MICHIGAN STATE UNIVERSITY

Project Plan

Insider Threat Detection

The Capstone Experience

Team AppDynamics

Andrew Jalbert
Andy Zhang
Ari Kohl
Chris Kulpa
Sumanth Rudraraju

Department of Computer Science and Engineering
Michigan State University

Fall 2020

From Students…
…to Professionals

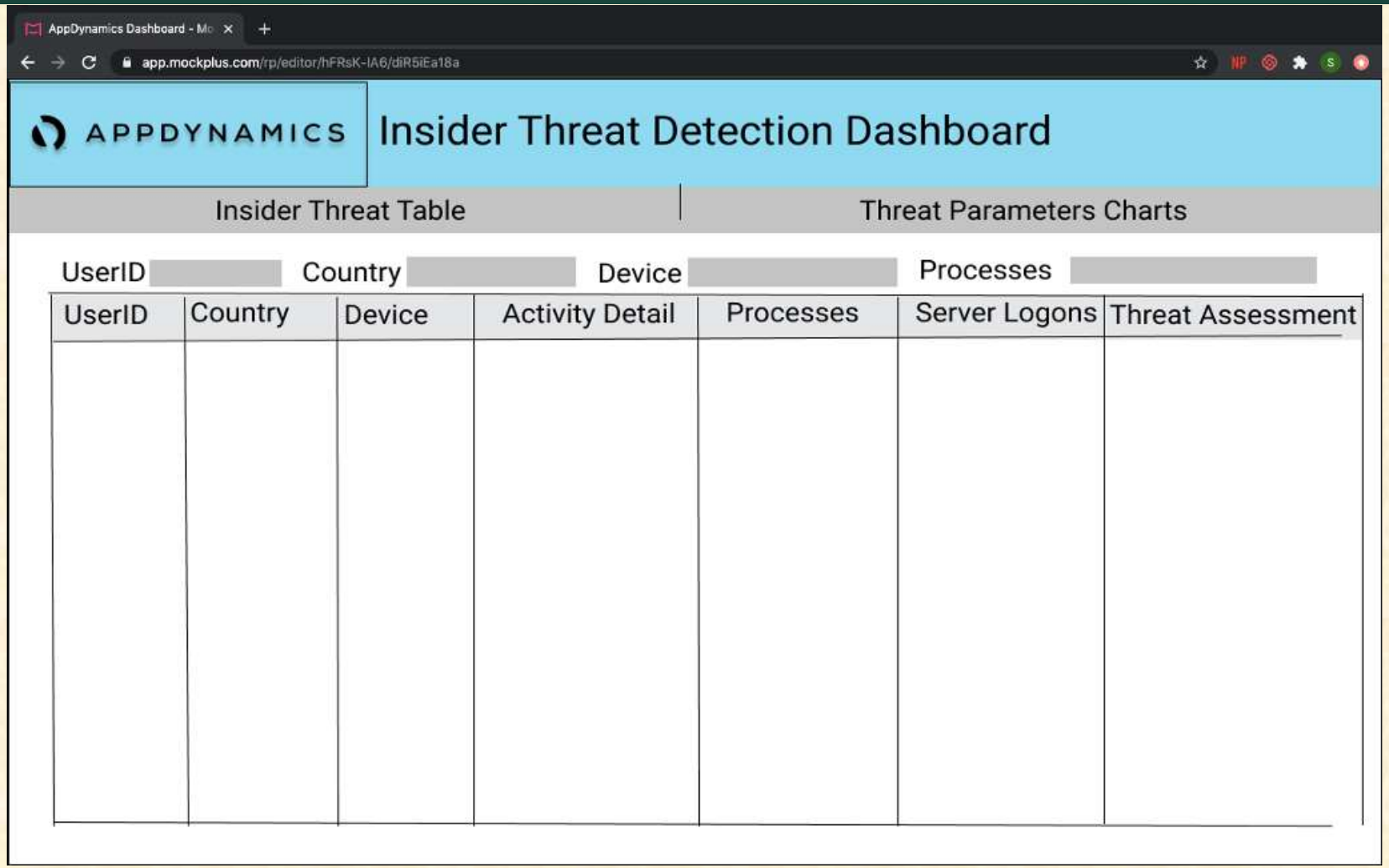
Functional Specifications

- Use analytic data gathered by the AppDynamics controller
- Feed the gathered data into a Threat Detection Algorithm
- Evaluates user's activity patterns to determine if they are performing anomalous activity and rank them accordingly
- Perform actions against users who commit anomalous activity

