

UX Aspects of Threat Information Sharing Platforms

An Examination & Lessons Learned Using Personas

Tomas Sander
Hewlett-Packard Labs
Princeton, NJ, USA
tomas.sander@hp.com

Joshua Hailpern
Hewlett-Packard ArcSight
Sunnyvale, CA, USA
joshua.hailpern@hp.com

ABSTRACT

This paper initiates the systematic study of the human elements of participating in an information exchange using a Threat Information Sharing Platform (TISP). Much of the most valuable information to be shared within a TISP is created or validated by human security analysts. Thus getting UX design and the human motivations for a TISP right is crucial for its success. We approach this problem from one of the primary HCI and UX methods | personas. Our results allow TISP engineers and designers to understand and articulate the value propositions as well as the obstacles of a TISP for the CSIRT (Computer Security Incident and Response Team) of an organization. Second, we crafted a set of design requirements explicitly drawn from our personas. These design requirements explicitly highlight how TISPs can be improved, or needs that should be addressed to increase their value-add and usability. Our five personas were created from nine hour long interviews as well as over 20 hours of ethnographic observation of CSIRTs and Security Operations Centers (SOCs.)

Categories and Subject Descriptors

K.6.5 [Management of Computing and Information Systems]: Security and Protection

Keywords

Security; Threat Information Sharing; Security Operations Centers

1. INTRODUCTION

Sharing of threat and cyber security related information is widely believed to greatly improve the ability of organizations to defend themselves against adversaries. Sharing between industry peers, e.g. in the sector-specific ISACs has been occurring for more than a decade now. However, much of this sharing has been manual so far via email, calls and in some cases via web-community portals.

The last few years has seen a push towards automating information exchange where possible that we refer to as **Threat Intelligence Sharing Platforms (TISPs)**. Several threat information sharing platforms are emerging that support the automated ex-

change of indicators, including Threat Central by HP, Threat Connect, Open Threat Exchange (OTX) by Alienvault, Threat Stream and Soltra Edge (whose origins are in the Financial Sector ISAC). Most recently Facebook has entered this space, launching their ThreatExchange. All of these technologies promise to provide automated information sharing, speed and scalability. In this regard, automated platforms are particularly well suited for sharing of lower level indicators, such as malicious IP addresses, domain names, URLs, file hashes etc.

However human users are still a major component in the identification remediation prevention process loop employed in many CSIRT operations and thereby in the utilization of information received from a TISP. For example **Security Operations Center (SOC)** analysts may need to manually review alerts from their networks that have been raised based on shared blacklists. Furthermore “higher level intelligence” (e.g. descriptions of threat actors, their motives, their tools, techniques and procedures, exploit targets and possible mitigations) will usually require human analysts to produce and consume. This contextual intelligence is the most valuable to an analyst as it has typically been validated by another analyst, is related to important security events as it is costly to produce and is more comprehensive thereby allowing an incident responder to better answer the crucial question on his mind what he needs to do if he sees shared lower level indicators on his network.

Subsequently, these TISPs require the ability to not only share data automatically, but also to allow individual contributors to add this rich contextual data. As TISPs are only as valuable as the content they provide, it is crucial to design them in a way that encourages human analysts to contribute and consume information (in addition to enabling automated sharing.) Without actively including human generated data, in addition to lower observables, into TISPs the promise of information sharing will not be realized because lower level observables carry too little contextual information to be truly useful in addressing sophisticated attacks.

Conflating this issue further, even if large organizations decide to share data with each other, an important remaining step is to create and implement the policy and the framework in which information sharing can happen. Companies do not necessarily want to reveal “too-much” information about their own vulnerabilities, but if sharing is too shallow, then the value add is minimal. Many of these decisions what can and can not be shared will also require some level of human decision making. Thus sharing needs first to be successfully operationalized, and it's the **Computer Security Incident Response Team (CSIRT)** [13] on the ground who determines how much is *actually* shared in the day-to-day. It is in those individuals' decisions that the success or failure of the TISP lives.

