MICHIGAN STATE
UNIVERSITY

Beta Presentation
Insider Threat Detection

The Capstone Experience

Team AppDynamics

Chris Kulpa
Andy Zhang
Sumanth Rudraraju
Ari Kohl

Department of Computer Science and Engineering
Michigan State University
Fall 2020

From Students…
…to Professionals

Project Overview

- Use AppDynamics' controller as the source of data
- Run a threat detection algorithm on the data
- The algorithm uses machine learning and kernel density estimation.
- Algorithm determines user's tendencies and finds any anomalies from those tendencies
- Display the results of the algorithm on the web app
- Allow user to take action on suspicious account

System Architecture

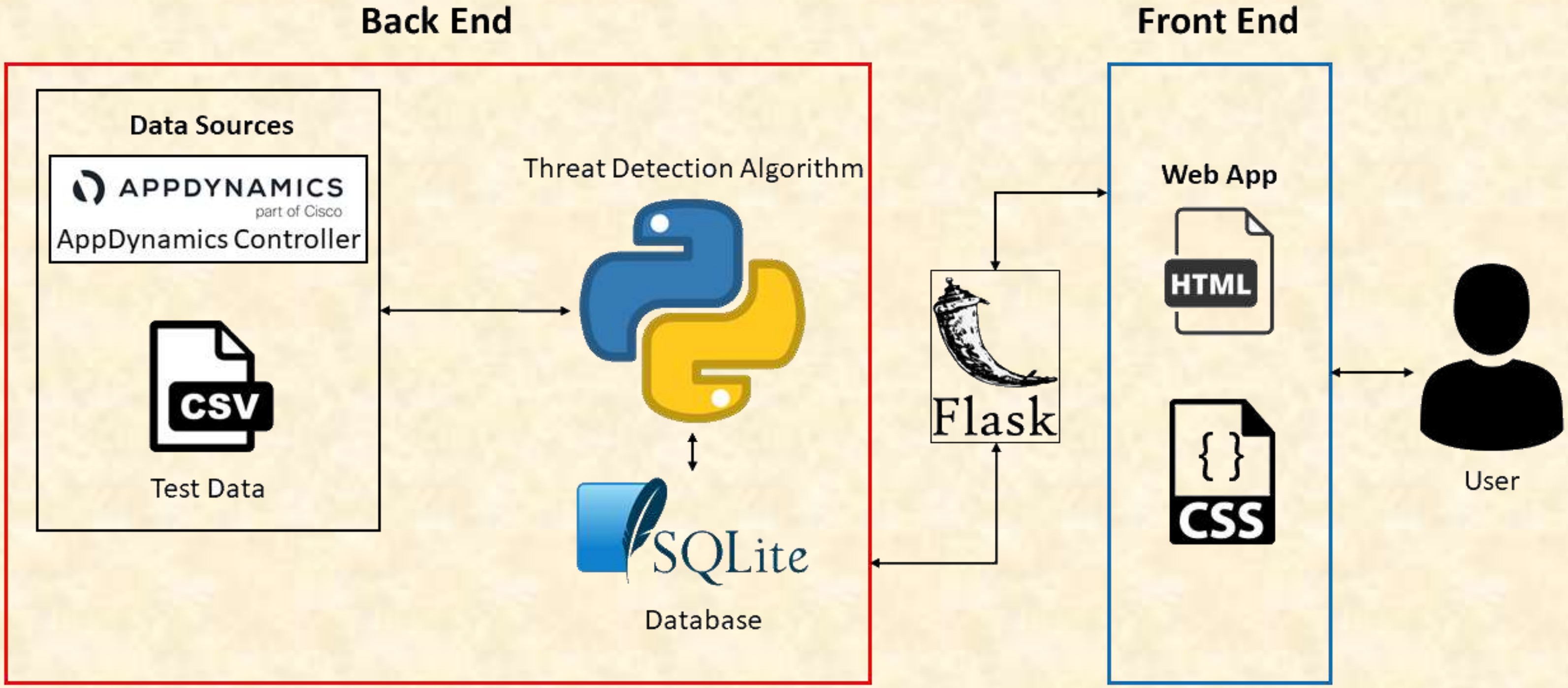
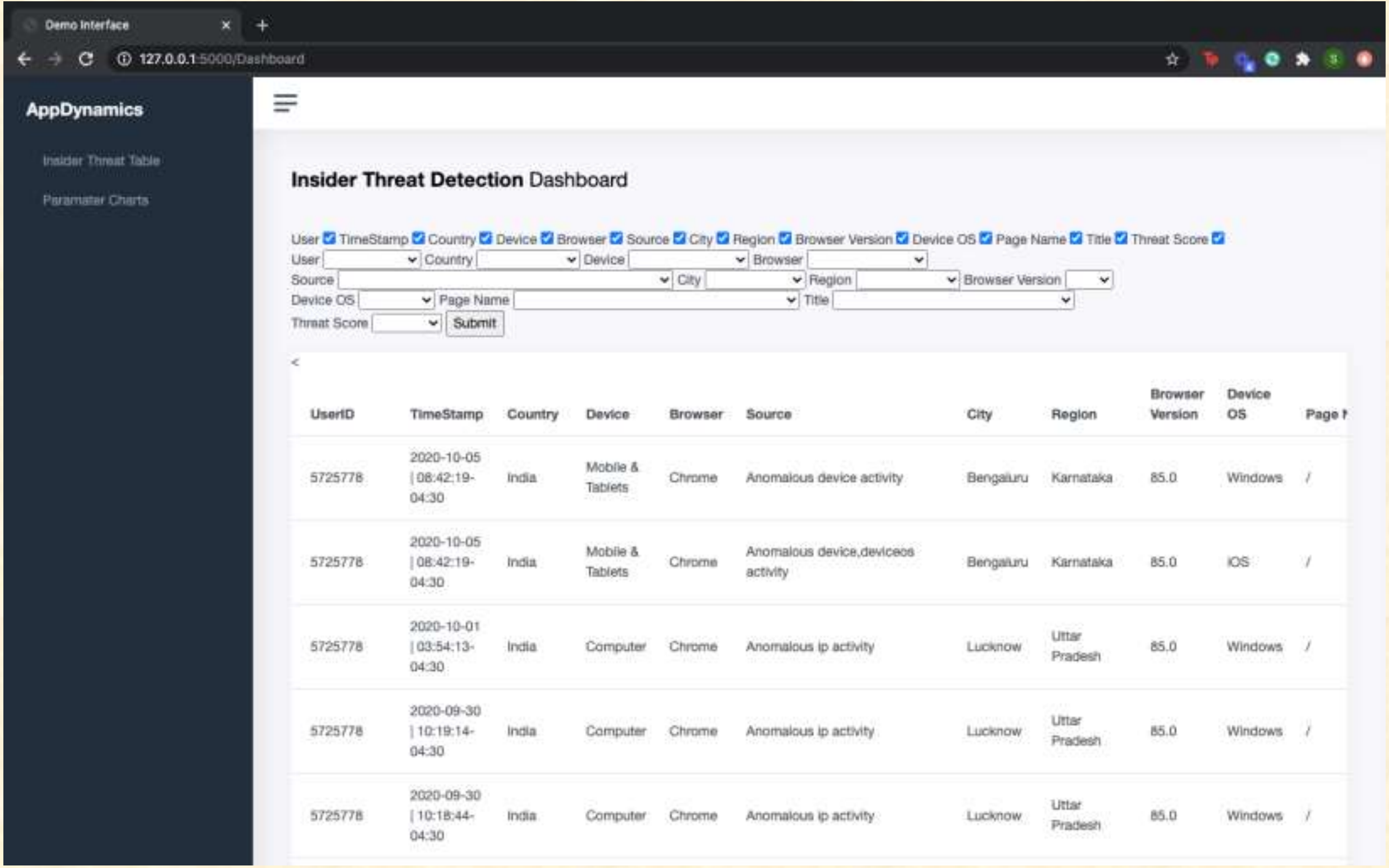


