Nimble Cybersecurity Incident Management through Visualization and Defensible Recommendations
Nimble Cybersecurity Incident Management through Visualization and Defensible Recommendations
Our Goal

Help online analysts in Security Operations Centers complete their tasks more quickly and accurately
Our Approach

- An interactive graph-based visualization of correlated IDS output
- Defensible recommendations based on machine learning from historical analyst behavior
- Prototype tested with professional analysts in a controlled study
Related Work: IDS Alert Visualization

SnortView

Hideki Koike and Kazuhiro Ohno, VizSec 2004
IDS RainStorm

Uses parallel axis to fit the large range of IP addresses

Kulsoom Abdullah et al., VizSec 2005
VisAlert

Yarden Livnat et al., 2005
Data Collection and Preparation

- 3 Monitored Organizations
- 8 Days
- 7 Sensors
- 2,869,108 IDS Events
- 164 Alerts
- 29 Analysts
- 106 Machines with Asset Information

No Identifying Information
- No plain text fields collected
- IP addresses anonymized using Crypto-PAn
- All unique identifiers replaced
In each partition, each source must be connected with each destination by each signature at least once.
Interactive Incident Diagram (IID)

- Each partition is rendered as a single arc, labeled with event signatures and counts.
- Sources and destinations are rendered as nodes.
- Multiple sources or destinations in a partition are rendered as a table.
- Visualization graphs can be manipulated, rearranged, zoomed, and explored.
Research Questions

- Is diagnosis better with this interactive visualization than a tabular display?

- Will analysts benefit from the display of classification recommendations?

- Will the benefits depend on whether the recommendations are accompanied by justifications?
The Study

- **Participants**
  - 18 professional security analysts
  - Minimum of three years experience, most had over five

- **Each participant completes 24 trials. For each trial:**
  - Analyst presented information about an alert
  - Asked to classify it with regards to issue type and priority
  - Two minute time limit with audible warnings
  - Once they have classified it indicate their confidence in their judgment
  - “Talk-Aloud” protocol

- **After trials, participants completed a survey**

- Discussion with all participants in a group debrief session
The Study

- Four experimental conditions
  - Presentation of Events: Visual or Tabular
  - Recommendation: No Suggestions, 3 Suggestions, or 3 Suggestions with Justifications
  - Correct Suggestion Available: Yes or No
  - Block of Trials: First or Second

- Measurements
  - **Accuracy** of response
  - **Time** to complete problem
  - **Confidence** in response
  - **Ratings** from survey
Visual Display
Tabular Display with Suggestion

<table>
<thead>
<tr>
<th>#</th>
<th>Event Name</th>
<th>Src IP</th>
<th>Dst IP</th>
<th>Src Port</th>
<th>Dst Port</th>
<th>Src Asset Info</th>
<th>Dst Asset Info</th>
<th>Suggested Explanations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>JavaScriptOOD_Good</td>
<td>54.203.206.74</td>
<td>100.172.37.41</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Issue Type:</td>
</tr>
<tr>
<td>2</td>
<td>JavaScriptOOD_Good</td>
<td>54.203.206.74</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Priority:</td>
</tr>
<tr>
<td>3</td>
<td>JavaScriptOOD_Good</td>
<td>54.203.206.74</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Issue Type:</td>
</tr>
<tr>
<td>4</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Priority:</td>
</tr>
<tr>
<td>5</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Issue Type:</td>
</tr>
<tr>
<td>6</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Priority:</td>
</tr>
<tr>
<td>7</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Issue Type:</td>
</tr>
<tr>
<td>8</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Priority:</td>
</tr>
<tr>
<td>9</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Issue Type:</td>
</tr>
<tr>
<td>10</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Priority:</td>
</tr>
<tr>
<td>11</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Issue Type:</td>
</tr>
<tr>
<td>12</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Priority:</td>
</tr>
<tr>
<td>13</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Issue Type:</td>
</tr>
<tr>
<td>14</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Priority:</td>
</tr>
<tr>
<td>15</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Issue Type:</td>
</tr>
<tr>
<td>16</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Priority:</td>
</tr>
<tr>
<td>17</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Issue Type:</td>
</tr>
<tr>
<td>18</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Priority:</td>
</tr>
<tr>
<td>19</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Issue Type:</td>
</tr>
<tr>
<td>20</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Priority:</td>
</tr>
<tr>
<td>21</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Issue Type:</td>
</tr>
<tr>
<td>22</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Priority:</td>
</tr>
<tr>
<td>23</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Issue Type:</td>
</tr>
<tr>
<td>24</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Priority:</td>
</tr>
<tr>
<td>25</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Issue Type:</td>
</tr>
<tr>
<td>26</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Priority:</td>
</tr>
<tr>
<td>27</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Issue Type:</td>
</tr>
<tr>
<td>28</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Priority:</td>
</tr>
<tr>
<td>29</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Issue Type:</td>
</tr>
<tr>
<td>30</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Priority:</td>
</tr>
<tr>
<td>31</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Issue Type:</td>
</tr>
<tr>
<td>32</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Priority:</td>
</tr>
<tr>
<td>33</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Issue Type:</td>
</tr>
<tr>
<td>34</td>
<td>HTTP-Unav_Rew Neal_Accessed</td>
<td>73.210.147.182</td>
<td>100.172.200.39</td>
<td>80</td>
<td>62664</td>
<td>151485</td>
<td>804984</td>
<td>Priority:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Time Remaining: 61:56</th>
<th>Issue Type:</th>
<th>Priority:</th>
<th>Issue Type:</th>
<th>Priority:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Visual Display with Justification
First set took longer overall than second set (p < 0.01)
Justifications and suggestions took longer than baseline (p < 0.01)
Visual displays took slightly longer than the tabular displays (p = 0.12)
Accuracy Across Display and Recommendation Conditions

- Slightly higher accuracy associated with visual (31%) than tabular (26%) across all recommendation conditions ($p < 0.10$)
- Effect stronger in second half, accuracy with visual was 35%, tabular was 20% ($p < 0.05$)
- Across both display types, there was no overall difference between the three level of recommendation ($p > 0.10$)
Research Questions Revisited

- Is diagnosis better with this interactive visualization than a tabular display?
  - Analysts were more accurate with the visualization, slightly slower
  - Two “camps”, strong proponents for both kinds of display

- Will analysts benefit from the display of classification recommendations?
  - Analysts were slower when recommendations shown, no impact on accuracy
  - The prevalence of incorrect recommendations may have reduced utility

- Will the benefits depend on whether the recommendations are accompanied by justifications?
  - Individual ratings for justifications significantly higher than for suggestions
  - Preference for justifications increased with tenure
Thank You!

Jamie Rasmussen
Software Engineer
jrasmus@us.ibm.com

Dan Gruen
Research Scientist
Daniel_Gruen@us.ibm.com

Steven Ross
Technical Lead
Steven_Ross@us.ibm.com

Kate Ehrlich
Research Scientist
katee@us.ibm.com

Susanna Kirk
Student Intern
sekirk@us.ibm.com

Kate Ehrlich
Research Scientist
katee@us.ibm.com

John Patterson
Manager & Distinguished Engineer
John_Patterson@us.ibm.com