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

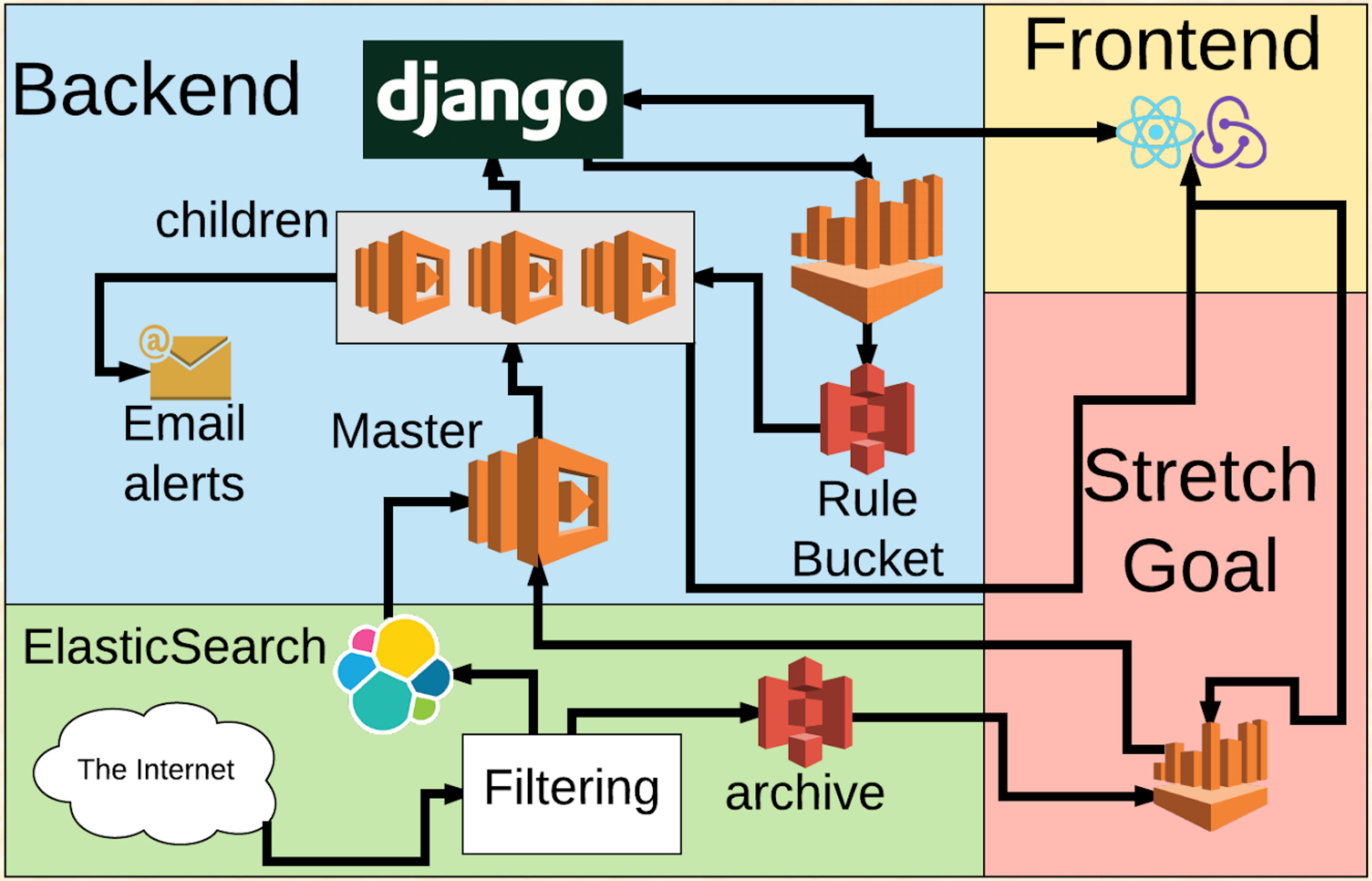
From Students…

…to Professionals

