Alpha Presentation
Insider Threat Detection

The Capstone Experience
Team AppDynamics

Ari Kohl
Chris Kulpa
Sumanth Rudraraju
Andy Zhang

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.
• 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

SQLite Database

Front End

Web App
- HTML
- CSS

User

The Capstone Experience
Team AppDynamics Alpha Presentation
Display of Anomalous Users
Filtering based on User ID
Filtering based on Threat Score

![Dashboard](image-url)

<table>
<thead>
<tr>
<th>UserID</th>
<th>TimeStamp</th>
<th>Country</th>
<th>Device</th>
<th>Browser</th>
<th>Source</th>
<th>Threat Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>5756758</td>
<td>2020-09-29T18:01:37-04:30</td>
<td>Belgium</td>
<td>Mobile &amp; Tablets</td>
<td>Safari</td>
<td>Abnormal Countries</td>
<td>8.01</td>
</tr>
<tr>
<td>5756758</td>
<td>2020-09-29T18:01:37-04:30</td>
<td>Belgium</td>
<td>Mobile &amp; Tablets</td>
<td>Safari</td>
<td>Abnormal Countries</td>
<td>8.01</td>
</tr>
<tr>
<td>5756758</td>
<td>2020-09-29T18:01:37-04:30</td>
<td>Belgium</td>
<td>Mobile &amp; Tablets</td>
<td>Safari</td>
<td>Abnormal Countries</td>
<td>8.01</td>
</tr>
<tr>
<td>1234567</td>
<td>2020-09-29T21:57:12-04:30</td>
<td>India</td>
<td>Mobile &amp; Tablets</td>
<td>Safari</td>
<td>Abnormal Countries</td>
<td>8.01</td>
</tr>
<tr>
<td>1234567</td>
<td>2020-09-29T21:57:12-04:30</td>
<td>India</td>
<td>Mobile &amp; Tablets</td>
<td>Safari</td>
<td>Abnormal Countries</td>
<td>8.01</td>
</tr>
</tbody>
</table>
Filtering based on User ID and Source of Anomaly
What’s left to do?

• Display the results in graphs and charts
• Sorting based on a certain field
• Further develop algorithm and threat score
  ▪ Incorporate more fields of data
  ▪ Track the fingerprint of activity
• Act against anomalous users
Questions?