

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



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

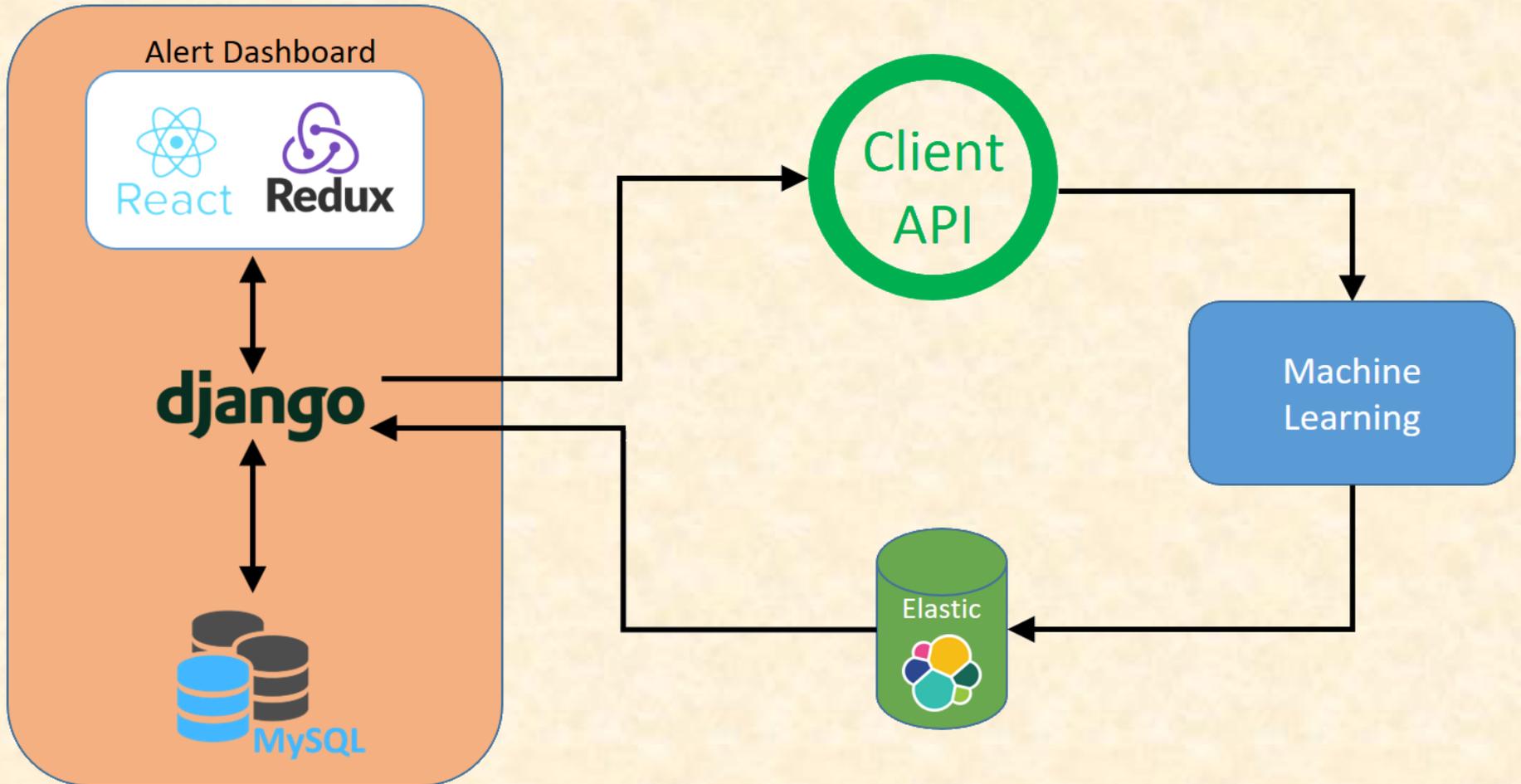
