MICHIGAN STATE UNIVERSITY

Beta Presentation

Force Platform Ingestion Tool

The Capstone Experience

Team Rook

Roy Barnes
Matt Hammerly
Will McGee
Chiyu Song
Mark Velez

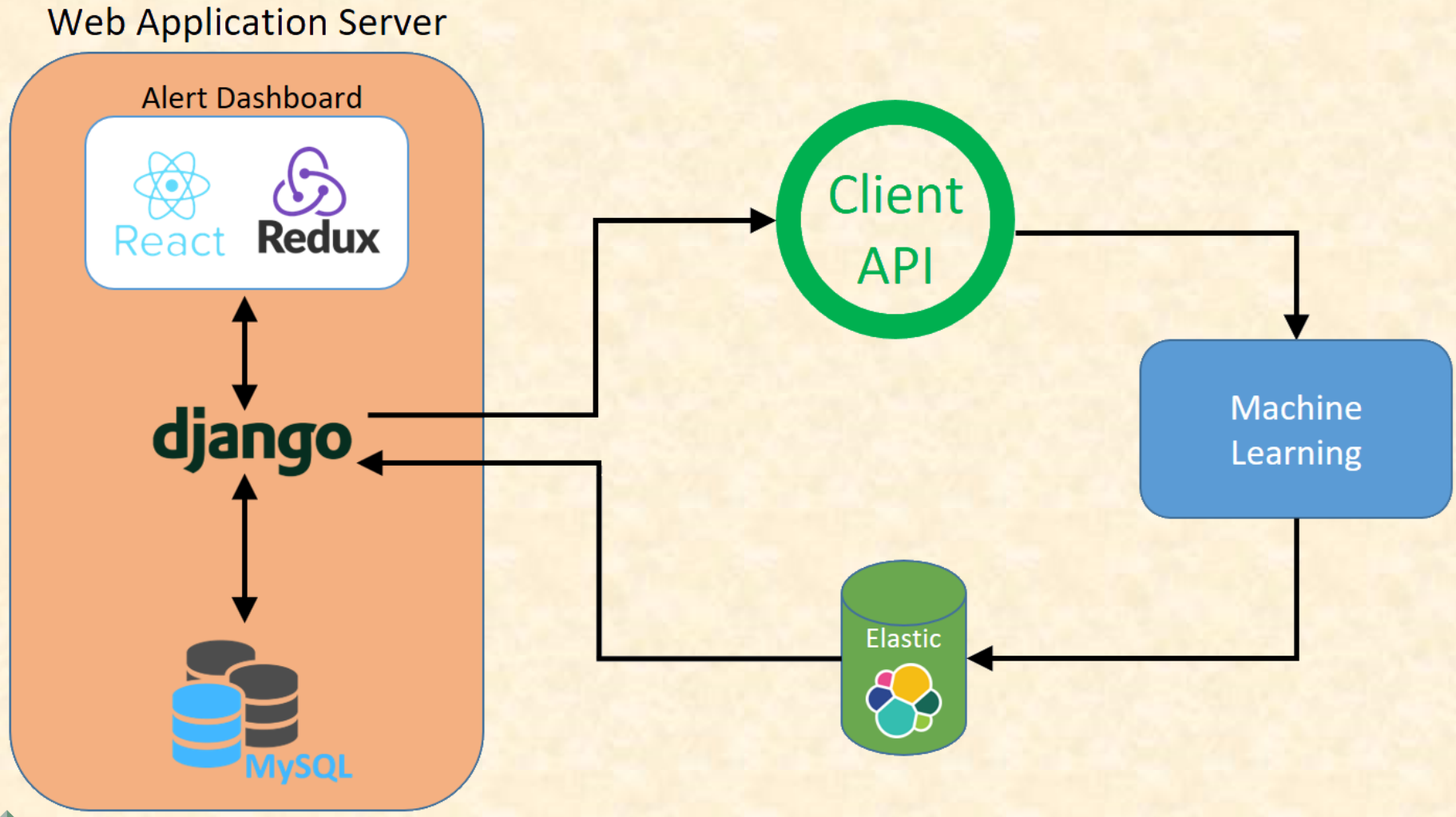
Department of Computer Science and Engineering
Michigan State University

