UX Aspects of Threat Information Sharing

Tomas Sander
Hewlett Packard Laboratories

February 25th 2016
Starting point

Human interaction still critically important at many stages of Threat Intelligence lifecycle.
Threat Information Sharing Platform (TISP)

Private Community
- SIEM
- STIX
- Friend

Sector Community
- STIX
- SIEM
- Portal

Global Community
- Other Sources

TISP Security Research
Feed

You
YOUR SIEM
YOUR STIX

TISP Privacy Enhanced Forums
Threat DB
Threat DB
Threat DB
Key challenge for TISPs

Encouraging users to contribute content.

Guiding question:
How can we encourage users to contribute more than they currently do?
TISP and UX

- UX, the process of putting users and human behavior at the forefront of any design activities is vastly underutilized in enterprise software, including security platforms.

- HCI and UX techniques can provide insight into the issues with TISP for Analysts and validate potential solutions - directing development strategy.
Our contribution to-date

– Initiate the systematic study of (some) UX and HCI aspects of TISPs

Key Task
Understanding TISP users
Our approach: Personas

Fictionalized representation of a group of users.

Relatable character

Helps prioritize and guide features

--- (See e.g. [Pruitt, Adler 2007])

Reason: Guesswork doesn’t work

--- Egocentric Intuition Fallacy

Source: Fake Crow
SOC Analyst – Chris Meyer

BIOGRAPHIC INFORMATION
BC.1 Age: 26
BC.2 Education: BS in Anthropology
BC.3 Experience: Self-taught & some classes
BC.4 Housing: Renting with roommate in Mountain View, CA
BC.6 Hobbies: Photography
BC.7 Values: Personal growth, creativity
BC.8 Other: Grew up and went to school in Midwest.

GOALS
GC.1 Build a successful career in IT security.
GC.2 Would like to manage his own team eventually.
GC.3 Contribute something good to society by making cyber space safer.
GC.4 Opportunities to grow and advance personally and professionally.
GC.5 Be more creative and artistic in life and work

WORKFLOW
WC.1 Performs triage on alerts by Arcsight SIEM.
WC.2 Accesses research sites on the Internet, commercial portals and internal asset management tools to determine criticality of events.

FRUSTRATION & CHALLENGES
FC.1 Too much repetitive activity of manual indicator look ups wastes time.
FC.2 Time pressure
FC.3 Unvetted intel
FC.4 Out-of-date intel

PERSONAL TECHNOLOGY USE
PC.1 Uses Apple product suite as everything works well together.
PC.2 Loves social networks.
PC.3 Shares his photos via Instagram.
PC.4 Enjoys learning from youtube and other online sources.

Table 1: Chris Meyer | SOC Analyst
“Security tools are inconvenient to use compared to most consumer technology”
3 Groups, 5 Personas

Based on 9h of interviews and 20h of ethnographic observation of CSIRTs and SOCs
Findings: TISP contributions differ by role

<table>
<thead>
<tr>
<th>SOC Analysts</th>
<th>Incident Responders</th>
<th>CTI Analysts</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Feedback on specific indicators</td>
<td>– New IOCs, cases, malware samples</td>
<td>– Gatekeeper</td>
</tr>
<tr>
<td>– Annotations</td>
<td>– Tools and practices how they solved certain problems</td>
<td>– Enable automated sharing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Detailed feedback on received intel</td>
</tr>
</tbody>
</table>
Findings: Needs from TISPs differ by role

SOC Analysts
- At least minimal context for indicators
- Vetted intel, low false positive rates
- Data enrichment to reduce repetitive work
- Good integration with SIEM tools.

Incident Responders
- Detailed IOCs, TTPs,
- Detailed context and enrichment
- Tailored responses that support their workflow.

CTI Analyst
- One stop shop for TI
  - Includes external and internal TI
- Unified management of sharing relationships
- Strategic Threat Intelligence
- Non-attribution for (most) contributed data.
Key Task
Research Round 2 – Ideas Validation
Additional Research Goals

– Understand analyst behaviours, priorities and concerns w.r.t. sharing

– Determine appetite for user profiles and gamification/ badges in TISP as a way of incentivizing sharing.

– What helps to add to the trustworthiness for received information

– Determine reception for commenting or up-voting systems
General Findings

– Good news!
  – Threat information sharing as a concept is universally considered beneficial. Analysts generally would like to actively participate. The platform needs to support this and remove barriers.

– Processes do not support sharing as well as they could.

  – Unclear authority of what to share
    – Which data can be shared by CTI and which by analysts/IR?
    – Do TISPs need a staging area where CTI experts can approve contributions?

  – Sharing not part of standard SOC processes and procedures.
    – Adding sharing to processes will have significant impact.

– Opinion on gamification and badges was mixed.
  – About half respondents were positive to enthusiastic. The other had at least some reservations (more details later).
Design Idea: Full User Profile

Phil Baker
British Private Telecom

Communications Industry
Larger than 100,000

Certifications

Contact Me

Expertise

Awards

Hewlett Packard
Enterprise
Findings: Privacy

– Disclosing full profile *within* organization OK, not without.

– Concerns about social engineering, job poaching.

– Only anonymized profile should be visible outside the organization.

– Organization data should not be shared, but vital statistics about the organization a contributor works for can be important for trust-building.

– But ability to open profile to trusted collaborators is an additional trust building resource.
Sanitized User Profile
Additional Findings

– Skill based badges were most favored by analysts.
  – E.g. related to core cyber security curriculum.

– Should be tied to some real world positive outcomes.

– Measure quality rather then only quantity.
  – Leverage social features to help with quality, e.g. endorsements.

– Job title was considered to be less reliable information to judge trustworthiness of shared data.
  – However the role and team an analyst belongs to may be relevant. Badges such as ‘5 year malware analyst’ could be meaningful.
  – Badges users inherit from the company they work are useful for tagging, such as size, vertical etc.

– Also include badges that reflect being a good collaborator.

– All users were less favorable about extending badges to everyday SOC work.

– Ability to comment and up-voting (validating) posts also seen as beneficial to help assess quality.
Conclusions

– UX perspective yields novel insights to drive developments for effective sharing.

– Different TISP users differ significantly in a) data they can contribute and b) functionalities they need leading to complimentary feature sets.

– Integrating sharing into standard SOC/IR processes helpful to increase sharing.

– Profile/gamification approach appealing and promising, but the devil is in the details.
Next Steps

– Build and user-test new design ideas.

– Explore cross-organizational aspects for badges and profiles.

– Refine personas and validate findings across broader range of organizations and roles.

Contact: tomas.sander@hpe.com