Project Overview

- 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

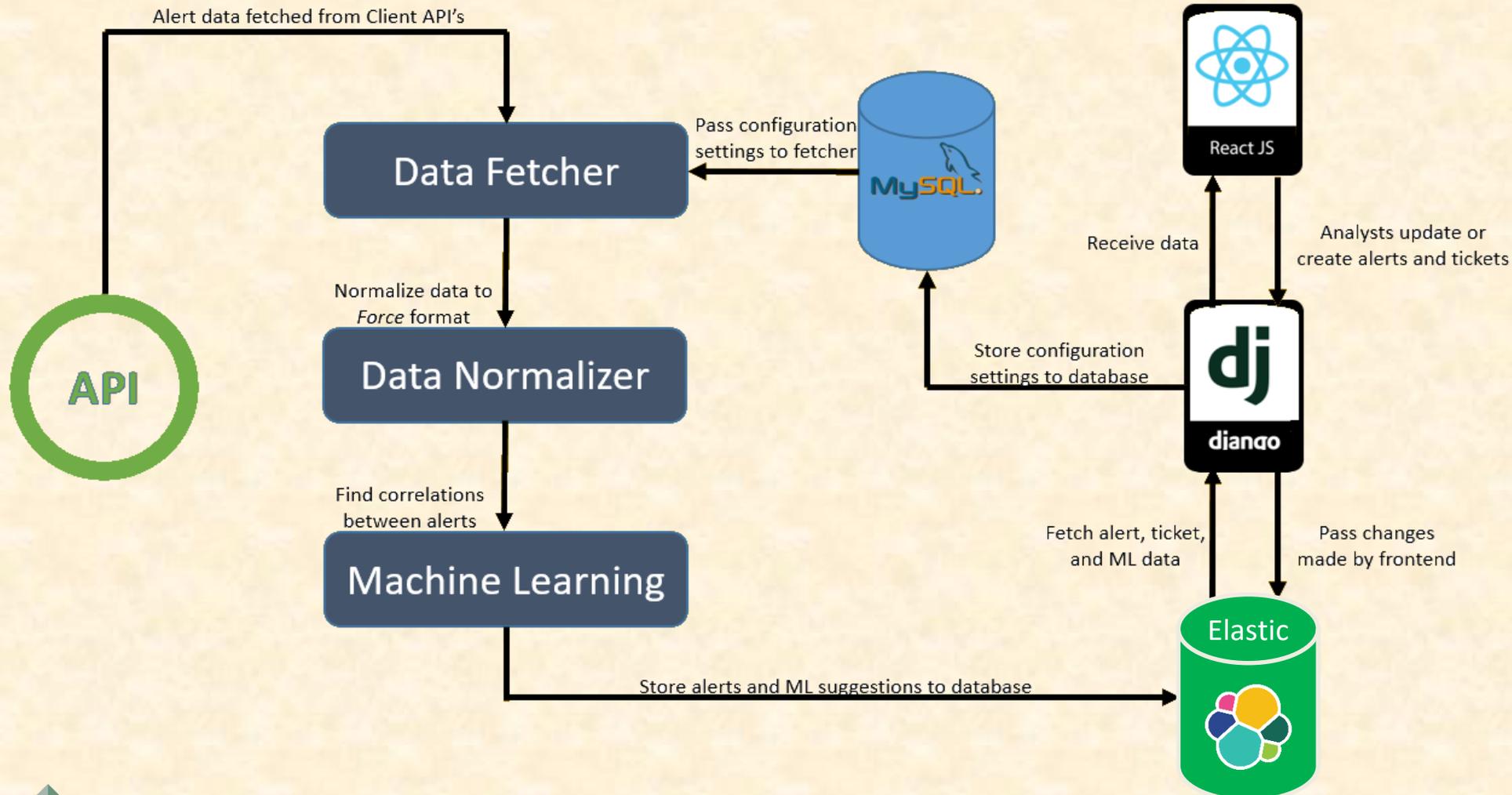


System Architecture