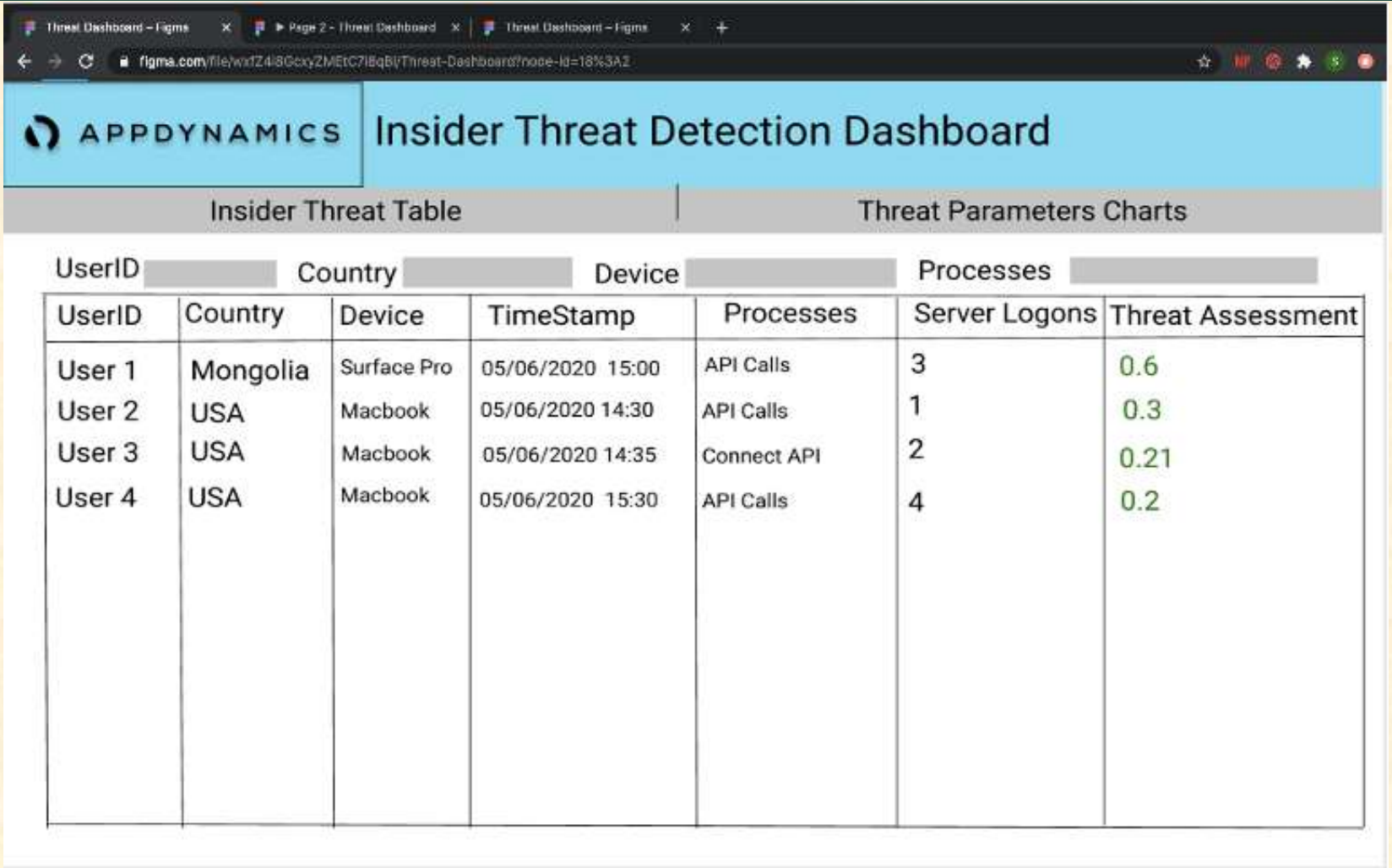
Design Specifications

- Display the results of the Threat Detection Algorithm
- List users who have committed anomalous behavior
- Rank the threat of the user compared to other user threats
- Show in real time new threats as one occurs