The primary contribution of this work is to begin the conversation surrounding the *human* elements and motivations in TISPs. In

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.

WISCS '15, October 12 2015, Denver, CO, USA

ACM 978-1-4503-3822-6/15/10 ...\$15.00.

DOI: <http://dx.doi.org/10.1145/2808128.2808136>.

particular, we approach this problem from one of the primary HCI and UX methods | personas. This method allows TISP engineers and designers to understand and articulate the value propositions as well as the obstacles for the CSIRT of an organization. CSIRTs make up a natural user group for TISPs as they are important consumers and contributors targeted by TISPs. Further, creating and publishing a set of personas allows the broader TISP community to have a common language and target use base when working to design great solutions. Our 5 personas were created from eight hour long interviews as well as over 20 hours of ethnographic observation of CSIRT and SOC.

Based on our investigation we articulated our findings in a number of ways. First, we present our fully fleshed-out personas that act as a basis for the remainder of our paper, but also for future reference by researchers and TISP designers. Second, we crafted a set of design requirements explicitly drawn from our personas. These design requirements explicitly highlight how TISPs can be improved, or needs that need to be addressed to increase their value-add and usability. Third, we outline how future work into TISPs can be done to continue to include the “human” aspects of incident response. While this approach may have been conducted in industrial settings and not been published, to our knowledge, this is the first published work to look at the human-centered aspect of TISPs.

2. RELATED WORK

IODEF/RID [5, 11] and STIX/TAXII [1] are formats for the exchange of threat information and key enablers for TISPs. In particular STIX has been designed to express human generated threat information in a structured way in addition to machine generated data.

The literature on operational aspects of information sharing is still relatively sparse. However NIST is in the process of creating a guide to information sharing [8] that clarifies key concepts and practices of how organizations can plan and implement information sharing practices and thus provides some useful background to this paper.

3. SCOPE AND MOTIVATION

Whereas much of the existing work has focused on the infrastructure and information sharing functionality of TISPs, there is a lack of understanding of the specific value-proposition for the end users of such a system. As these TISPs only succeed if end-users contribute and see value add, this work looks to understand and articulate these users’ value proposition.

To this end, this paper uses observational study and open-form interviews to construct representative profiles of different classes of end-users, known as **Personas**. A persona is a rich profile of a specific sub-group of target users. These profiles are highly detailed, capturing the background, personal history, and experience with the domain subject matter. By creating a detailed and rich persona, creators can then put themselves in the shoes of that specific persona’s value set - and evaluate the design choices they are making. Using these personas, future developers of these intelligence sharing systems can be better guided by the design requirements extracted by doing this exercise.

This work is not designed to be the list of all possible personas, but rather a starting set that can and should be built upon as the area of information sharing networks grows and expands.

4. TISP EXAMPLE

To provide a better basis for discussion of TISPs, we here describe some crucial feature of Threat Central (TC). This should not be viewed as explicit support for this one solution, but rather as a specific illustrative example of how TISPs work. Other sharing platforms share many common features with Threat Central, so we believe this description provides a good overview about the type of technologies emerging in this area. Figure 1 highlights screenshots of a typical TC workflow as discussed in this section.

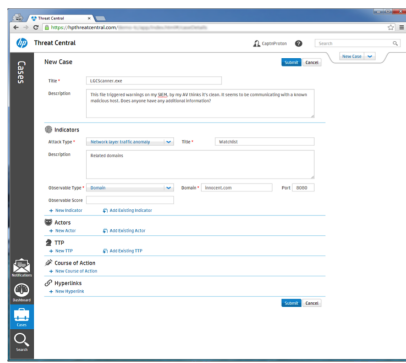
TC supports automated and manual sharing. Automated sharing is supported via close integration with a market-leading Security Incident and Event Management (SIEM) tool (ArcSight ESM) that allows for the automated exchange of indicator lists (e.g. containing malicious domain names, IP addresses etc.) As additional background note that SIEM tools collect security relevant data from system and network logs as well security alerts from firewalls, IDS systems etc. SIEMs perform correlations among these data sources and will flag up suspicious events. In the common SIEM-based set-up of CSIRTs SOC analysts (sometimes also called level 1 analysts) will monitor these SIEM alerts that can range in the hundreds or thousands per day and will perform an initial triage on the data. Alerts that seem worth investigating further will be escalated to Incident Responders (or level 2 analysts). An analyst can receive more information about the indicators implicated in an alert from the Threat Central portal if available. Automated exchange is also supported via the STIX and TAXII standards.