Web Application Server



Data Flow Diagram

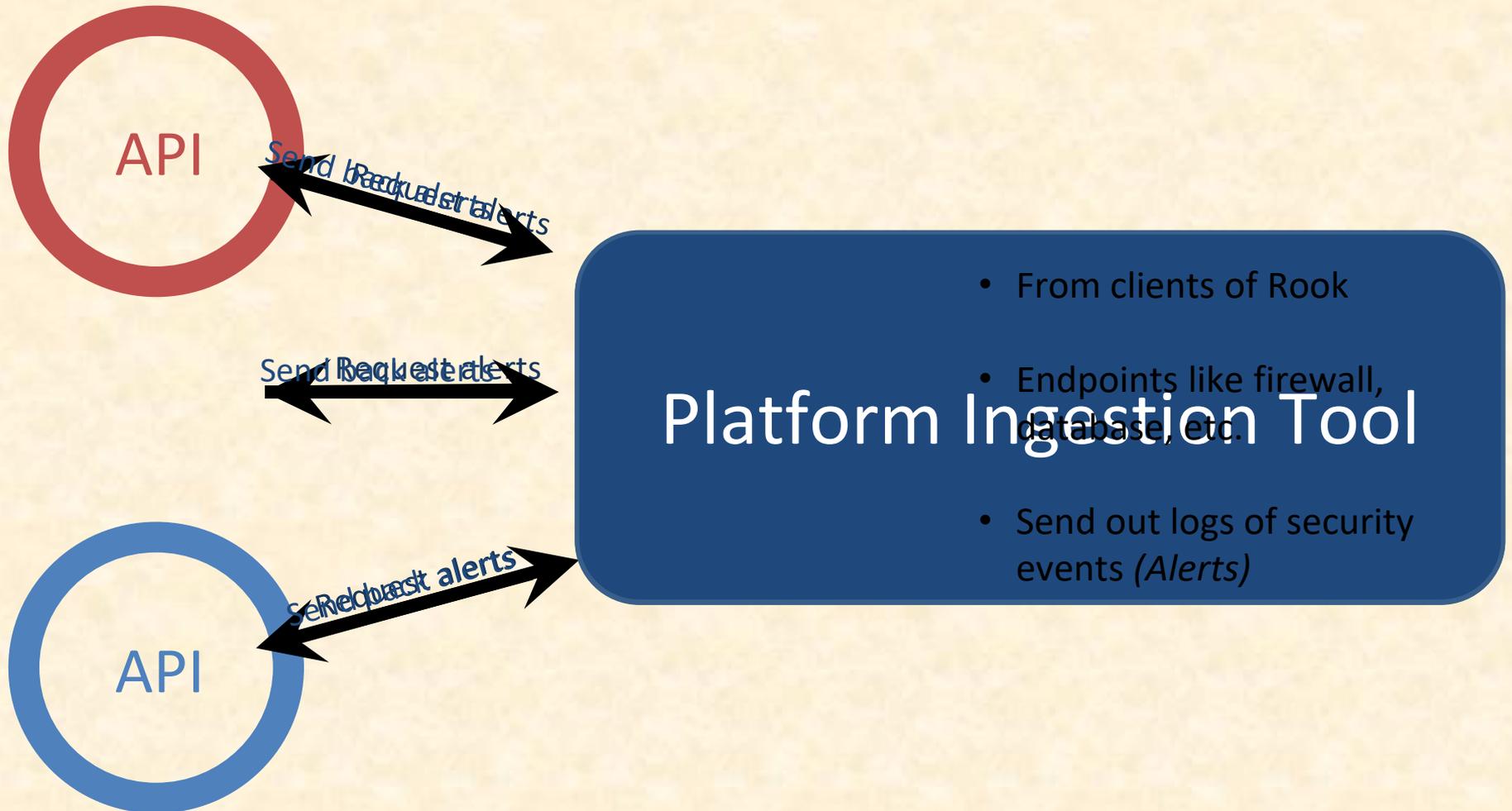


Data Flow Diagram

Brief presentation of Data Flow



