Development and evaluation of information elements for simplified cyber-incident reports

Patrik Lif, Teodor Sommestad & Dennis Granåsen
Information elements

• What information elements should be included in an incident report?
Background

- Litterature
- Frameworks
- SA elements
- Practical experiences

Info. elements
STIX - Structured Threat Information Expression

- Information sharing
- 178 properties + relations
- No description of own network
## Information elements for simplified incident report

<table>
<thead>
<tr>
<th>Background</th>
<th>Victim</th>
<th>Attacker</th>
<th>Incident description</th>
<th>Damage assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rapporteur</td>
<td>Node</td>
<td>Node</td>
<td>Suspected attack objective</td>
<td>Probability that the attacker succeeded</td>
</tr>
<tr>
<td>Observations/indications</td>
<td>User</td>
<td>User</td>
<td>Attack or vulnerability details</td>
<td>Asset criticality</td>
</tr>
<tr>
<td></td>
<td>Comment</td>
<td>Comment</td>
<td>Attack mechanisms</td>
<td>Attack impact</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Attack domains</td>
<td>Response urgency</td>
</tr>
</tbody>
</table>
iPilot – 4 day exercise

Participants (30)  Adversary (3)  Tech. support (5)
Staff (10)  Evaluation (7)  Visitors (65)

Attacks & tools
- μTorrent downloads malware.
- DDos attack.
- Similar Ukraine scada-attack.
- Unauthorized hardware.
- Analysis with Wireshark, ELK, Snort, and Windows Event Log to collect information in a central system.
CRATE & SVED

400 + 400 servers
iPilot - evaluation

Purpose

- Use of the 16 information elements?
- Correlation between use of information elements and quality of the incident reports?
- Subjective experiences?
- Any training effects?
Results – quantitative use of elements

- Background
- Victim
- Attacker
- Incident description
- Damage Assessment

![Graph showing number of used information elements (max=16) with p <0.001)](image)

(p <0.001)
Results – qualitative use of elements

Correlation

- Small, but statistically significant, correlation $r = 0.22$ and $p = 0.003$ between the number of elements used and the quality.
Subjective ratings

• Content rating of 4.3 (scale 1-7).

• Too much information despite the efforts to create a simple template with only 16 information elements.
Conclusions

Overall

Elements

Training

5 categories

Dynamics

Log analysts