A second way to access the system is manually via a portal where an analyst can create a Case. A Case consists of a collection of security relevant templates that an analyst can fill in. They follow the general outline of the STIX data model. There are lower level Observables (IP addresses, domains names, domain servers, mutex, registry data, or behavioral aspects of malware, email headers etc.). Indicators contain one or more observables and add some context to these observables explaining what they mean. Context here includes time stamps, when the observables were active, confidentiality and severity scores, as well as information about the role these observables play in an attack (e.g. for a malicious URL whether it is a phishing site or a drive-by malware download site, for a domain name, if it’s a C&C server, or to which phase in the kill chain [7] the observables are related). In addition we can express “higher level intelligence” such as information about Threat Actors, the Campaigns they’re running, Exploit Targets, the Tools, Techniques and Procedures (TTPs) used in an attack as well as Mitigations to remediate a threat. Analysts can receive notifications about cases of interest, search the list of cases, and enrich and add comments to those cases that have been posted in communities to which they belong.

Threat Central supports several sharing communities such as a global community, industry sector specific communities and private communities that Threat Central members can freely create among themselves. Analysts can choose which communities they wish to share information with and whether they want to do so anonymously, via a pseudonym or with their real identity.

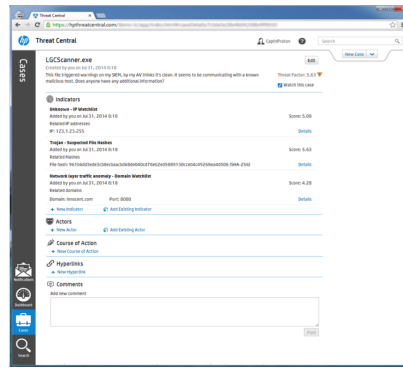
Analysts can also search the Threat Central repository of indicators.

At the Threat Central backend data received from participants will be enriched with data from other intelligence feeds and sources and cross-correlated with each other, e.g. to identify attack trends. Confidence, severity and impact scores are also computed for these data. Data with sufficiently high scores will be pushed automatically as watchlists to participants.



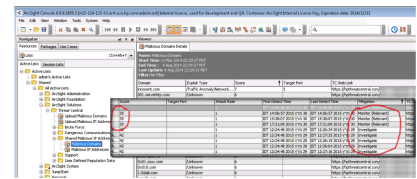
(a) Create a Case

CaptnProton runs into suspicious behavior with LGCScanner.exe



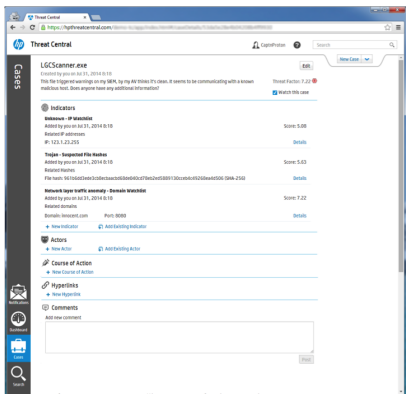
(b) Distribute Indicators

CaptnProton submits the case. Indicators are now extracted and sent to community members.