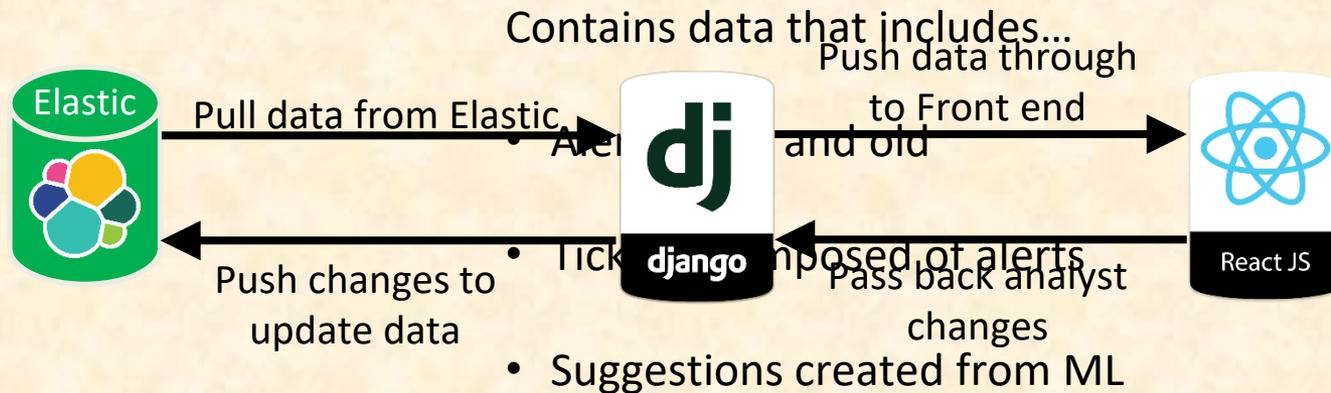
Data Flow Walkthrough



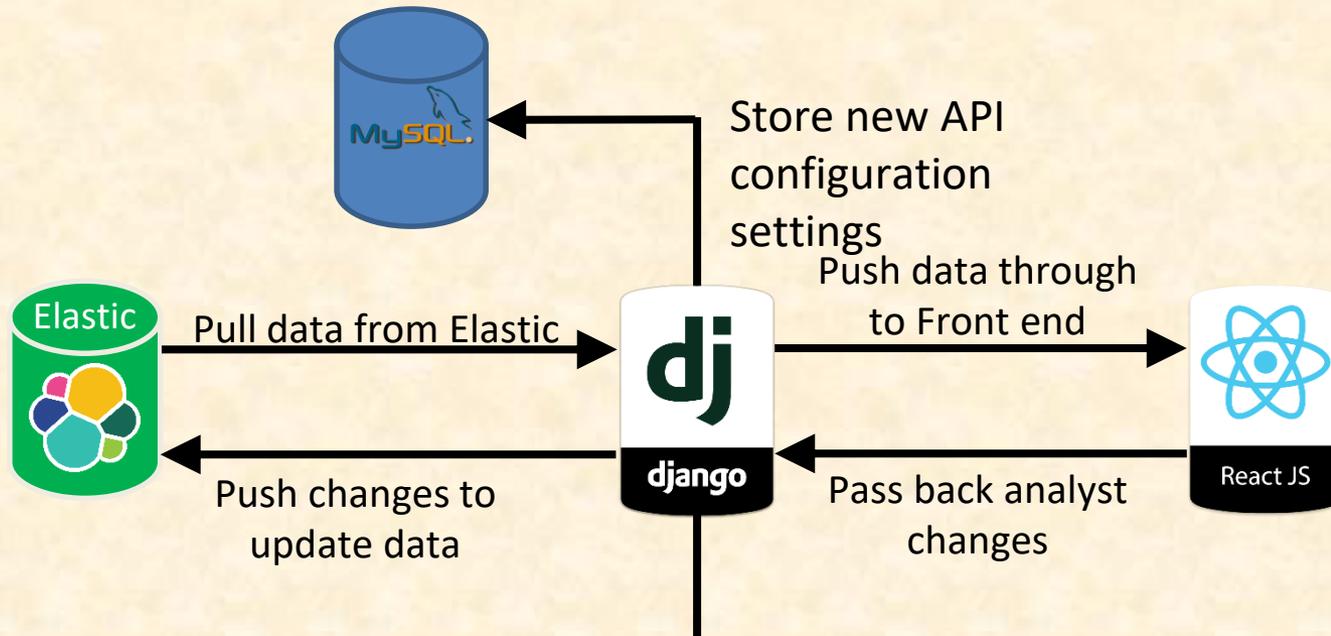
Data Flow Walkthrough (cont.)