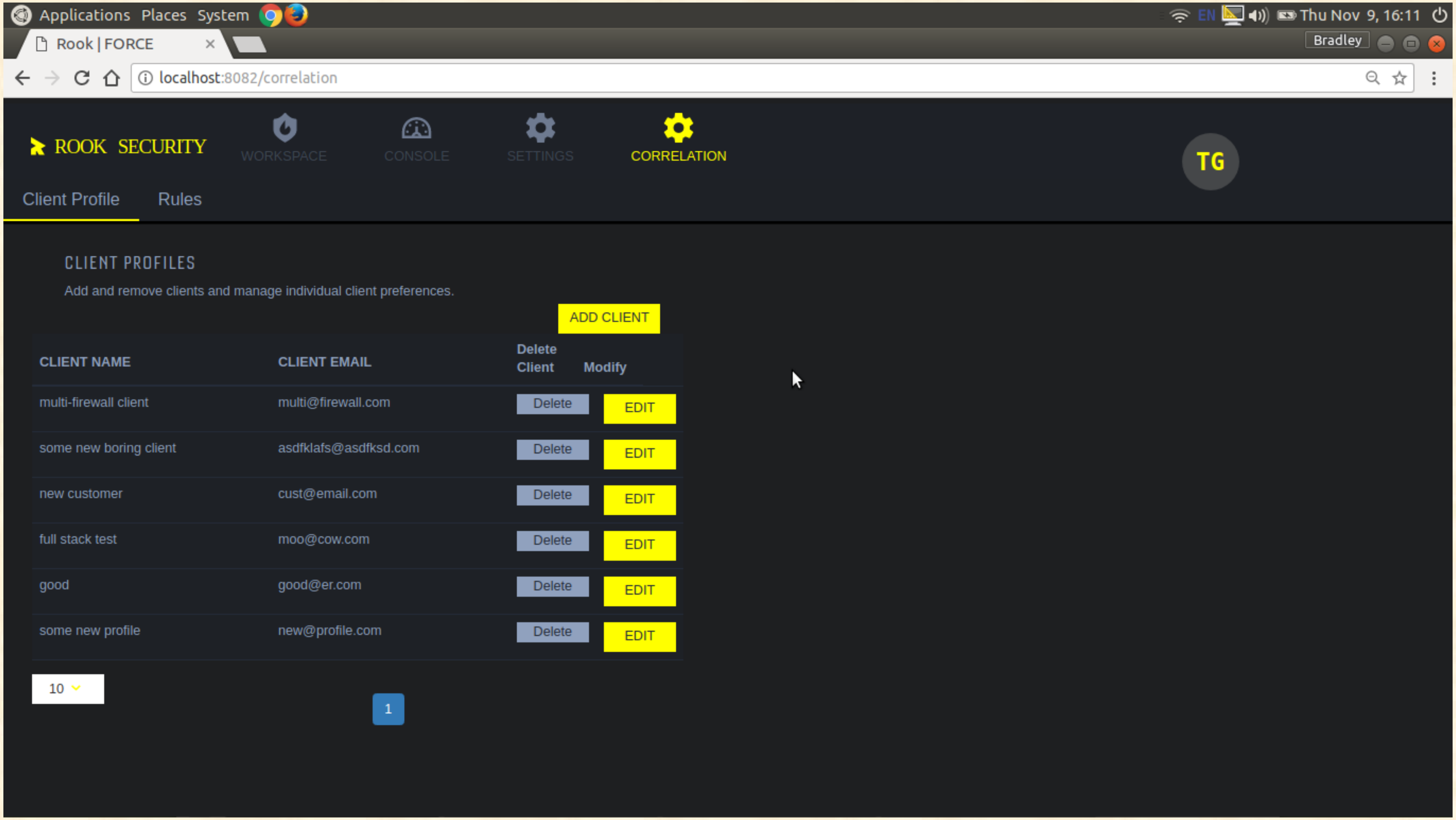
Project Overview

- 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



Client Profile Page



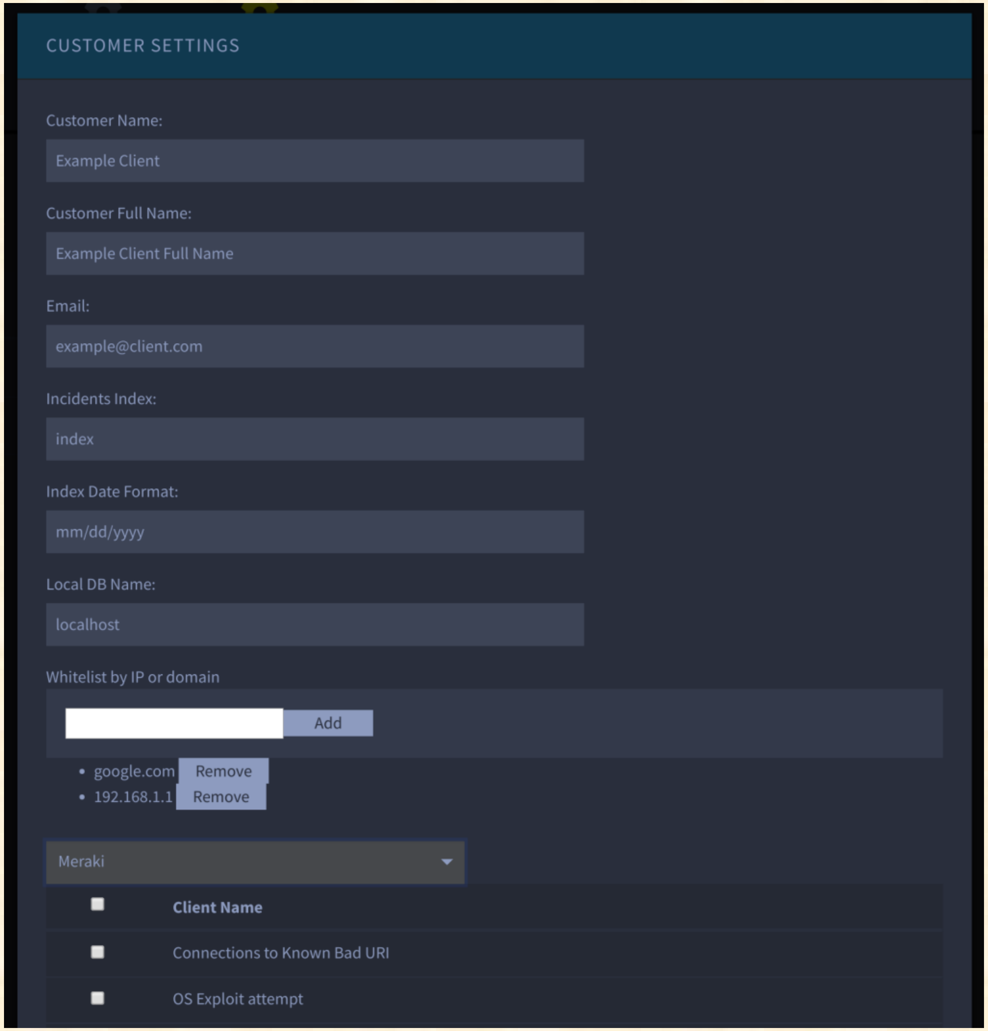
CLIENT PROFILES

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@asdfksd.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

