

MICHIGAN STATE
UNIVERSITY

Beta 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

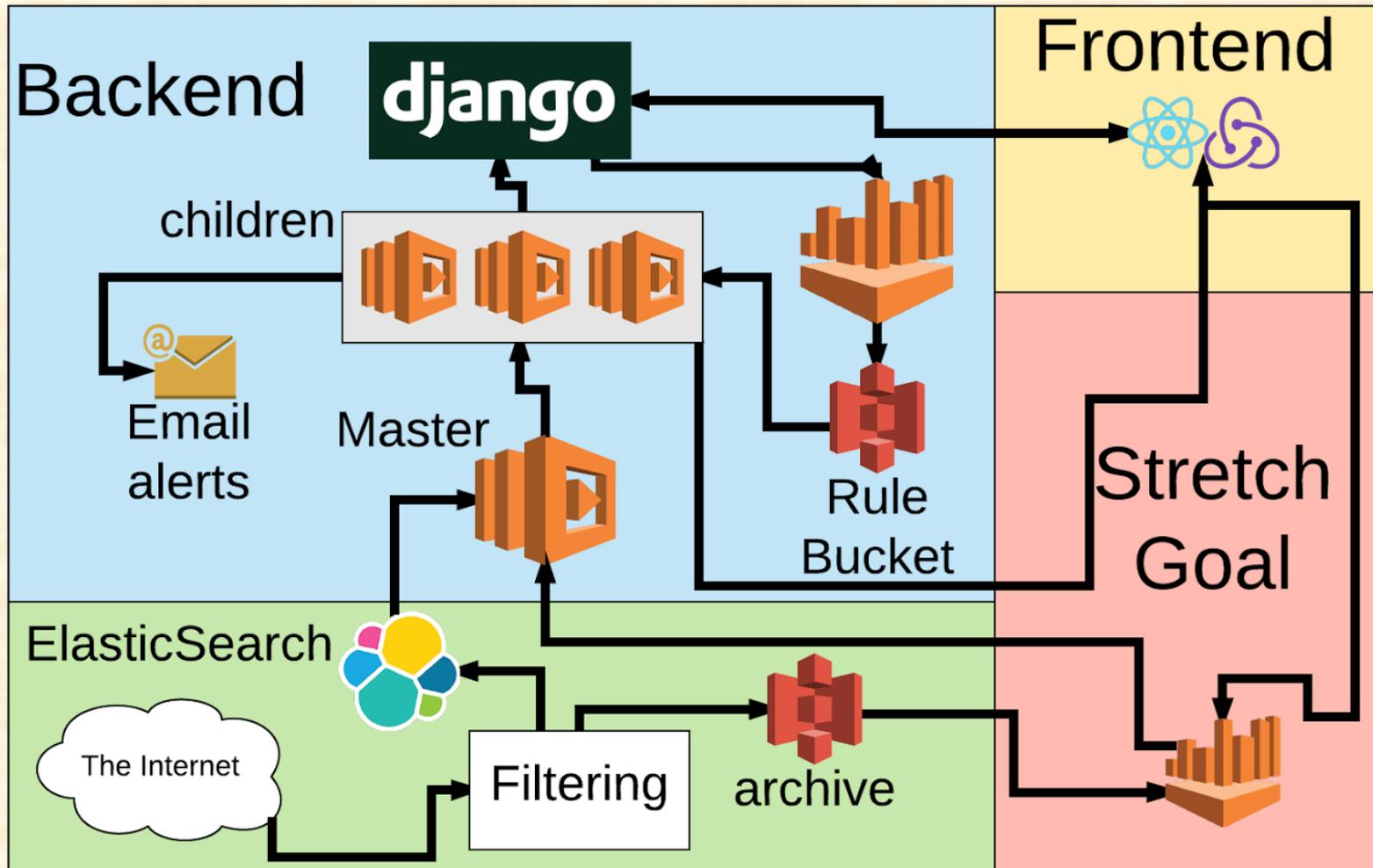
Fall 2017



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

System Architecture



Client Profile Page

Applications Places System Rook | FORCE Thu Nov 9, 16:11 Bradley

localhost:8082/correlation

ROOK SECURITY WORKSPACE CONSOLE SETTINGS CORRELATION TG

Client Profile Rules

CLIENT PROFILES

Add and remove clients and manage individual client preferences.

ADD CLIENT

CLIENT NAME	CLIENT EMAIL	Delete Client	Modify
multi-firewall client	multi@firewall.com	Delete	EDIT
some new boring client	asdfklafs@asdfsds.com	Delete	EDIT
new customer	cust@email.com	Delete	EDIT
full stack test	moo@cow.com	Delete	EDIT
good	good@er.com	Delete	EDIT
some new profile	new@profile.com	Delete	EDIT

10 1



Add/Edit Client Modal

CUSTOMER SETTINGS

Customer Name:

Customer Full Name:

Email:

Incidents Index:

Index Date Format:

Local DB Name:

Whitelist by IP or domain

- google.com
- 192.168.1.1

- Client Name
- Connections to Known Bad URI
- OS Exploit attempt



Rules Page

The screenshot shows a web browser window with the URL `localhost:8082/correlation`. The application header includes the Rook Security logo and navigation tabs for WORKSPACE, CONSOLE, SETTINGS, and CORRELATION. The user profile 'TG' is visible in the top right. The main content area is titled 'Rules' and features a dropdown menu set to 'Meraki' and an 'ADD' button. Below this is a table of rules:

TITLE	DELETE	EDIT
Connections to Known Bad URI	DELETE	EDIT
OS Exploit attempt	DELETE	EDIT
Known-bad activity	DELETE	EDIT
Policy Violation	DELETE	EDIT
Malware Infection Detected	DELETE	EDIT

At the bottom of the table, there is a pagination control showing '5' items per page and a row of buttons for pages 1, 2, 3, 4, 5, and a next button '>'. The '1' button is currently selected.



Add/Edit Rule Modal

The screenshot displays the Rook Security web interface. A modal window titled "EDIT RULE" is open, allowing for the configuration of a security rule. The background shows a list of rules under the "Rules" tab, with a search bar and an "ADD" button. The modal fields are as follows:

- title:** Connections to Known Bad URI
- type:** meraki
- module:** ids-alerts
- alert_message:** BLACKLIST URI*
- direction:** egress
- event_count:** 1
- event_ttl:** 9
- track_by:** src_ip

At the bottom of the modal, there are two buttons: "CANCEL" and "EDIT RULE".



What's left to do?

- Finish migrating the firewall architectures for child lambda functions
- Get final feedback from Rook personal on front end design choices
- Work on project video



Questions?

?

?

?

?

?

?

?

?

?

