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
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

Back End

- Data Sources
  - AppDynamics Controller
  - CSV
  - Test Data
- Threat Detection Algorithm
- Database

Front End

- Web App
  - HTML
  - CSS
- User
# Table of Reported Activity

![Dashboard Image]

## Insider Threat Detection Dashboard

<table>
<thead>
<tr>
<th>UserID</th>
<th>TimeStamp</th>
<th>Country</th>
<th>Device</th>
<th>Browser</th>
<th>Source</th>
<th>City</th>
<th>Region</th>
<th>Browser Version</th>
<th>Device OS</th>
<th>Page Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>5725778</td>
<td>2020-10-05 08:42:19-04:30</td>
<td>India</td>
<td>Mobile &amp; Tablets</td>
<td>Chrome</td>
<td>Anomalous device activity</td>
<td>Bengaluru</td>
<td>Karnataka</td>
<td>85.0</td>
<td>Windows</td>
<td>/</td>
</tr>
<tr>
<td>5725778</td>
<td>2020-10-05 08:42:19-04:30</td>
<td>India</td>
<td>Mobile &amp; Tablets</td>
<td>Chrome</td>
<td>Anomalous device, deviceos activity</td>
<td>Bengaluru</td>
<td>Karnataka</td>
<td>85.0</td>
<td>IOS</td>
<td>/</td>
</tr>
<tr>
<td>5725778</td>
<td>2020-10-01 03:54:13-04:30</td>
<td>India</td>
<td>Computer</td>
<td>Chrome</td>
<td>Anomalous ip activity</td>
<td>Lucknow</td>
<td>Uttar Pradesh</td>
<td>85.0</td>
<td>Windows</td>
<td>/</td>
</tr>
<tr>
<td>5725778</td>
<td>2020-09-30 10:19:14-04:30</td>
<td>India</td>
<td>Computer</td>
<td>Chrome</td>
<td>Anomalous ip activity</td>
<td>Lucknow</td>
<td>Uttar Pradesh</td>
<td>85.0</td>
<td>Windows</td>
<td>/</td>
</tr>
<tr>
<td>5725778</td>
<td>2020-09-30 10:18:44-04:30</td>
<td>India</td>
<td>Computer</td>
<td>Chrome</td>
<td>Anomalous ip activity</td>
<td>Lucknow</td>
<td>Uttar Pradesh</td>
<td>85.0</td>
<td>Windows</td>
<td>/</td>
</tr>
</tbody>
</table>
Filtering and Customization of the Table
Graphs of the Activity

- 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 Countries
Filtering the Graphs based on User
What’s left to do?

• Save checkbox and filter states
• Optimize algorithm
• Customization of graphs
Questions?