Add/Edit Client Modal



CUSTOMER SETTINGS

Customer Name: Example Client

Customer Full Name: Example Client Full Name

Email: example@client.com

Incidents Index: index

Index Date Format: mm/dd/yyyy

Local DB Name: localhost

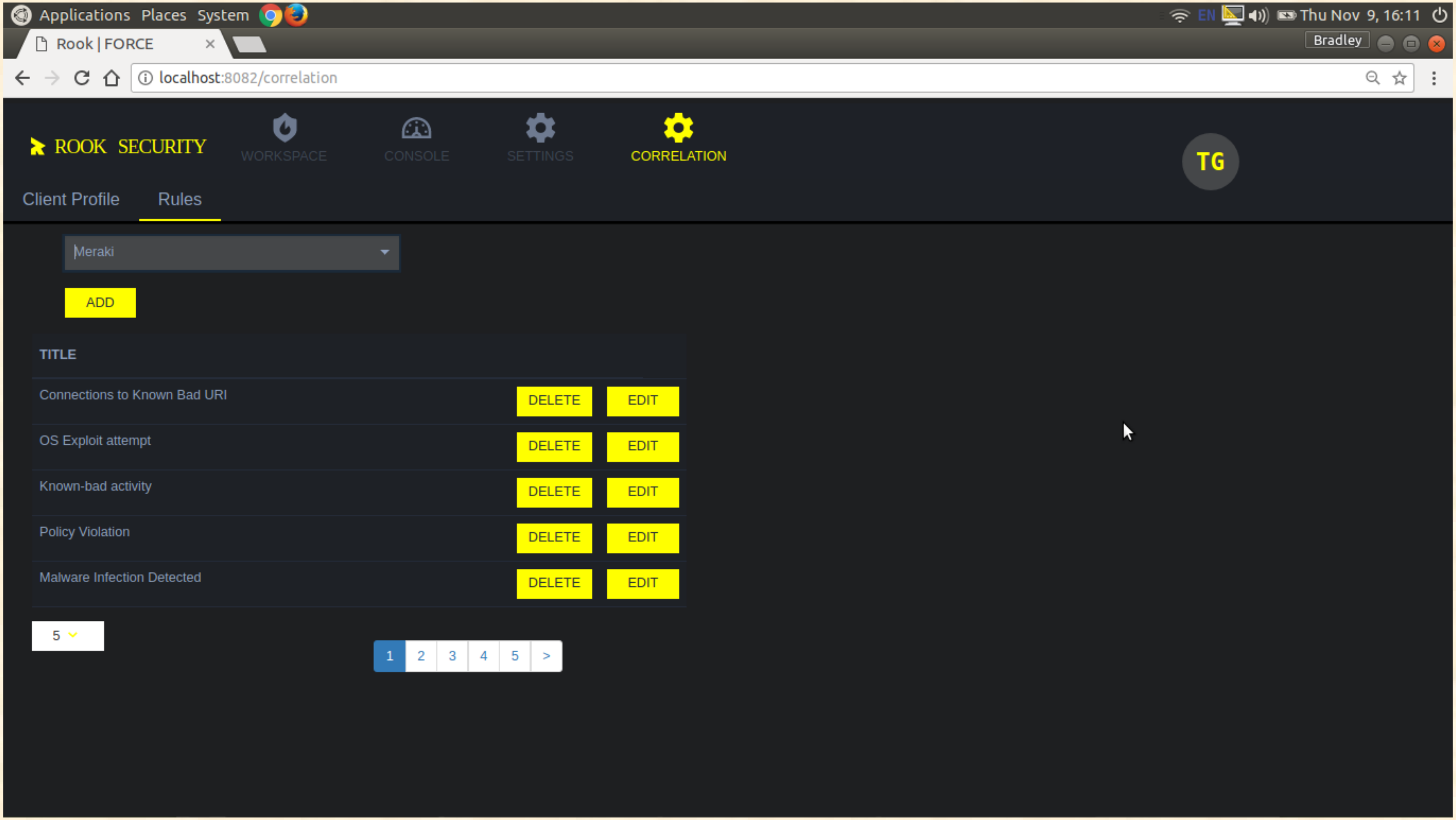
Whitelist by IP or domain

- google.com Remove
- 192.168.1.1 Remove

Meraki

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

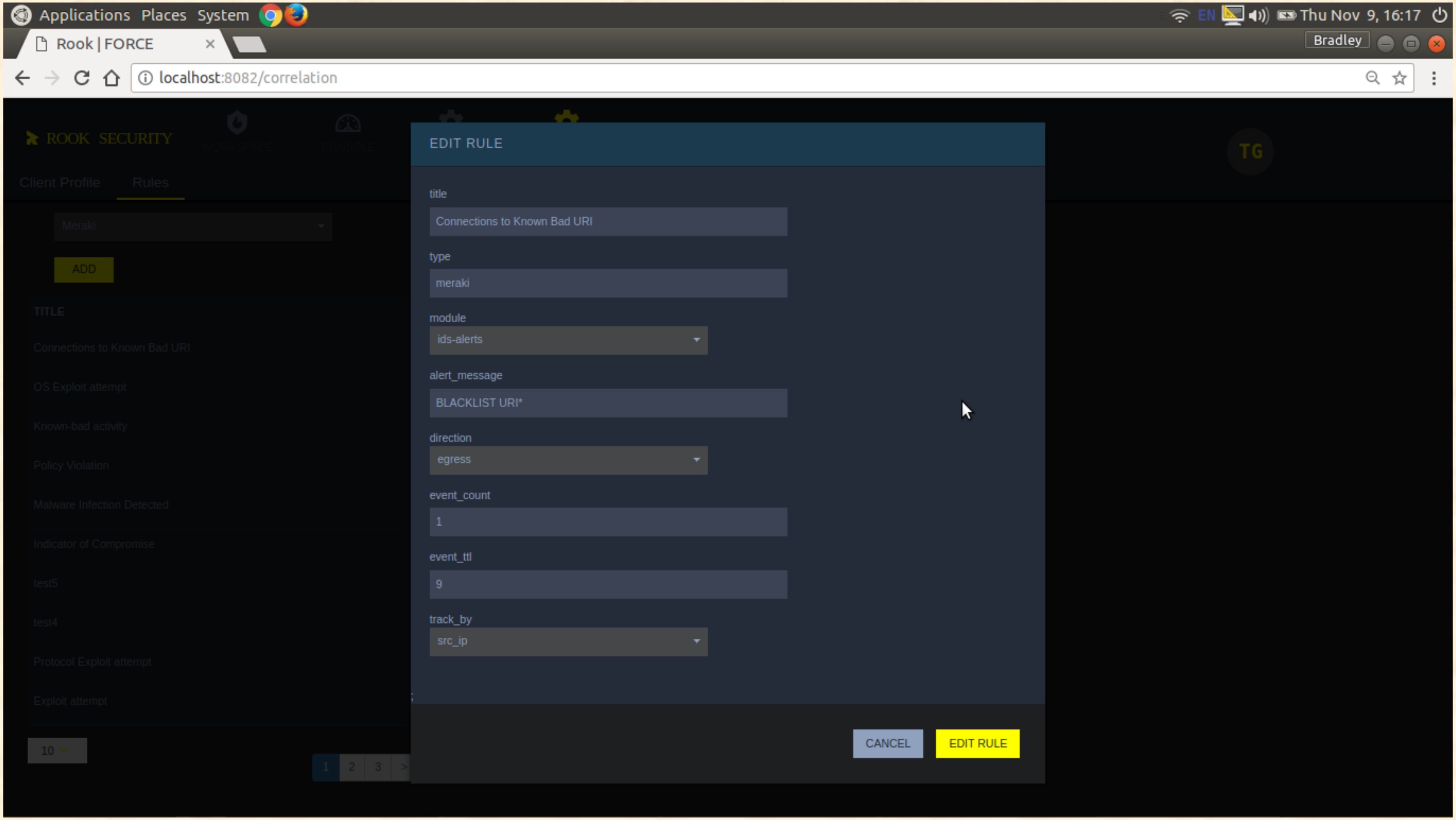
Rules Page



Meraki

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

Add/Edit Rule Modal



TITLE

Connections to Known Bad URI

OS Exploit attempt

Known-bad activity

Policy Violation

Malware Infection Detected

Indicator of Compromise

test5

test4

Protocol Exploit attempt

Exploit attempt

EDIT RULE

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

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?

? ? ? ?

? ?

? ? ?