Table of Reported Activity



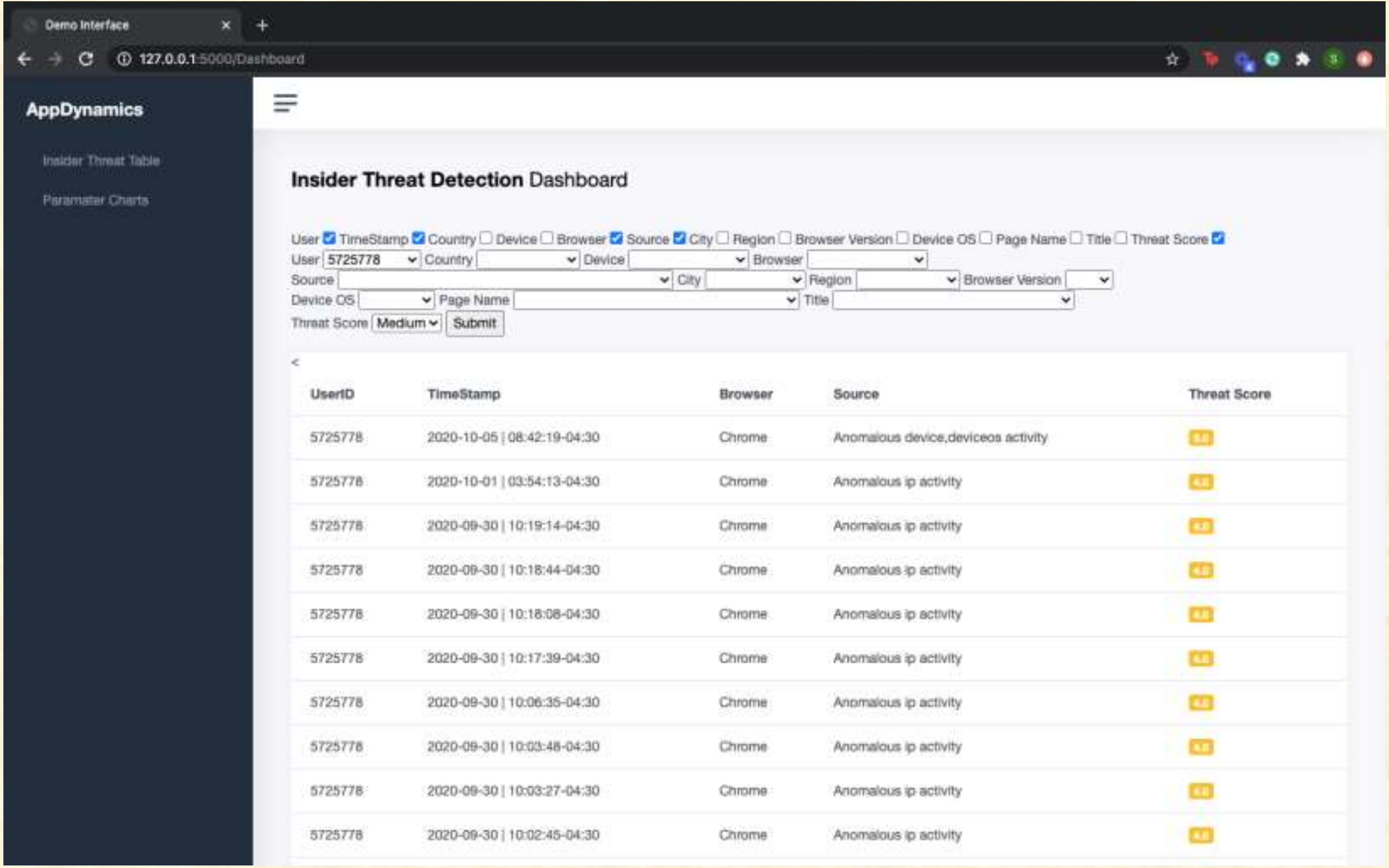
Insider Threat Detection Dashboard

User ☑ TimeStamp ☑ Country ☑ Device ☑ Browser ☑ Source ☑ City ☑ Region ☑ Browser Version ☑ Device OS ☑ Page Name ☑ Title ☑ Threat Score ☑

User Country Device Browser
Source City Region Browser Version
Device OS Page Name Title
Threat Score Submit

UserID	TimeStamp	Country	Device	Browser	Source	City	Region	Browser Version	Device OS	Page
5725778	2020-10-05 | 08:42:19-04:30	India	Mobile & Tablets	Chrome	Anomalous device activity	Bengaluru	Karnataka	85.0	Windows	/
5725778	2020-10-05 | 08:42:19-04:30	India	Mobile & Tablets	Chrome	Anomalous device,deviceos activity	Bengaluru	Karnataka	85.0	iOS	/
5725778	2020-10-01 | 03:54:13-04:30	India	Computer	Chrome	Anomalous ip activity	Lucknow	Uttar Pradesh	85.0	Windows	/
5725778	2020-09-30 | 10:19:14-04:30	India	Computer	Chrome	Anomalous ip activity	Lucknow	Uttar Pradesh	85.0	Windows	/
5725778	2020-09-30 | 10:18:44-04:30	India	Computer	Chrome	Anomalous ip activity	Lucknow	Uttar Pradesh	85.0	Windows	/

Filtering and Customization of the Table



Insider Threat Detection Dashboard

User ☑ TimeStamp ☑ Country □ Device □ Browser ☑ Source ☑ City □ Region □ Browser Version □ Device OS □ Page Name □ Title □ Threat Score ☑