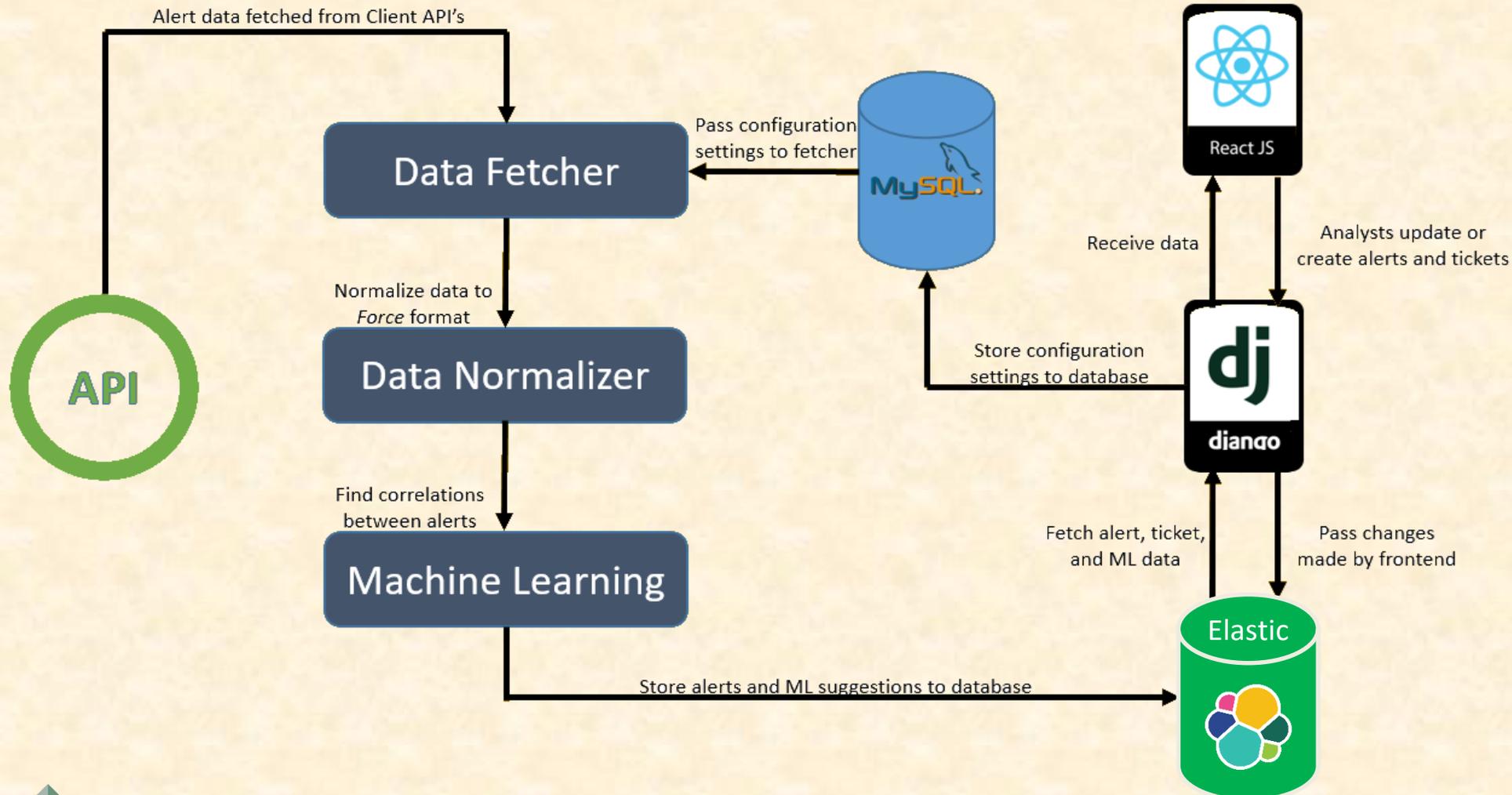
Data Flow Walkthrough (cont.)