Spring 2017

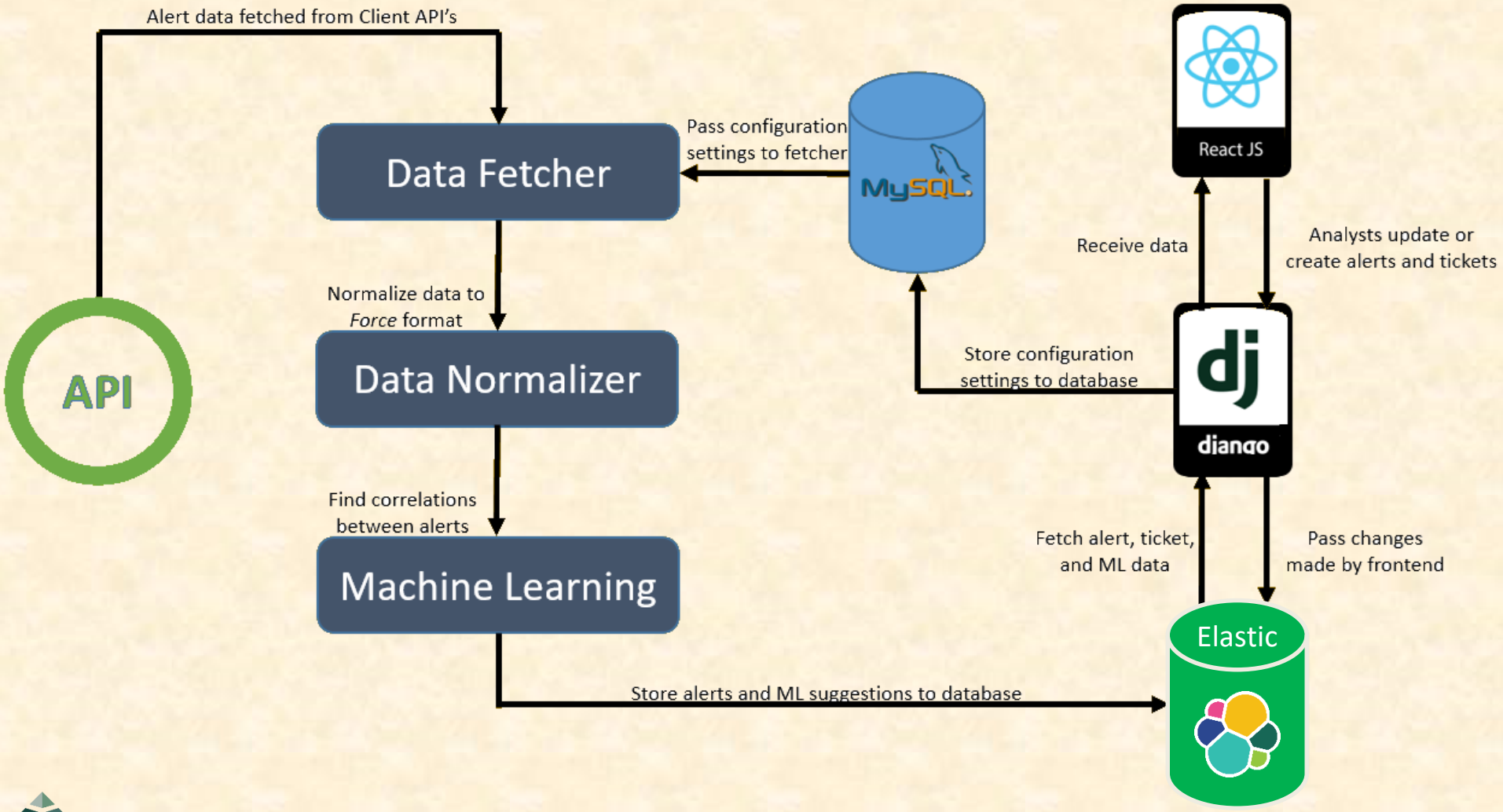
Project Overview

- Force platform for security alert management/analysis
- Force accepts data in one format, but clients send data in different formats
- Force PIT provides a way for clients to integrate existing monitoring tools with Force
- Suggests groups of related alerts to save Rook analysts time

