Starting point

Dr. Anton Chuvakin
@anton_chuvakin

Why so many security vendors are such fans of 1980s-style UIs?

Human interaction is critically important at all stages of the threat intelligence lifecycle.
Threat Information Sharing Platform (TISP)

TISP - Privacy Enhanced Forums

Private Community
SIEM, STIX, Portal

Sector Community
STIX, SIEM, Portal

Global Community

YOU
YOUR SIEM
YOUR STIX

TISP Security Research
Feed
Other Sources
Overview
Encouraging users to contribute quality content

Who are TISP users?

What data can/do they contribute?

What motivates them to contribute?

What are the obstacles to sharing (and how do we remove them)?
TISP UX research

UX
Puts users and human behavior at the forefront of any design activities
Vastly underutilized in enterprise software, including security platforms

HCI and UX methods can
Provide insight into the issues with TISPs for Analysts
Validate potential solutions, directing development strategy

Our research
Initiate the systematic study of (some) UX and HCI aspects of TISPs
In Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security (WISCS '15)
Understanding TISP users
Our approach: Personas

Fictionalized representation of users
Create relatable characters
Help prioritize and guide features

Clark Andrews

Motivations
- Incentive
- Fear
- Achievement
- Growth
- Power
- Social

Goals
- To cut down on unhealthy eating and drinking habits
- To measure multiple aspects of life more scientifically
- To set goals and see and make positive impacts on his life

Frustrations
- Unfamiliar with wearable technology
- Saturated tracking market
- Manual tracking is too time consuming

Bio
Aaron is a systems software developer, a “data junkie” and for the past couple years, has been very interested in tracking aspects of his health and performance. Aaron wants to track his mood, happiness, sleep quality and how his eating and exercise habits affects his well being. Although he only drinks occasionally with friends on the weekend, he would like to cut down on alcohol intake.

Source: Fake Crow
Persona: Chris Meyer - SOC analyst

**BIOGRAPHICAL INFORMATION**

BC.1 Age: 26  
BC.2 Education: BS in Anthropology  
BC.3 Experience: Self-taught and some classes  
BC.4 Housing: Renting with roommate in Mountain View, CA  
BC.5 Relationship: Single. Dating  
BC.6 Hobbies: Photography  
BC.7 Values: Personal growth, creativity  
BC.8 Other: Grew up and went to school in the 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

**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

**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

Table 1: Chris Meyer | SOC Analyst

“Security tools are inconvenient to use compared to most consumer technology”
Persona groups

- CISO/Managers
- SOC Analysts
- CTI Analysts
- Incident Responders
- Power users
Power users

- Fuse intel from various sources
- Create or enrich cases
- Import third party reports
- Create detailed profiles
Data contribution by users
TISP user contributions

**SOC Analyst**
- Feedback on indicators he does triage on.
- Annotations

**Benefits:**
- Lower FP rate
- Enhanced context for basic indicators

**Incident Responders**
- New IOCs, cases, malware samples
- In depth analysis results from IR with deep knowledge in malware analysis, log analysis or forensics
- Tools and methods relevant to an investigation
- Contributions to cases from others

**Benefits:**
- Live IOCs
- Can add more context during attack investigation

**CTI Analyst**
- Gatekeeper for in and outgoing intel
- Enriches data with context
- Links between intel pieces
- Detailed feedback on intel and sources

**Benefits:**
- Evaluates quality and relevance of intel and how to improve it
- Has trusted personal relationships necessary for sensitive data sharing
TISP user contributions

Power Users

- Original threat research
- External research reports
- Detailed analysis results for customer cases and queries
- Research derived from a number of sources and tools

Benefits:
- Contribute large amounts of high quality content

CISO/Managers

- Decision makers when sharing highly sensitive data, e.g. APT related.
- Set overall sharing policy and culture for sharing in organization

Benefits:
- His/her buy-in critical for more than occasional analyst driven sharing to take place
TISP user needs

SOC Analyst
- Minimal indicator context
- Vetted intel, low false positive rates
- Automatic data enrichment to reduce repetitive work
- Good integration with SIEM tools

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

CTI Analyst
- One-stop TI management capability
- Unified relationship management
- Strategic threat intelligence
- Non-attribution for (most) data contributed to platform
- Development of mutually trusted peer-relationships to ensure access to important information
TISP user needs

Power Users
• API support for importing data streams into tools of their choice
• Ability to customize UI to support their particular workflows, e.g. showing far greater level of detail than to average analyst
• Automated, intelligent support for bulk upload of IOCs.

CISO/Managers
• Overview of top threats and (changing) threat landscape relevant to their organization
• Successful investigations and metrics showing ROI for intel investments
• Metrics and evidence showing ROI of outward sharing
• Assurance that outward sharing does not create risks for company
Motivation and gamification
General findings

Threat information sharing, as a concept, is universally considered beneficial. Analysts would like to actively participate so the platform needs to support this and remove barriers.