Screen Mockup: Insider Threat Table

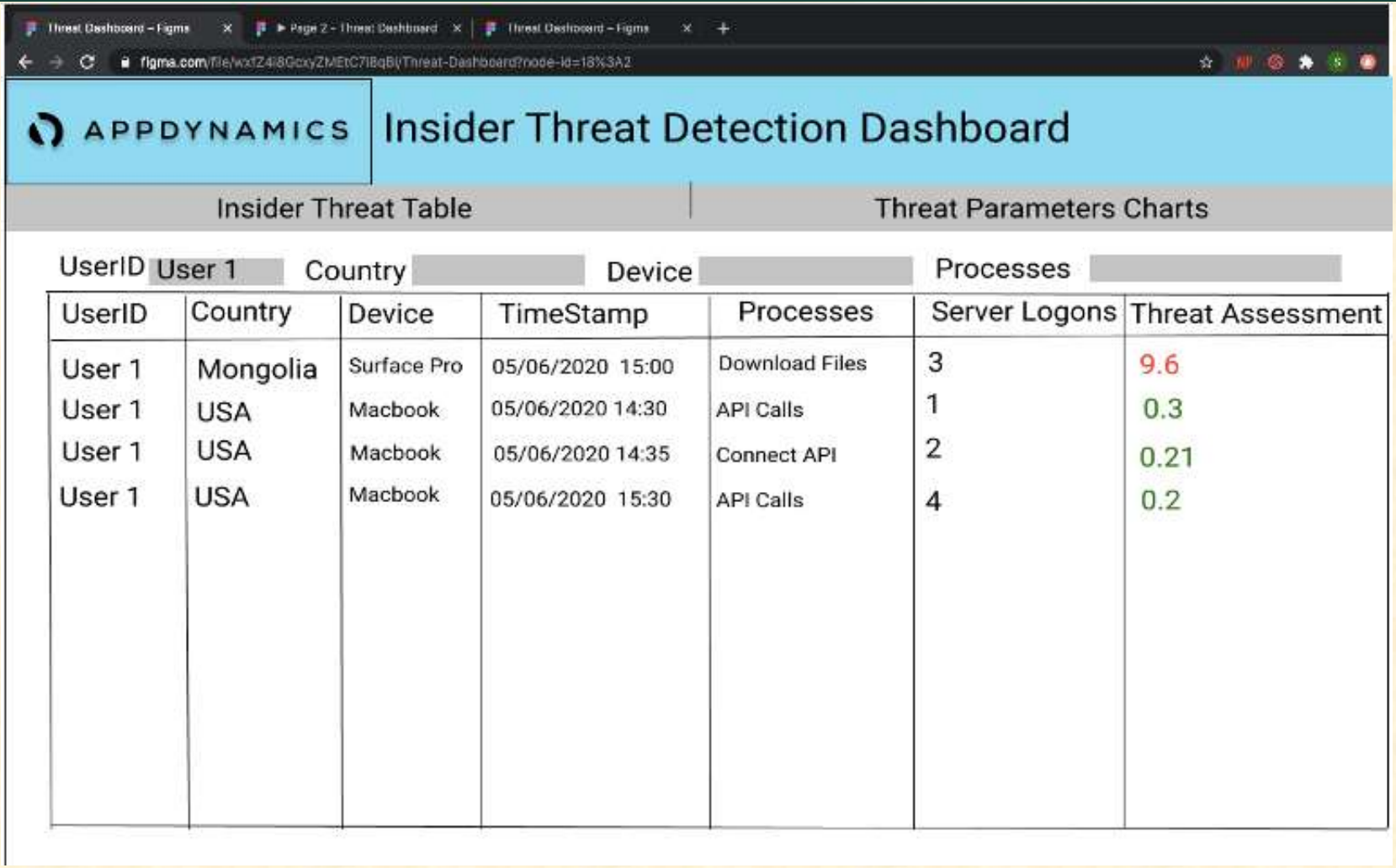


Screen Mockup: Insider Threat Table with Data



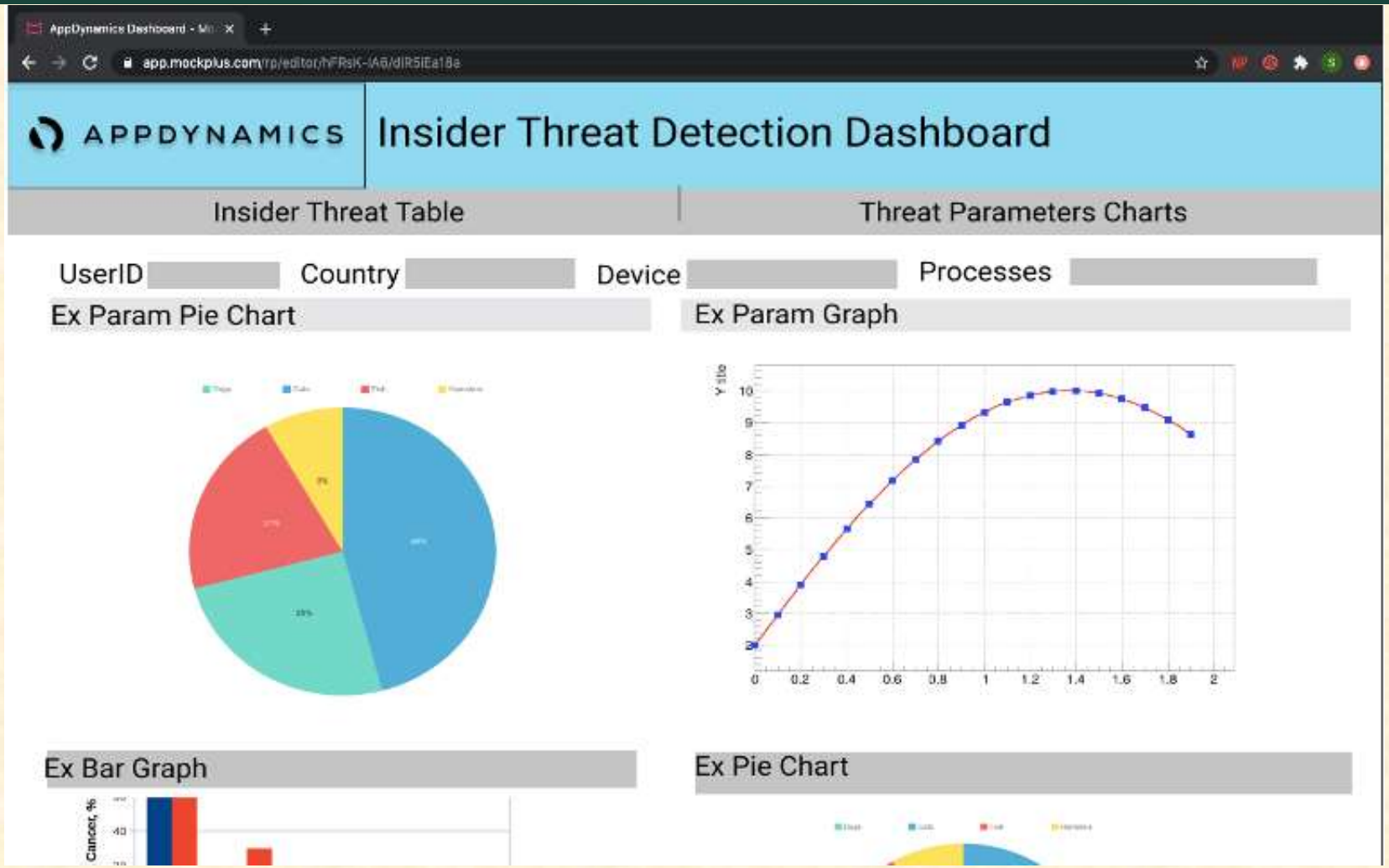
UserID	Country	Device	TimeStamp	Processes	Server Logons	Threat Assessment
User 1	Mongolia	Surface Pro	05/06/2020 15:00	API Calls	3	0.6
User 2	USA	Macbook	05/06/2020 14:30	API Calls	1	0.3
User 3	USA	Macbook	05/06/2020 14:35	Connect API	2	0.21
User 4	USA	Macbook	05/06/2020 15:30	API Calls	4	0.2

Screen Mockup: Insider Threat Table with Filters



UserID	Country	Device	TimeStamp	Processes	Server Logons	Threat Assessment
User 1	Mongolia	Surface Pro	05/06/2020 15:00	Download Files	3	9.6
User 1	USA	Macbook	05/06/2020 14:30	API Calls	1	0.3
User 1	USA	Macbook	05/06/2020 14:35	Connect API	2	0.21
User 1	USA	Macbook	05/06/2020 15:30	API Calls	4	0.2