System Architecture



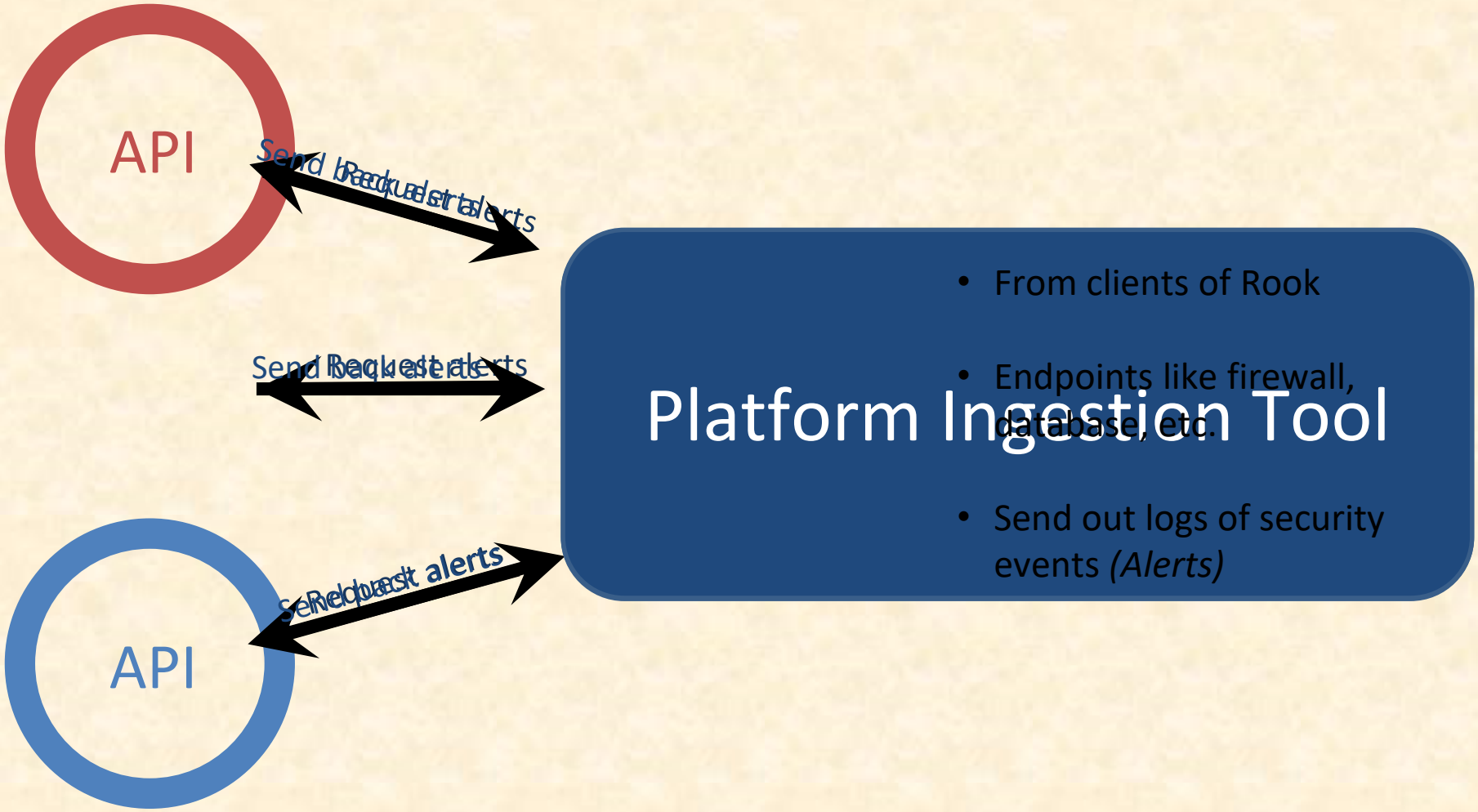
Data Flow Diagram



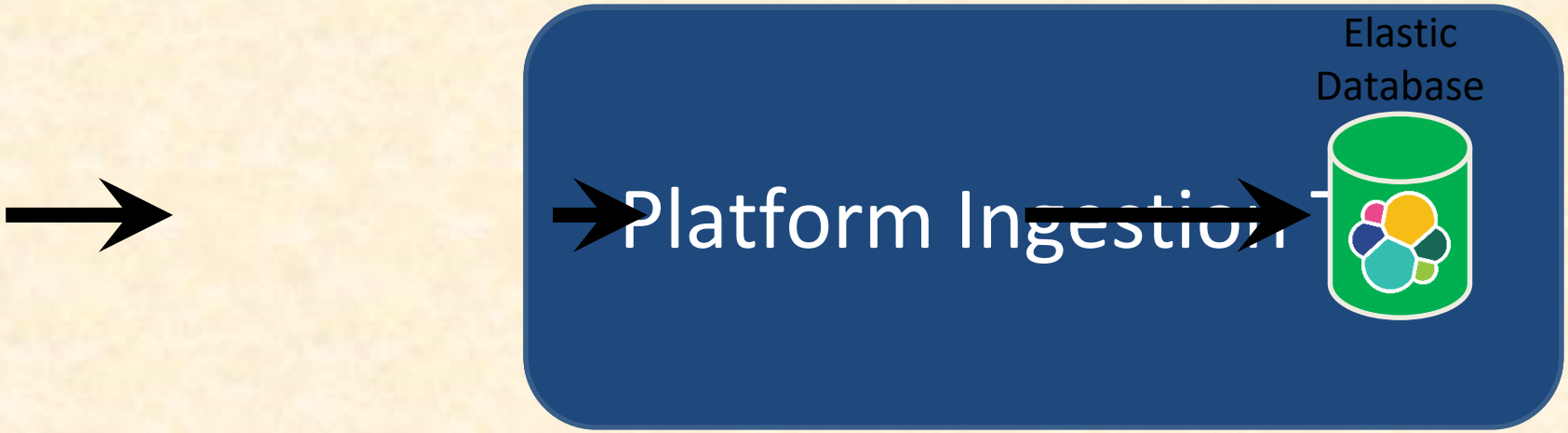
Data Flow Diagram

Brief presentation of Data Flow

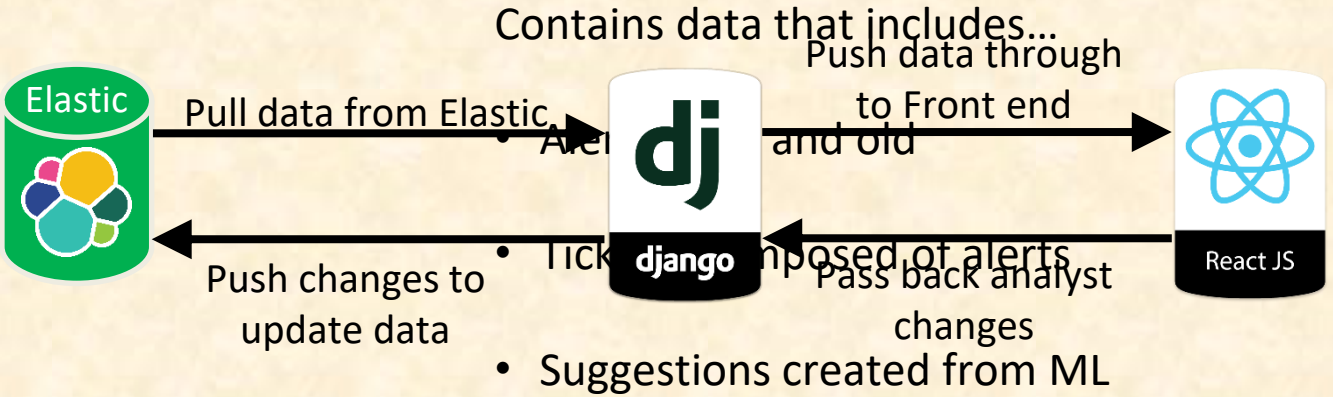
Data Flow Walkthrough



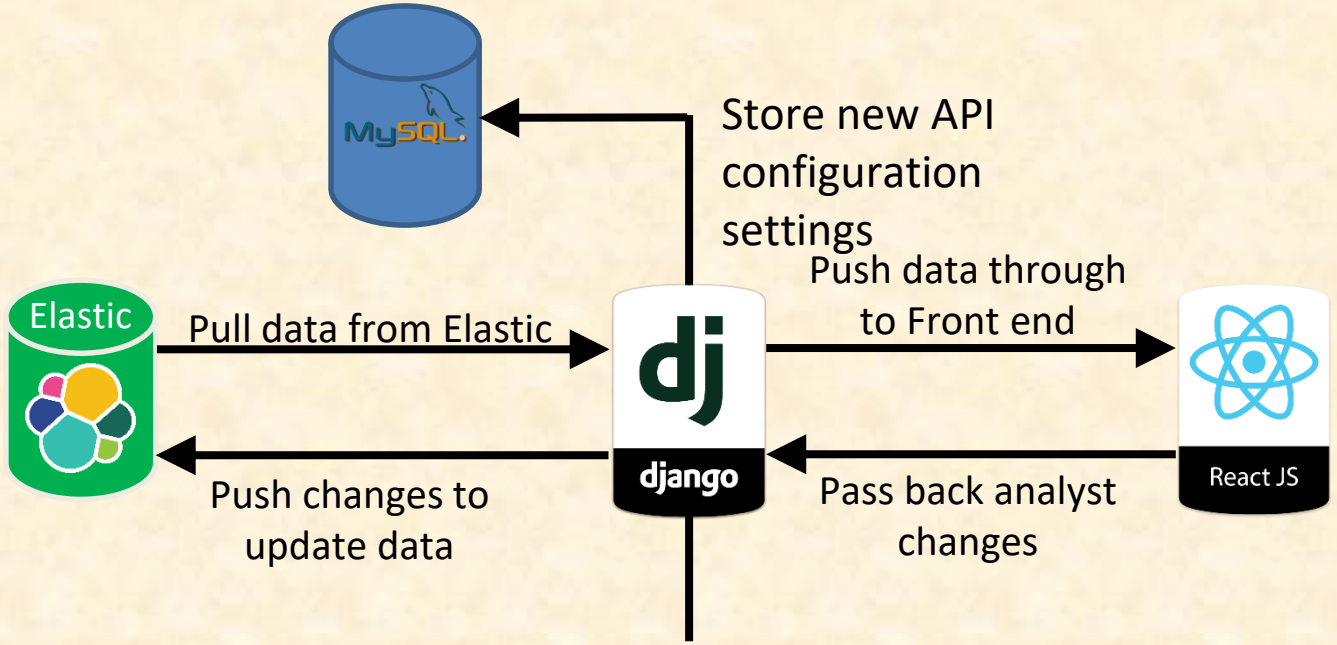
Data Flow Walkthrough (cont.)



