Beta Presentation
Detecting Security Threats from User Patterns
The Capstone Experience

Team Symantec

Stephen Alfa
Keerthana Kolisetty
Robert Novak
Abby Urbanski
Xiaoyu Wu

Department of Computer Science and Engineering
Michigan State University
Spring 2018
Project Overview

• The goal of the project is to provide VIP customers a Splunk add-on and an ELK application on an AWS AMI to visualize various operational and security trend information present in log data and analyze it in near real-time.

• Both applications should alert users when suspicious or malicious activity is detected.
System Architecture
Splunk: Operation Trends Dashboard

Operational: Trends

Total Authentications Per Day

Time Range

- All time

Total Authentications Per Minute

Time Range

- Previous week

Graphs showing trends in total authentications per day and per minute.
# Splunk: Risk Analysis Dashboard

## Security Trends: Risk Analysis

**Total Number of Risky Users**

**Time Range**
- All time

**Risky Authentication Reasons**

**Time Range**
- All time

### Top Risky Users

<table>
<thead>
<tr>
<th>User ID</th>
<th>Sparkline</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>6SY22W</td>
<td><img src="sparkline_image" alt="" /></td>
<td>297</td>
</tr>
<tr>
<td>OHAN0E</td>
<td><img src="sparkline_image" alt="" /></td>
<td>295</td>
</tr>
<tr>
<td>3K100R</td>
<td><img src="sparkline_image" alt="" /></td>
<td>253</td>
</tr>
<tr>
<td>LUKUMI</td>
<td><img src="sparkline_image" alt="" /></td>
<td>284</td>
</tr>
<tr>
<td>JQ0K0T</td>
<td><img src="sparkline_image" alt="" /></td>
<td>269</td>
</tr>
<tr>
<td>TKMP9T</td>
<td><img src="sparkline_image" alt="" /></td>
<td>238</td>
</tr>
<tr>
<td>RSM00F</td>
<td><img src="sparkline_image" alt="" /></td>
<td>262</td>
</tr>
<tr>
<td>PWG30P</td>
<td><img src="sparkline_image" alt="" /></td>
<td>247</td>
</tr>
<tr>
<td>TRHY813</td>
<td><img src="sparkline_image" alt="" /></td>
<td>244</td>
</tr>
<tr>
<td>U39B3L</td>
<td><img src="sparkline_image" alt="" /></td>
<td>244</td>
</tr>
</tbody>
</table>

**Risky Users This Week vs. Last Week**

- **This Week**: 61,311
- **Last Week**: [Count]
Splunk: Geolocation Dashboard
ELK: Operational Overview Dashboard

Number of Authentications: 16,572
Number of Users: 2,166

Successful vs. Failed Authentications:
- Success
- User does not have a...
- Operation not allowed...
ELK: Operational User Analysis Dashboard

Users Created Over Time

Unique Users Authenticated

2,166 Users

Number of Users Created

128 Users Created

Top Authenticating Users

<table>
<thead>
<tr>
<th>Users</th>
<th>Number of Authentications</th>
</tr>
</thead>
<tbody>
<tr>
<td>spiker</td>
<td>350</td>
</tr>
<tr>
<td>GLDC5I</td>
<td>15</td>
</tr>
<tr>
<td>OUBO68</td>
<td>15</td>
</tr>
<tr>
<td>6H9QRI</td>
<td>14</td>
</tr>
<tr>
<td>7S1LYA</td>
<td>14</td>
</tr>
<tr>
<td>FBU6GF</td>
<td>14</td>
</tr>
<tr>
<td>4O7PLU</td>
<td>13</td>
</tr>
<tr>
<td>1BT7XF</td>
<td>12</td>
</tr>
<tr>
<td>AD2ACH</td>
<td>12</td>
</tr>
<tr>
<td>07APPR</td>
<td>11</td>
</tr>
</tbody>
</table>
ELK: Geolocation Dashboard
What’s left to do?

• Adding any additional pre-built panels
• Clean up Splunk UI
• Packaging the applications
Questions?