Designing a Vulnerability Management Dashboard to Enhance Security Analysts’ Decision Making Processes
Dalya Manatova, Inna Kouper, Sagar Samtani, Indiana University

Motivation
- The main source of information for analysts and security operations centers (SOCs) is detailed network vulnerability scan reports.
- Such reports often contain large amounts of difficult to read or comprehend information and may not immediately provide the whole picture of organization’s exposure.

Solution
- **Aggregated** information from vulnerability scans;
- **Review trends** and perform comparisons over time;
- Drill down to details of a specific vulnerability;
- **Focus on high-risk** ones;
- **Prioritize** vulnerabilities based on their age, persistence, and impact on the system.

Steps of the vulnerability assessment procedure (workflow)
Through the exploratory interviews with three analysts and our literature review, we identified common security analysts’ tasks and gaps in tool support.

We propose a vulnerability assessment dashboard that provides security analysts with the ability to:
- **Aggregate** information from vulnerability scans;
- Review trends and perform comparisons over time;
- Drill down to details of a specific vulnerability;
- **Focus** on high-risk ones;
- **Prioritize** vulnerabilities based on their age, persistence, and impact on the system.

Results

Detailed monthly information for Organization 1

<table>
<thead>
<tr>
<th>Vulnerabilities by organization and age</th>
<th>1 month</th>
<th>3 months</th>
<th>6 months</th>
<th>9 months</th>
<th>12 months</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>10</td>
<td>20</td>
<td>30</td>
<td>40</td>
<td>50</td>
</tr>
<tr>
<td>Medium</td>
<td>15</td>
<td>30</td>
<td>45</td>
<td>60</td>
<td>75</td>
</tr>
<tr>
<td>Low</td>
<td>20</td>
<td>40</td>
<td>60</td>
<td>80</td>
<td>100</td>
</tr>
</tbody>
</table>

New vulnerabilities by severity and affected network size

<table>
<thead>
<tr>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>15</td>
<td>58</td>
</tr>
</tbody>
</table>

The varying saturation of red is used across all visuals in the dashboard to distinguish between severity scores (the more red - the higher the severity).

Design Approach

- **Literature analysis**
- **Data reporting and analysis requirements from the literature**
- **Exploratory UI Mockups**
- **Heuristic evaluation**
- **Semi-structured interviews (contextual inquiry)**
- **Dashboard recommendations**
- **Gaps in data analysis and reporting**
- **Exploratory interviews about analyst workflows**
- **User insight on data reporting and analysis needs**

Future Work

- **Feedback collection and assessment of the dashboard usefulness**;
- **Conducting contextual inquiry interviews with increased sample size of operational security specialists**;
- **Heuristic evaluation of user-friendliness and design-efficacy**;
- **Introduction of new ideas and improvement emerged after the feedback and evaluation assessment**;
- **Introduction of streamed data to the dashboard**.

Acknowledgments: Data collection for this project was conducted with support from the ResearchSOC, a collaborative cybersecurity response center managed by Indiana University, Duke University, and Carnegie Mellon University. This work was supported in part by NSF grants 1840034, 1850362, and 1917117.