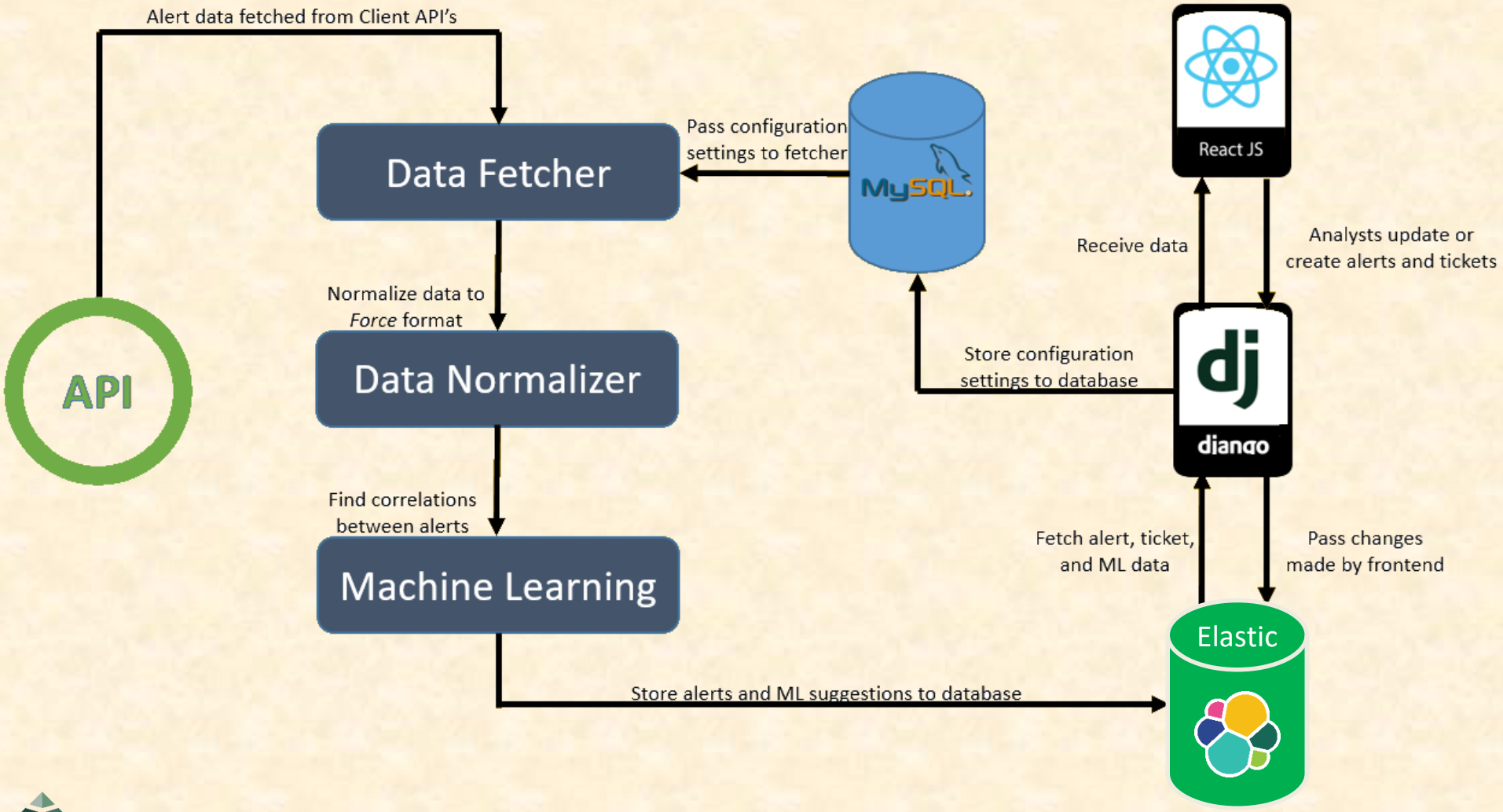
Data Flow Walkthrough (cont.)



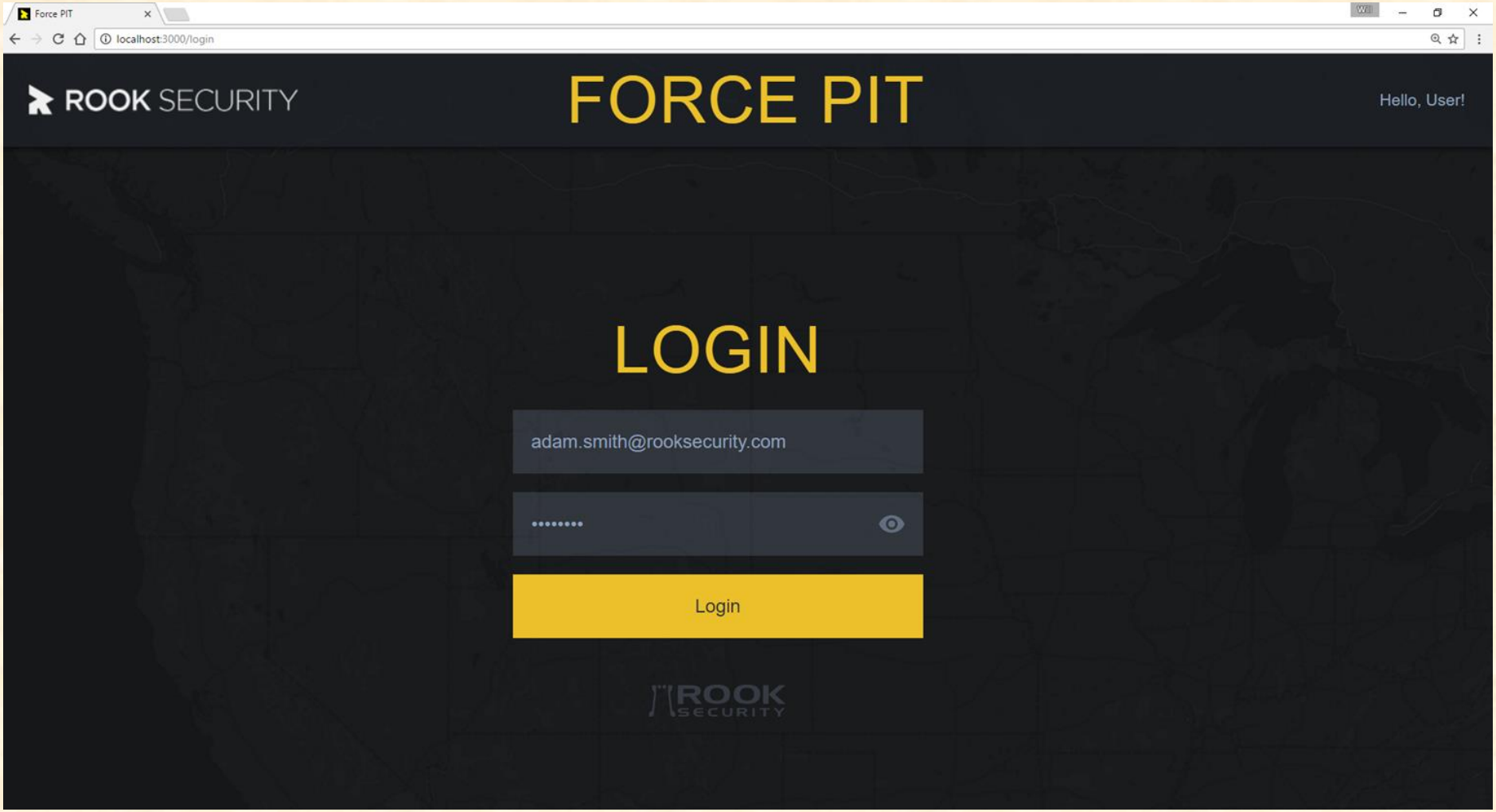
Data Flow Walkthrough (cont.)