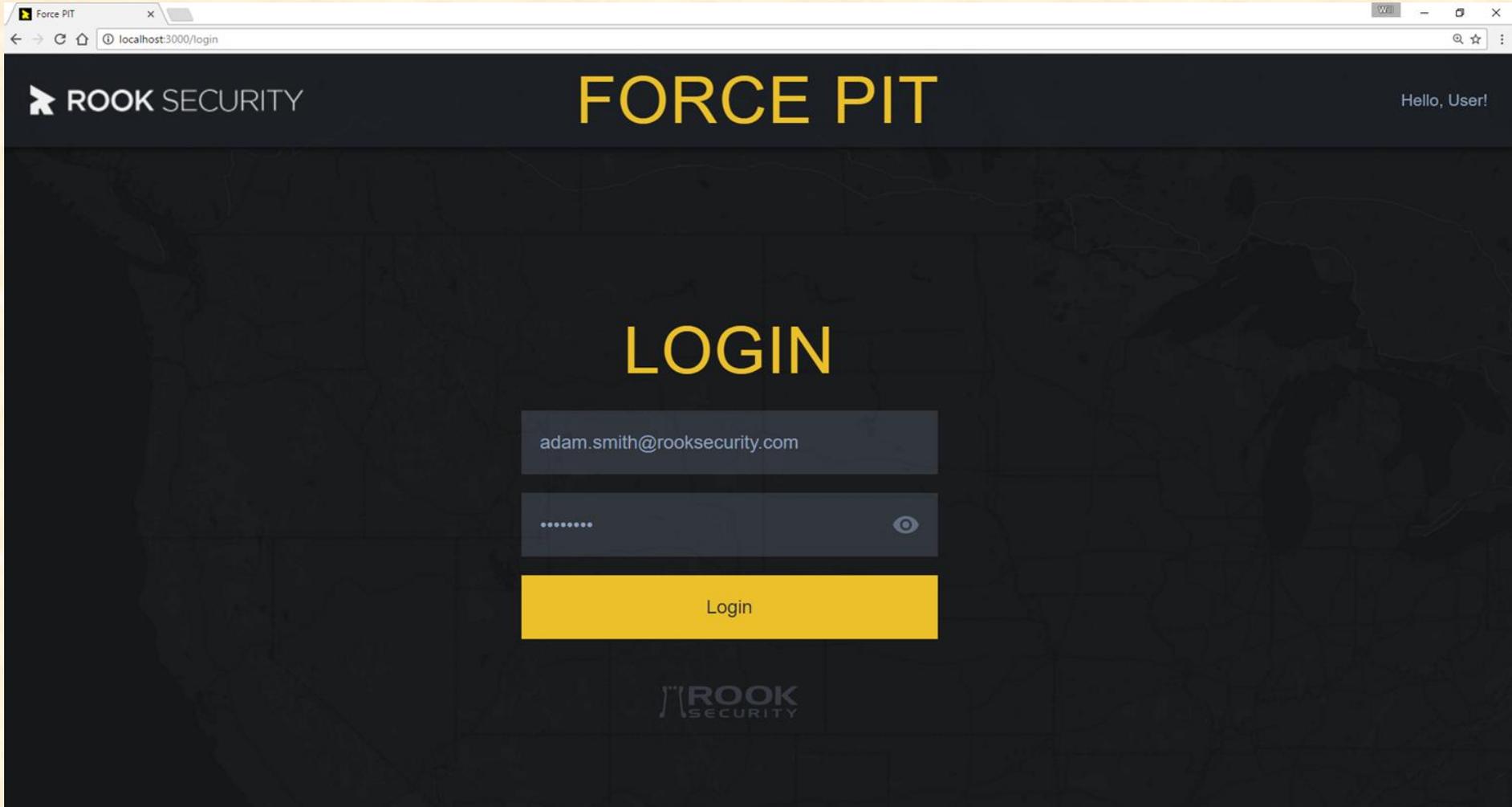
Data Flow Walkthrough (cont.)