User 5725778 Country Device Browser

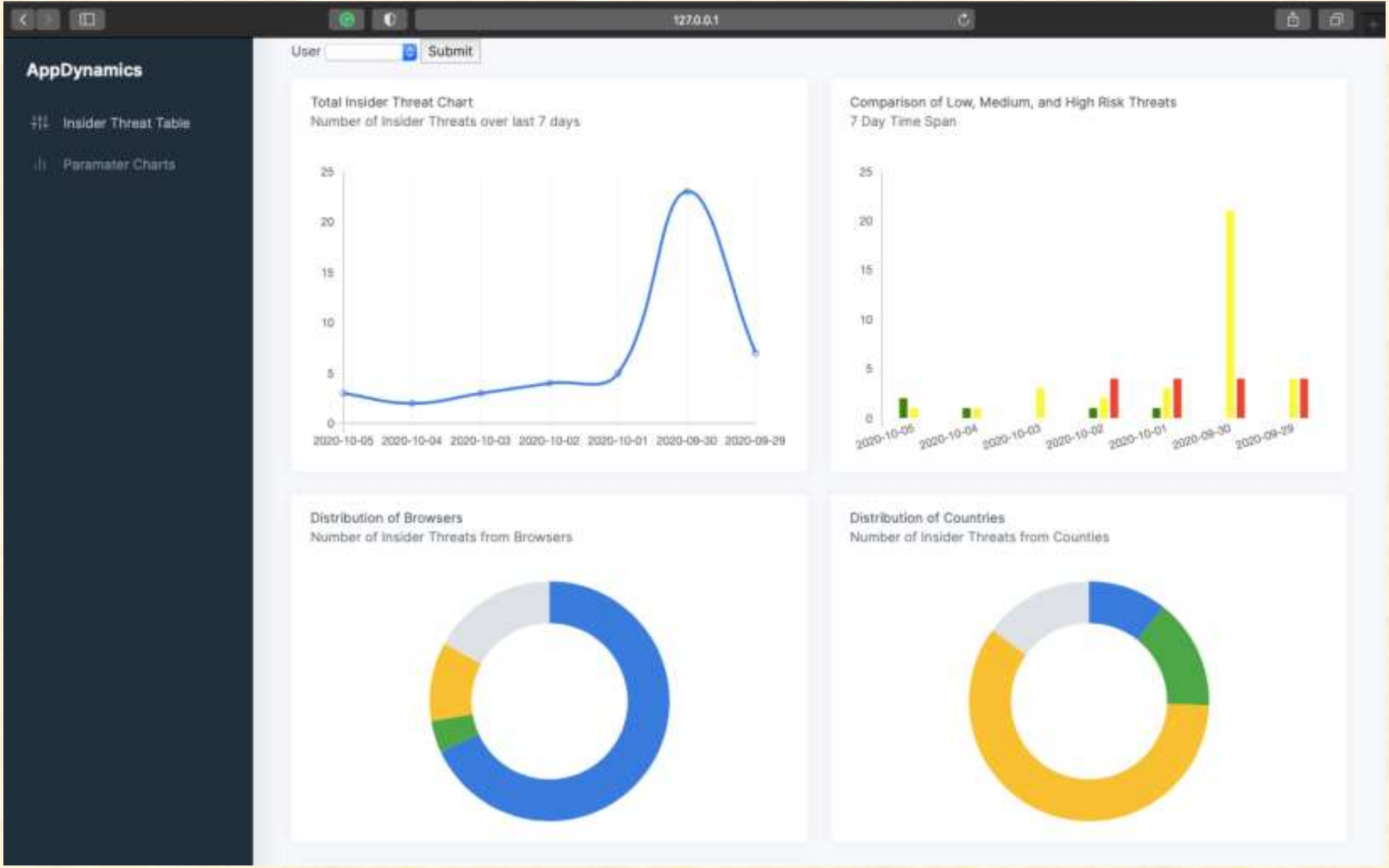
Source City Region Browser Version

Device OS Page Name Title

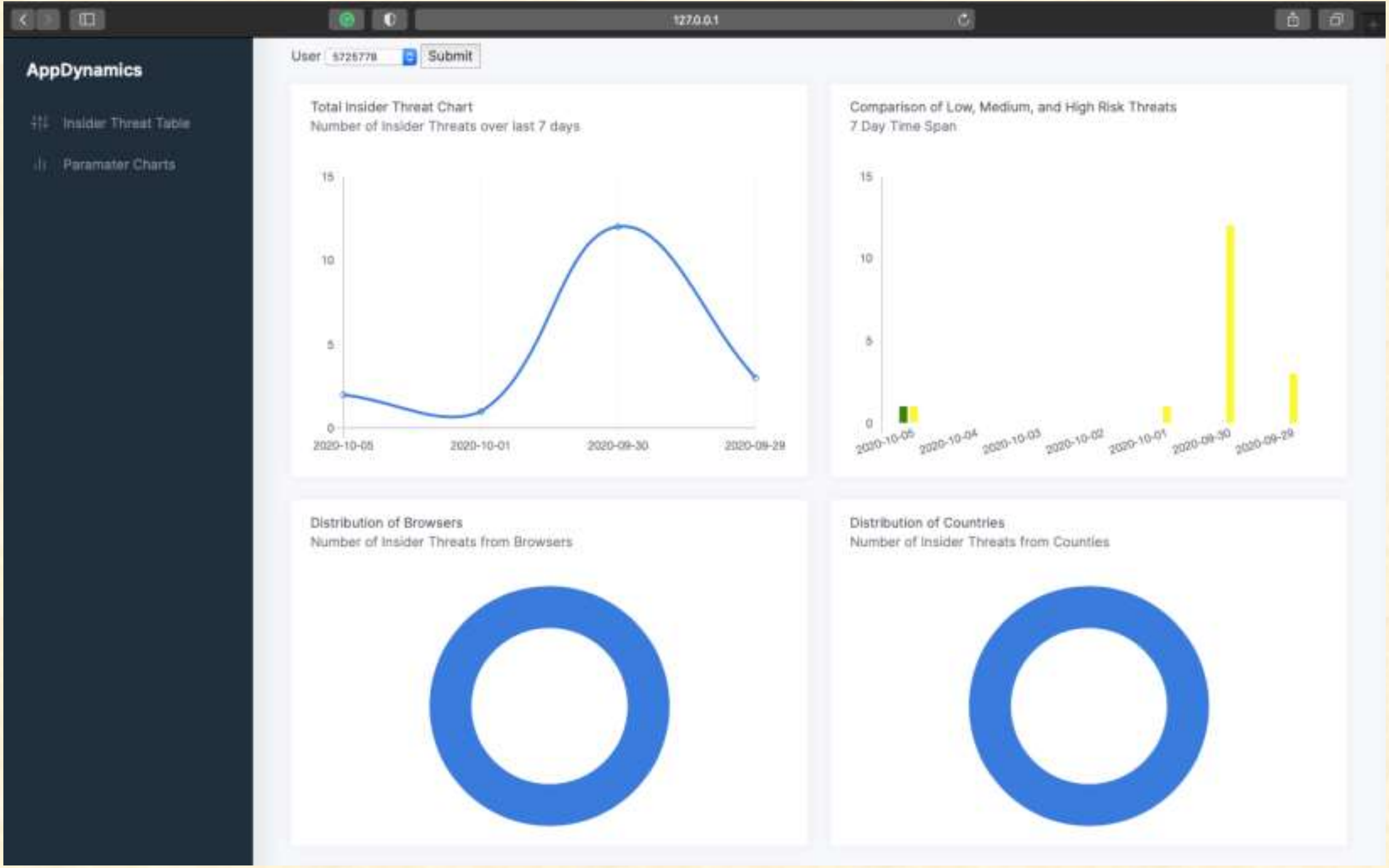
Threat Score Medium Submit

UserID	TimeStamp	Browser	Source	Threat Score
5725778	2020-10-05 | 08:42:19-04:30	Chrome	Anomalous device,deviceos activity	5.0
5725778	2020-10-01 | 03:54:13-04:30	Chrome	Anomalous ip activity	4.0
5725778	2020-09-30 | 10:19:14-04:30	Chrome	Anomalous ip activity	4.0