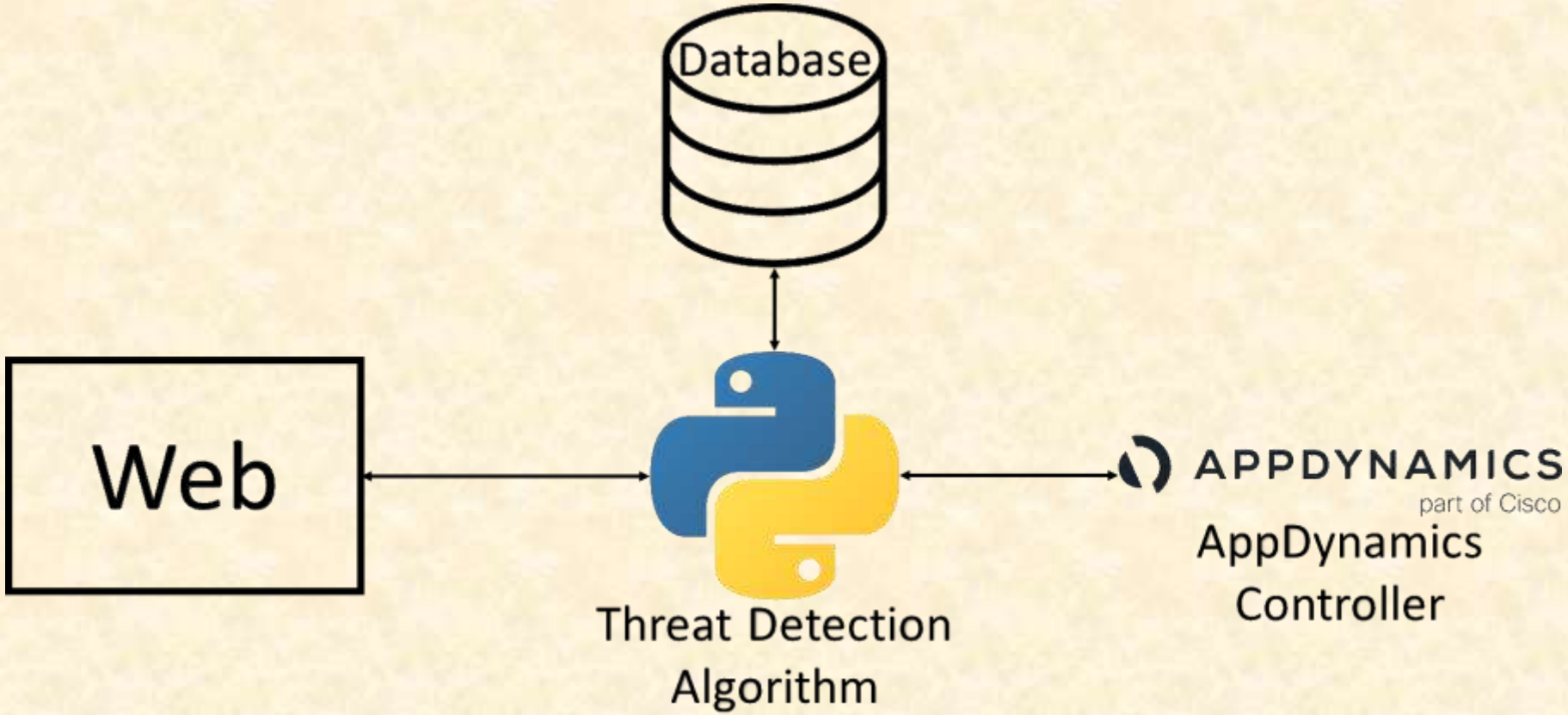
Screen Mockup: Threat Parameter Charts



Technical Specifications

- AppDynamics Controller
- MySQL Database
- Web Server for Application
- Threat Detection Algorithm

System Architecture



System Components

- Hardware Platforms
  - None
- Software Platforms / Technologies
  - AppDynamics Controller
  - Python
  - Postman API
  - MySQL Database
  - Web Server

Risks

- Generation of the Test Data
  - The controller has generated data; however it might not be a good representation of users with possible insider threats.
  - We have asked AppDynamics for more data and they are working on supplying it to us.
- Potentially Computationally Intensive Algorithm
  - Machine Learning and Data Science algorithms often have a very high run time and space complexity.
  - We will create a light algorithm to start with and grow it over time to be as efficient as possible while adding complexity
- False Positives
  - Accuracy is a very important part machine learning and threat detection algorithms which often have high rates of false positives.
  - Create a scoring system that shows severity of threat when displayed

Questions?