Opinion on gamification and badges was mixed. Half of younger and earlier career respondents were positive to enthusiastic. The rest of the younger respondents had at least some reservations, while older and more advanced respondents were less interested in badges overall.
Design Idea: Full User Profile

Phil Baker
British Private Telecom
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Dolore sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Certifications
- Secure Networking
- OSINT
- IOC Hunter
- YARA

Skills
- Communications Industry
- Larger than 100,000
- London (UK)
- Joined September 2015
- 20,56 Profile Views
- 500 Followers

Awards
- Forensics Mentor
- Money Saver
- Trusted Sharer

Contact me
- @phb
- phib@exploit.im
TISP common badge types

Skill based Badges
Recognize demonstrated skills

- Malware Analyst
- Secure Networking
- OSINT

Award Badges
Recognize community contributions

- Hacktivism
- Forensics Mentor

Certification Badges
Recognize completion of trainings & exams

- Master
- AICPA
- SOC

IOC Hunter
YARA

Trusted Sharer
Money Saver
Points, badges, leaderboards (PBL)

**Points**

<table>
<thead>
<tr>
<th>Level</th>
<th>Required Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beginner</td>
<td>50</td>
</tr>
<tr>
<td>Intermediate</td>
<td>100</td>
</tr>
<tr>
<td>Advanced</td>
<td>250</td>
</tr>
<tr>
<td>Master</td>
<td>800</td>
</tr>
<tr>
<td>UBER</td>
<td>1500</td>
</tr>
</tbody>
</table>

**Badges**

- Beginner
- Intermediate
- Advanced
- Master
- UBER

**Leaderboards**

- Recognize top contributors
- Personalized for peer comparison
Badges – Findings

– Skill based badges most favored by younger/early career analysts
– Mission badges also appealed to advanced professionals
– Badges should measure quality, not just quantity.
– Being a good collaborator should be rewarded; one-upmanship is a concern
– Analysts less favorable about extending badges to everyday SOC work
– Some users liked badges linked to real world rewards
– SOC teams can pool badges for use in self-marketing/recruitment
Mission Badges
Gamification beyond PBL
Can leverage social incentives: introducing users, who made good contributions or gained certain badges.

Early career and advanced users interested in TISP helping them achieve social goals.

Younger users
• like features such as commenting and up-voting of posts which makes for more lively interaction

Advanced users
• expanding their professional network
• building more mutually trusted peer-relationships
• it provides better access to information
Badges useful for evaluating credibility of contributions

Contributors can tag their anonymous messages to allow recipients to judge credibility without knowing the source.

Badges suitable for establishing credibility of information
- Most of the previous badges.
- Recognized team, role and length of service
- Company badges (size, vertical etc.)
Profile privacy

Disclosing full profile within organization OK, but not without

Contributor organization specifics should not be shared

Organization’s vital statistics are OK

Opening full profile to selected collaborators is a valuable trust-building tool
Sanitized User Profile
Removing obstacles
Sharing policies, processes and workflow
Key findings

Processes and policies do not support sharing as well as they could!

Senior-level interviewees perceived lack of adequate sharing policies as THE major obstacle for effective sharing

Perceived risks
- Inappropriate sharing may result in exposure for organization
- Less experienced analysts may not always fully understand what they are sharing
- Not everyone in IR/SOC has complete information about sensitive cases
Information sharing policies

Organizational sharing policies need to govern (partial list)

– Who can share?
– Provide practical criteria to distinguish between sharable and non-sharable information
– With whom data can be shared
– Under which conditions
– If/when approvals are required and by whom

Interviewees saw value for the community creating policy templates that organizations can adapt to their needs
**Approval workflows**

- Level 1 Analysts cannot share
- Level 2, IR, and CTI are automatically trusted to share
- Level 1 Analysts and IR submit request to share
- Senior Analysts, Power users and Managers approve
Conclusions

UX perspective provides novel insights

TISP users differ significantly

Profile/gamification approach shows promise

Integrating sharing into SOC/IR processes helpful to increase sharing
Next steps

- Refine personas
- Build and test new designs for specific personas (power users)
- Explore cross-organizational aspects of badges/profiles
- Share suitable sharing policy templates and guidance
Thank you
tomas.sander@hpe.com
bhein@hpe.com

ACKNOWLEDGEMENTS

Interviewees from various organizations who graciously donated their time and insights to support this research

UX researchers Joshua Hailpern, Martha Aldridge, Rotem Hagay, Carsten Schlipf who supported various phases of this project

The HPE Global Cyber Security Team for their generous support