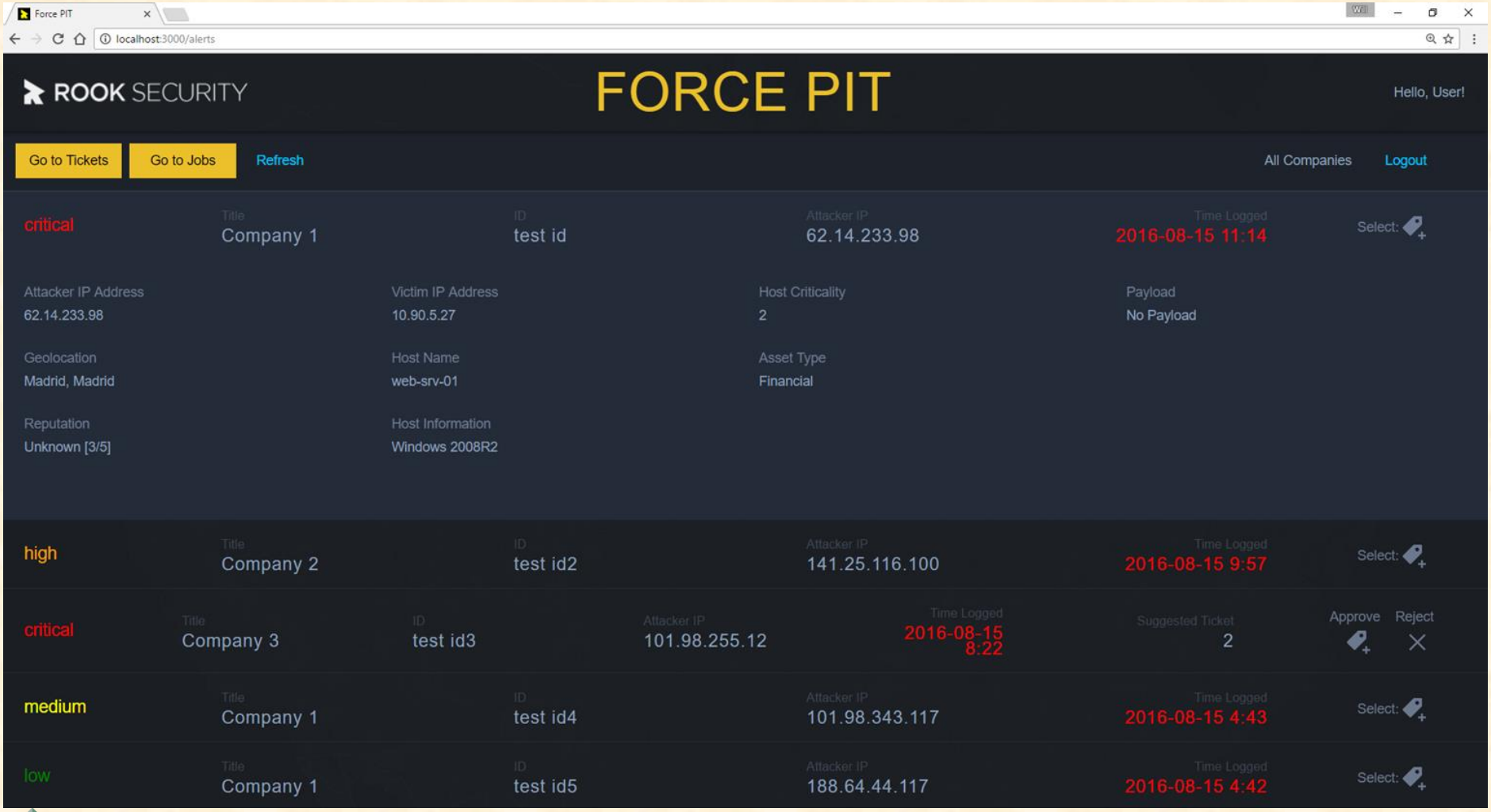
Data Flow Diagram



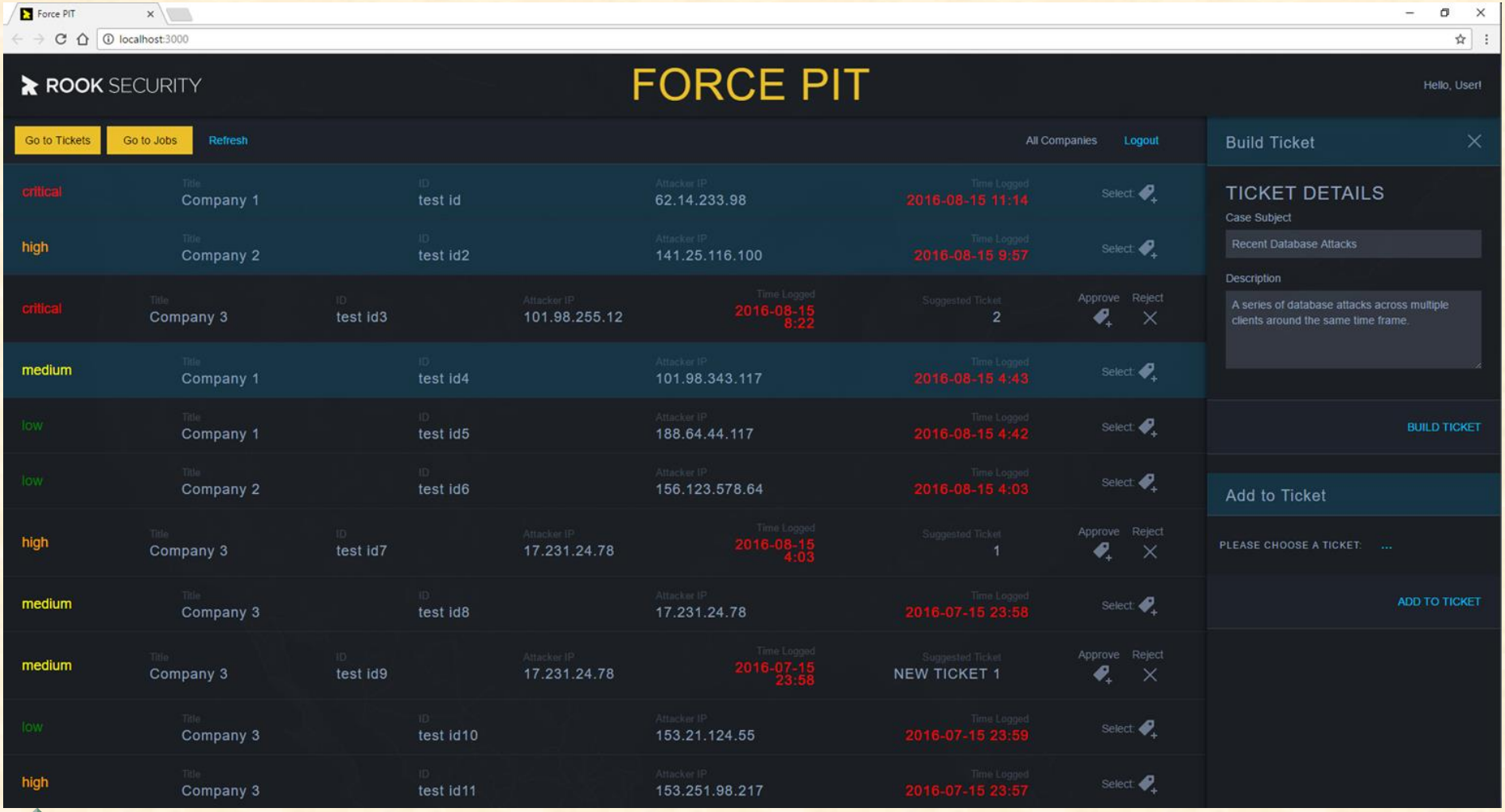
Login Page


Force PIT
localhost:3000/login
ROOK SECURITY
FORCE PIT
Hello, User!
LOGIN
adam.smith@rooksecurity.com
Login
ROOK SECURITY

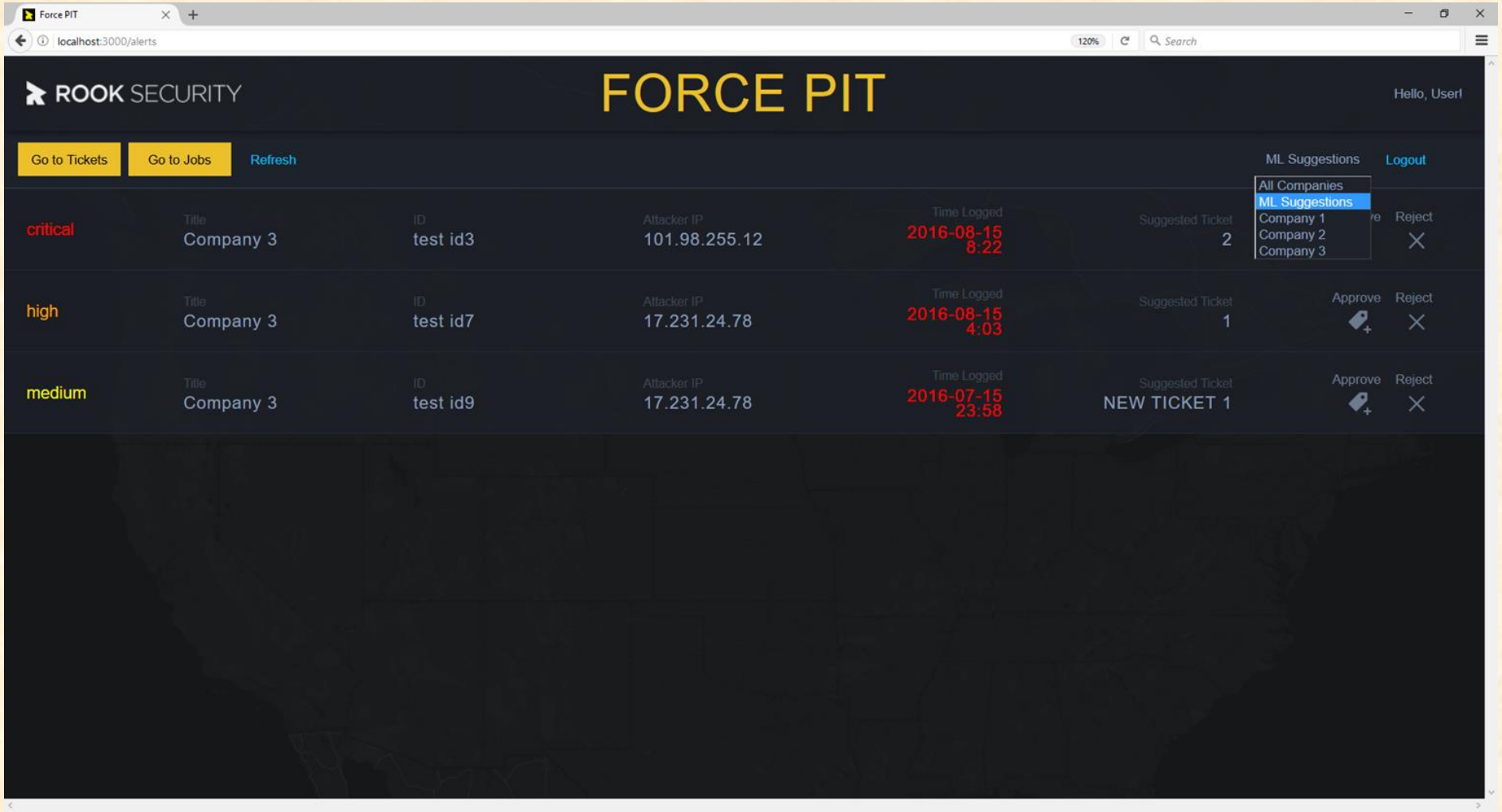
Alerts Page


Force PIT
localhost:3000/alerts
ROOK SECURITY
FORCE PIT
Hello, User!
Go to Tickets
Go to Jobs
Refresh
All Companies
Logout
critical
Title
Company 1
ID
test id
Attacker IP
62.14.233.98
Time Logged
2016-08-15 11:14
Select:
Attacker IP Address
62.14.233.98
Victim IP Address
10.90.5.27
Host Criticality
2
Payload
No Payload
Geolocation
Madrid, Madrid
Host Name
web-srv-01
Asset Type
Financial
Reputation
Unknown [3/5]
Host Information
Windows 2008R2
high
Company 2
test id2
141.25.116.100
2016-08-15 9:57
critical
Company 3
test id3
101.98.255.12
2016-08-15 8:22
Suggested Ticket
2
Approve
Reject
medium
Company 1
test id4
101.98.343.117
2016-08-15 4:43
low
Company 1
test id5
188.64.44.117
2016-08-15 4:42