5725778	2020-09-30 | 10:18:44-04:30	Chrome	Anomalous ip activity	4.0
5725778	2020-09-30 | 10:18:08-04:30	Chrome	Anomalous ip activity	4.0
5725778	2020-09-30 | 10:17:39-04:30	Chrome	Anomalous ip activity	4.0
5725778	2020-09-30 | 10:06:35-04:30	Chrome	Anomalous ip activity	4.0
5725778	2020-09-30 | 10:03:48-04:30	Chrome	Anomalous ip activity	4.0
5725778	2020-09-30 | 10:03:27-04:30	Chrome	Anomalous ip activity	4.0
5725778	2020-09-30 | 10:02:45-04:30	Chrome	Anomalous ip activity	4.0

Graphs of the Activity



Filtering the Graphs based on User



AppDynamics

Insider Threat Table

Paramater Charts

User 5725778 Submit

Total Insider Threat Chart
Number of Insider Threats over last 7 days

Comparison of Low, Medium, and High Risk Threats
7 Day Time Span

Distribution of Browsers
Number of Insider Threats from Browsers

Distribution of Countries
Number of Insider Threats from Counties

What’s left to do?

- Save checkbox and filter states
- Optimize algorithm
- Customization of graphs

Questions?

? ? ? ?

? ?

? ? ?