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
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

<table>
<thead>
<tr>
<th>User ID</th>
<th>Country</th>
<th>Device</th>
<th>Activity Detail</th>
<th>Processes</th>
<th>Server Logons</th>
<th>Threat Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Screen Mockup: Insider Threat Table with Data

<table>
<thead>
<tr>
<th>UserID</th>
<th>Country</th>
<th>Device</th>
<th>TimeStamp</th>
<th>Processes</th>
<th>Server Logons</th>
<th>Threat Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>User 1</td>
<td>Mongolia</td>
<td>Surface Pro</td>
<td>05/06/2020 15:00</td>
<td>API Calls</td>
<td>3</td>
<td>0.6</td>
</tr>
<tr>
<td>User 2</td>
<td>USA</td>
<td>Macbook</td>
<td>05/06/2020 14:30</td>
<td>API Calls</td>
<td>1</td>
<td>0.3</td>
</tr>
<tr>
<td>User 3</td>
<td>USA</td>
<td>Macbook</td>
<td>05/06/2020 14:35</td>
<td>Connect API</td>
<td>2</td>
<td>0.21</td>
</tr>
<tr>
<td>User 4</td>
<td>USA</td>
<td>Macbook</td>
<td>05/06/2020 15:30</td>
<td>API Calls</td>
<td>4</td>
<td>0.2</td>
</tr>
</tbody>
</table>
Screen Mockup: Insider Threat Table with Filters

<table>
<thead>
<tr>
<th>UserID</th>
<th>Country</th>
<th>Device</th>
<th>TimeStamp</th>
<th>Processes</th>
<th>Server Logons</th>
<th>Threat Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>User 1</td>
<td>Mongolia</td>
<td>Surface Pro</td>
<td>05/06/2020 15:00</td>
<td>Download Files</td>
<td>3</td>
<td>9.6</td>
</tr>
<tr>
<td>User 1</td>
<td>USA</td>
<td>Macbook</td>
<td>05/06/2020 14:30</td>
<td>API Calls</td>
<td>1</td>
<td>0.3</td>
</tr>
<tr>
<td>User 1</td>
<td>USA</td>
<td>Macbook</td>
<td>05/06/2020 14:35</td>
<td>Connect API</td>
<td>2</td>
<td>0.21</td>
</tr>
<tr>
<td>User 1</td>
<td>USA</td>
<td>Macbook</td>
<td>05/06/2020 15:30</td>
<td>API Calls</td>
<td>4</td>
<td>0.2</td>
</tr>
</tbody>
</table>
Screen Mockup: Threat Parameter Charts
Technical Specifications

• AppDynamics Controller
• MySQL Database
• Web Server for Application
• Threat Detection Algorithm
System Architecture

Web

Database

Threat Detection Algorithm

AppDynamics Controller
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?