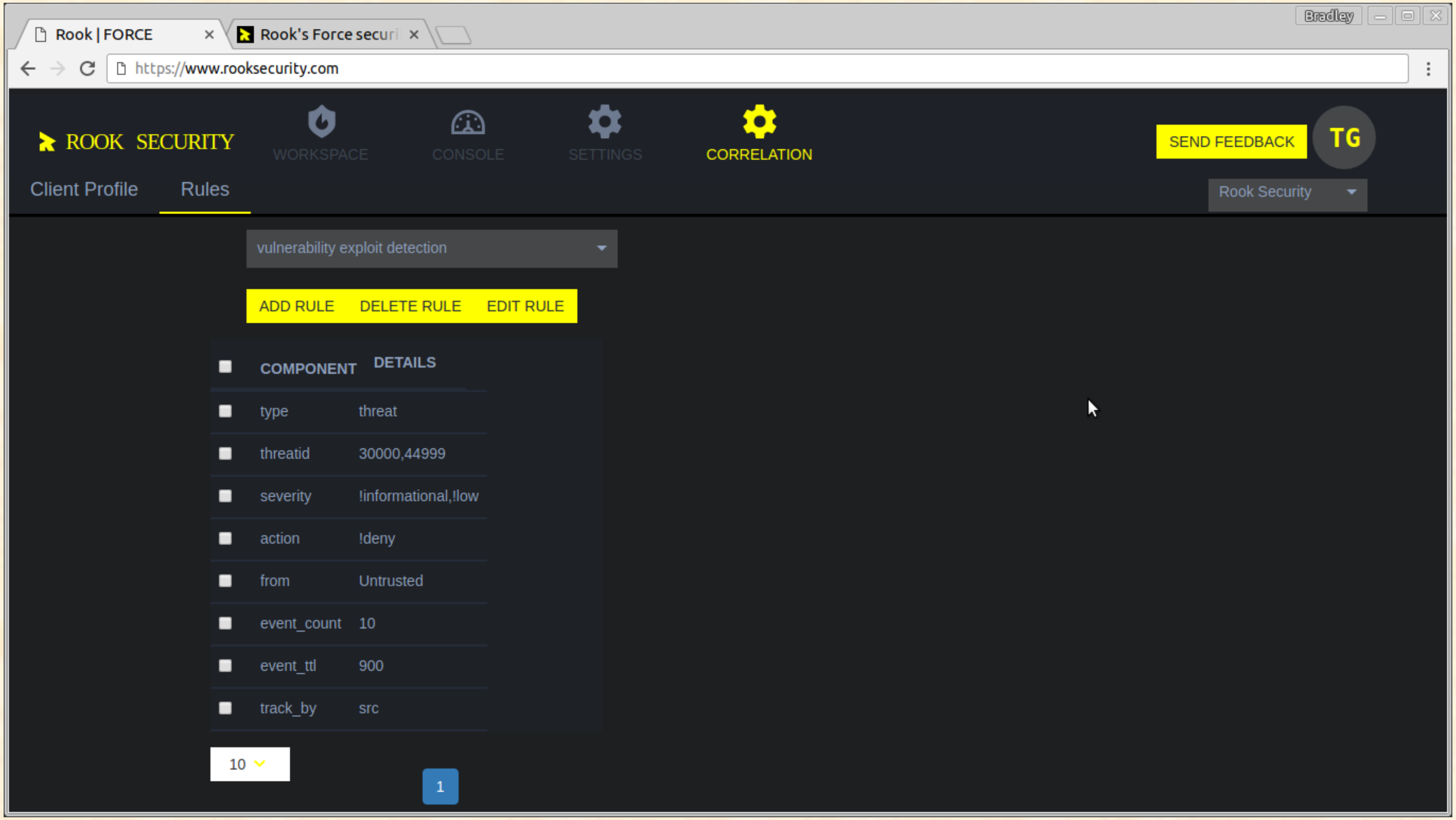
Index Date Format: YYY:MM:DD

Local DB Name: local.db

Whitelist by IP or domain

- notathreat.org
- 11.22.33.44

User Interface – Rule View



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

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?

? ? ? ?

? ?

? ? ?