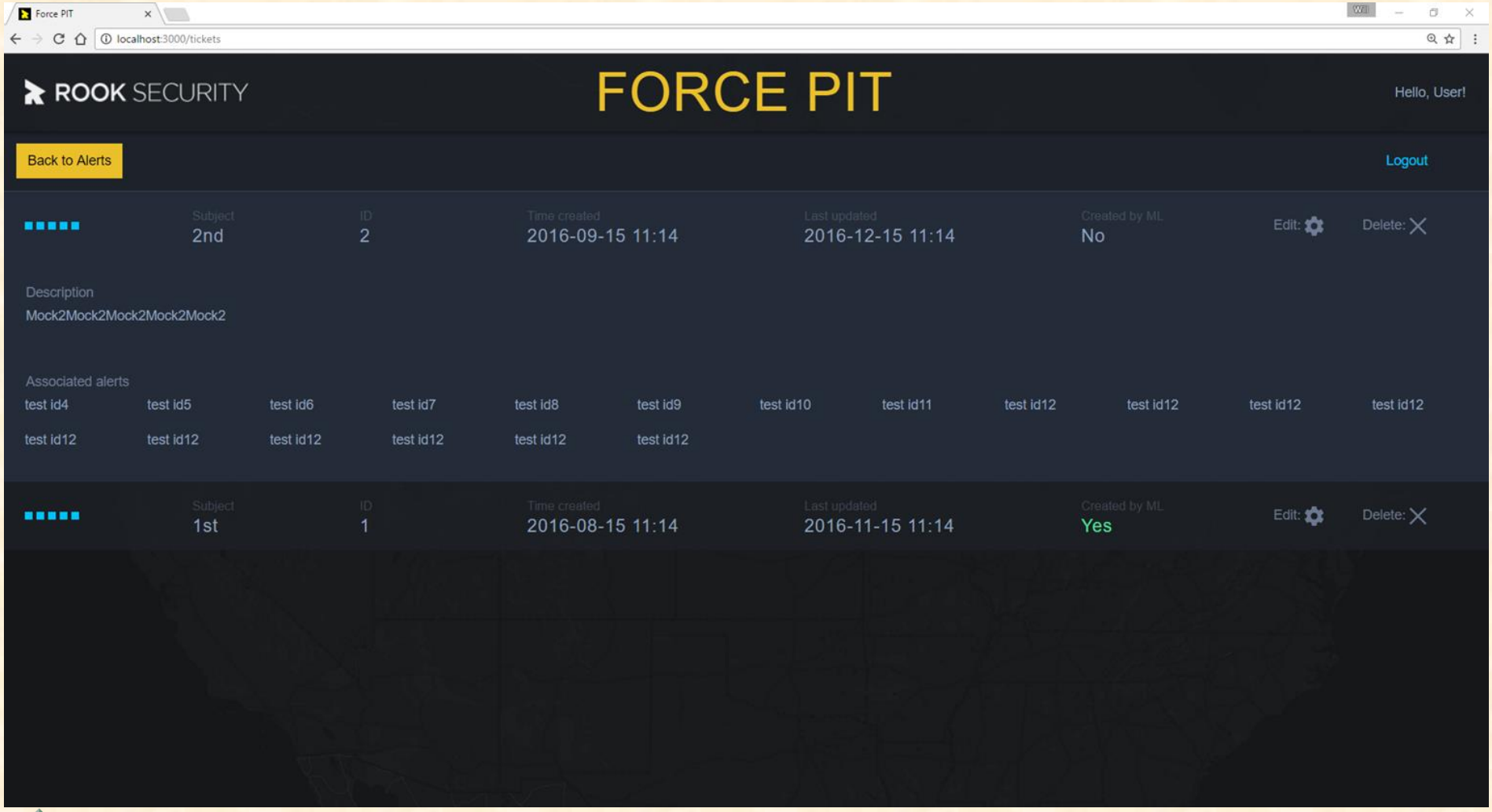
Alerts Page – Ticket Panel



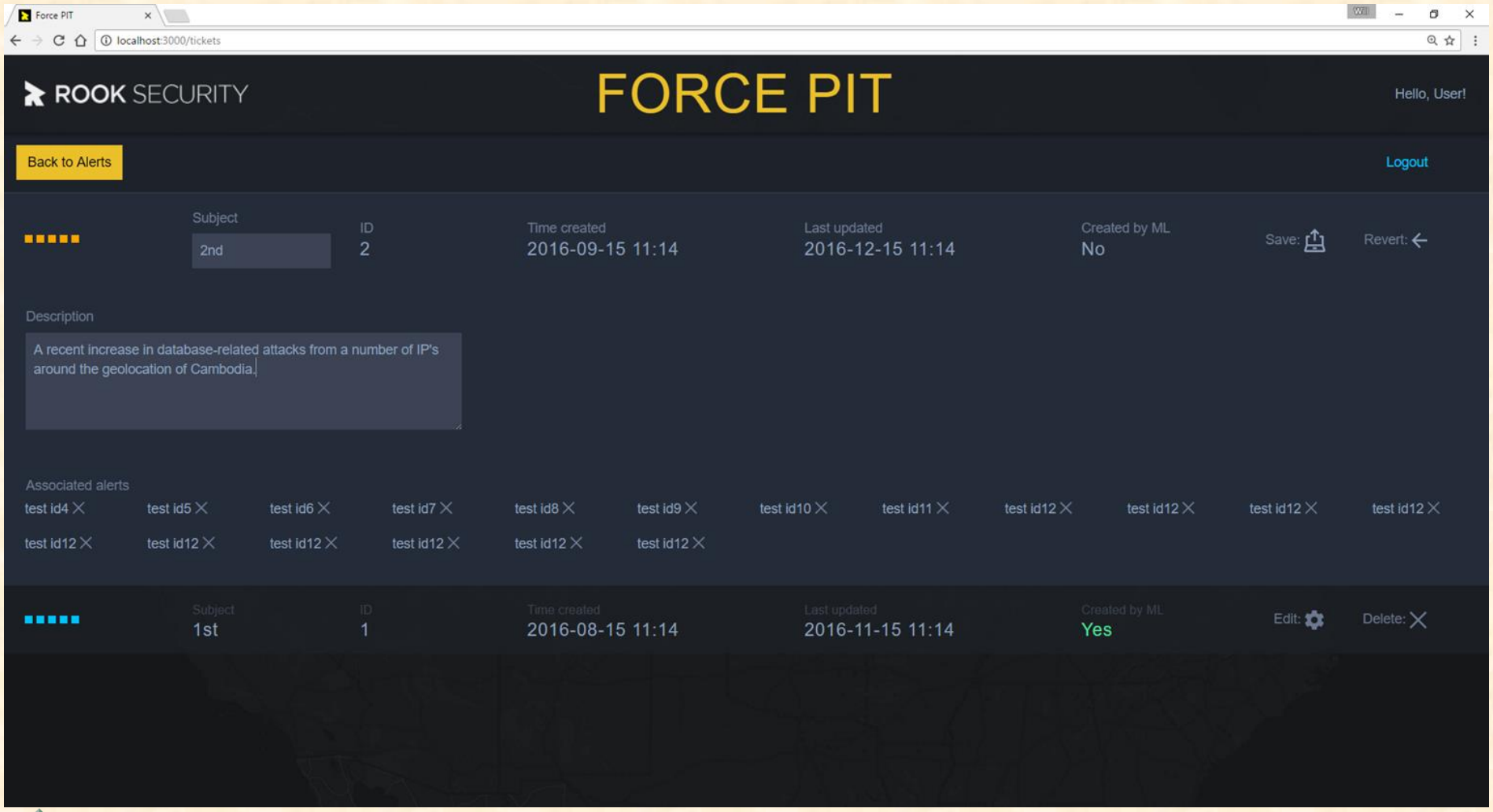
Alerts - Filtered



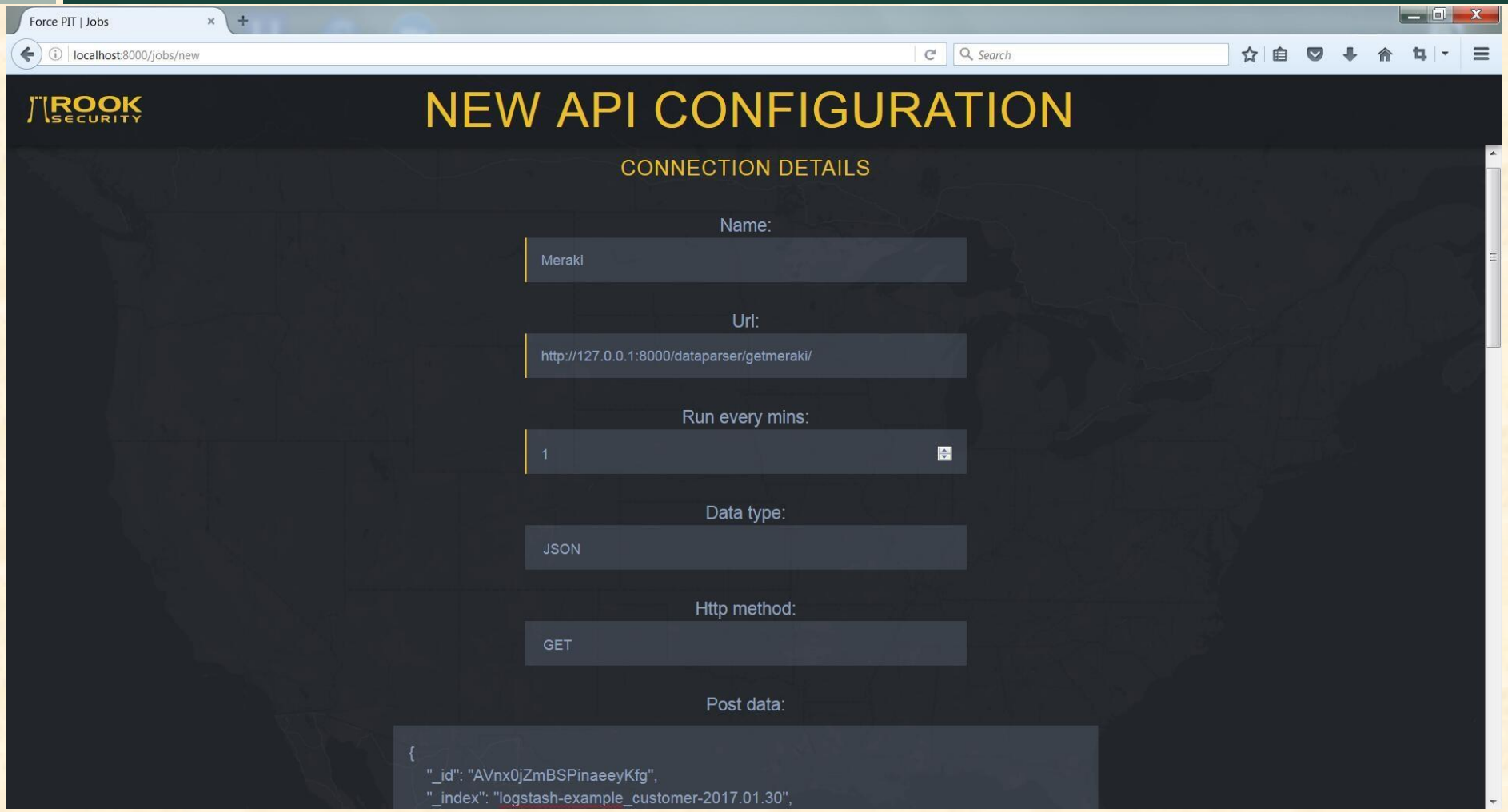
Tickets Page



Tickets - Editing Ticket



Jobs Page


Force PIT | Jobs
localhost:8000/jobs/new
Search
ROOK SECURITY
NEW API CONFIGURATION
CONNECTION DETAILS
Name:
Meraki
Url:
http://127.0.0.1:8000/dataparser/getmeraki/
Run every mins:
1
Data type:
JSON
Http method:
GET
Post data:
{
"_id": "AVnx0jZmBSPinaeeyKfg",
"_index": "logstash-example_customer-2017.01.30",

What's left to do?

- Update color scheme to Rook's updated colors
- Continue building out support for more types of APIs

Questions?