Data Flow Diagram



Login Page



Alerts Page

The screenshot shows a web browser window with the URL `localhost:3000/alerts`. The page header includes the Rook Security logo, the title "FORCE PIT", and a user greeting "Hello, User!". Navigation buttons for "Go to Tickets", "Go to Jobs", and "Refresh" are visible, along with "All Companies" and "Logout" links.

Severity	Title	ID	Attacker IP	Time Logged	Select
critical	Company 1	test id	62.14.233.98	2016-08-15 11:14	Select: +
Alert Details:					
Attacker IP Address		Victim IP Address		Host Criticality	
62.14.233.98		10.90.5.27		2	
Geolocation		Host Name		Asset Type	
Madrid, Madrid		web-srv-01		Financial	
Reputation		Host Information			
Unknown [3/5]		Windows 2008R2			
high	Company 2	test id2	141.25.116.100	2016-08-15 9:57	Select: +
critical	Company 3	test id3	101.98.255.12	2016-08-15 8:22	Suggested Ticket: 2, Approve: +, Reject: X
medium	Company 1	test id4	101.98.343.117	2016-08-15 4:43	Select: +
low	Company 1	test id5	188.64.44.117	2016-08-15 4:42	Select: +



Alerts Page – Ticket Panel

The screenshot displays the Force PIT interface. At the top, there's a navigation bar with 'ROOK SECURITY' and 'FORCE PIT' in large yellow letters. Below this, a table lists various alerts with columns for severity, title, ID, attacker IP, time logged, and suggested tickets. A right-hand panel titled 'TICKET DETAILS' is open, showing information for a 'Recent Database Attacks' ticket, including a description of database attacks across multiple clients.

Severity	Title	ID	Attacker IP	Time Logged	Suggested Ticket	Actions
critical	Company 1	test id	62.14.233.98	2016-08-15 11:14		Select: +
high	Company 2	test id2	141.25.116.100	2016-08-15 9:57		Select: +
critical	Company 3	test id3	101.98.255.12	2016-08-15 8:22	2	Approve +, Reject X
medium	Company 1	test id4	101.98.343.117	2016-08-15 4:43		Select: +
low	Company 1	test id5	188.64.44.117	2016-08-15 4:42		Select: +
low	Company 2	test id6	156.123.578.64	2016-08-15 4:03		Select: +
high	Company 3	test id7	17.231.24.78	2016-08-15 4:03	1	Approve +, Reject X
medium	Company 3	test id8	17.231.24.78	2016-07-15 23:58		Select: +
medium	Company 3	test id9	17.231.24.78	2016-07-15 23:58	NEW TICKET 1	Approve +, Reject X
low	Company 3	test id10	153.21.124.55	2016-07-15 23:59		Select: +
high	Company 3	test id11	153.251.98.217	2016-07-15 23:57		Select: +

TICKET DETAILS
 Case Subject: Recent Database Attacks
 Description: A series of database attacks across multiple clients around the same time frame.

Buttons: BUILD TICKET, ADD TO TICKET, PLEASE CHOOSE A TICKET...



Alerts - Filtered

The screenshot displays the Force PIT web application interface. The browser address bar shows 'localhost:3000/alerts'. The application header includes the Rook Security logo and the title 'FORCE PIT'. A navigation bar contains buttons for 'Go to Tickets', 'Go to Jobs', and 'Refresh'. The main content area shows a table of filtered alerts. The table has columns for severity, title, ID, attacker IP, time logged, suggested ticket, and actions. A dropdown menu is open over the 'ML Suggestions' column, showing options for 'All Companies', 'ML Suggestions', 'Company 1', 'Company 2', and 'Company 3'. The 'ML Suggestions' option is currently selected.

Severity	Title	ID	Attacker IP	Time Logged	Suggested Ticket	Actions
critical	Company 3	test id3	101.98.255.12	2016-08-15 8:22	2	ML Suggestions, Reject
high	Company 3	test id7	17.231.24.78	2016-08-15 4:03	1	Approve, Reject
medium	Company 3	test id9	17.231.24.78	2016-07-15 23:58	NEW TICKET 1	Approve, Reject



Tickets Page

The screenshot shows a web browser window with the URL `localhost:3000/tickets`. The page header includes the Rook Security logo and the title "FORCE PIT". A user is logged in, indicated by "Hello, User!" and a "Logout" link. A "Back to Alerts" button is visible on the left. The main content area displays a list of tickets. The first ticket (ID 2) has a subject of "2nd", was created on 2016-09-15 11:14, and last updated on 2016-12-15 11:14. Its description is "Mock2Mock2Mock2Mock2Mock2". The second ticket (ID 1) has a subject of "1st", was created on 2016-08-15 11:14, and last updated on 2016-11-15 11:14. Both tickets have "Edit" and "Delete" actions available.

Subject	ID	Time created	Last updated	Created by ML	Edit	Delete
2nd	2	2016-09-15 11:14	2016-12-15 11:14	No	⚙️	✖️
Description Mock2Mock2Mock2Mock2Mock2						
Associated alerts						
test id4	test id5	test id6	test id7	test id8	test id9	test id10
test id11	test id12	test id12	test id12	test id12	test id12	test id12
test id12	test id12	test id12	test id12	test id12	test id12	test id12
1st	1	2016-08-15 11:14	2016-11-15 11:14	Yes	⚙️	✖️

Tickets - Editing Ticket

The screenshot shows a web browser window with the URL `localhost:3000/tickets`. The application header includes the Rook Security logo, the title "FORCE PIT", and a user greeting "Hello, User!". A "Back to Alerts" button is visible on the left, and a "Logout" link is on the right.

The main content area displays a ticket editing form for ticket ID 2. The form includes a "Subject" field with the value "2nd", a "Time created" field with the value "2016-09-15 11:14", a "Last updated" field with the value "2016-12-15 11:14", and a "Created by ML" field with the value "No". There are "Save" and "Revert" buttons. The "Description" field contains the text: "A recent increase in database-related attacks from a number of IP's around the geolocation of Cambodia." Below the description is a section for "Associated alerts" showing a grid of 14 alert items, each labeled "test id" followed by a number and a close icon.

At the bottom of the form, there is a summary row for the ticket with the following details:

Subject	ID	Time created	Last updated	Created by ML	Edit	Delete
1st	1	2016-08-15 11:14	2016-11-15 11:14	Yes	⚙️	✖️



Jobs Page

The screenshot shows a web browser window with the URL `localhost:8000/jobs/new`. The page title is "NEW API CONFIGURATION" and the Rook Security logo is in the top left. The main heading is "CONNECTION DETAILS". The form contains the following fields:

- 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?

?

?

?

?

?

?

?

?

?