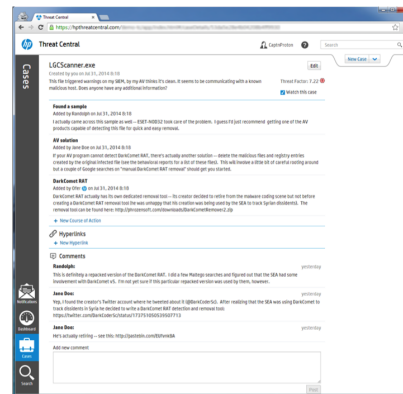
(c) Distribute Indicators cont.

SIEM customers benefit from direct integration and targeted intelligence \ ArcSight ESM Pictured



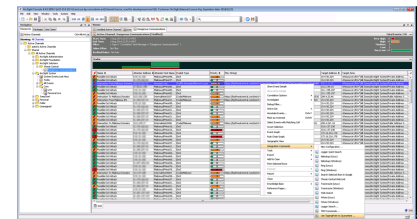
(d) Collaborate with Experts

Security Researcher enhances indicators with contextual information



(e) Get Results

By the end of the process, CaptnProton's case is filled out with relevant and contextual information.



(f) Mitigate

Easily quarantine bad IPs/domains using your favorite SIEM and IPS \ ArcSight ESM and TippingPoint SMS Pictured

Figure 1: Illustrative Example of TISPs | HP Threat Central Screenshots
All product views are illustrations and might not represent actual product screens
Images are high resolution, and can be zoomed in digitally in PDF

5. PERSONA CREATION

A persona [10] is a fictionalized representation of a collection or demographic of end users. These personas are in many ways a direct response to the Egocentric Intuition Fallacy which, paraphrased from the Handbook of Human Computer Interaction [6], states that the creators of systems (engineers, UI designers, etc) overestimate the degree to which what is true for them will be true for others. In short, when creators build systems to solve their specific needs, they generally only solve their own needs, and don't take into account the needs of the broader user population.

Personas, on the other hand, are an easy way to overcome the Egocentric Intuition Fallacy in early stage development (user studies are always recommended upon completion of a prototype). Personas are created by a detailed examination of the target population(s), breaking them down into as many as necessary sub-groups, to capture the majority of needs, concerns, and values. In this regard, "personae should not be used to stereotype personal characteristics...but rather to capture the diversity..."[10], thus it is often needed to create multiple personas for each "role" being studied.

While there are many techniques to create personas (e.g. marketing research), or raw data [9], they are often created through interviews and observational ethnographies[2, 4, 3]. The creation of the

persona can vary in detail, but all should include a fictional name, role, set of needs (personal and professional), interests (personal and professional), and concerns/challenges [10]. Even seemingly innocuous details (e.g. relationship/family, hobbies, and housing) can provide insights into motivations and needs¹. When examining personas, they often can benefit from pictures and personal history. This can reduce stereotypes, and give concrete backstory to help inform system design.

5.1 Methods

The authors of this work simultaneously conducted two processes to create the personas presented in this paper. One author conducted a series of nine and a half hours of one-on-one interviews, with 11 domain experts from a large company's CSIRT - ranging from analysts, to managers, to members of the hunt team. At the same time, the other author conducted a series of observational

¹An individual who is single (and looking to date), living in an apartment has more disposable income and little to know financial responsibilities, has fewer time commitments, and is more likely to engage in risks in their life. In contrast, someone who has a home (with a mortgage) a spouse and children (extra expenses and college funds) has less financial flexibility, and is less likely to take risk and would value job security and steady schedules.

ethnographies of security analysts and hunt teams totaling over 20 hours. These two simultaneous approaches generated a series of observations and patterns that were distilled into five personas, detailed in the remainder of this section.

5.2 Personas

We created in total five personas to exemplify the main users of TISPs. Two personas represent SOC Analysts (Table 1, 2), two Incident Responders (IR) (Table 3, 4), and one a Cyber Threat Intelligence (CTI) analyst (Table 5). In our personas we present relevant aspects of their work, information about their education and background, their personal and professional goals and aspirations as well as their frustrations and challenges. It may be helpful for the reader to review the personas before moving on to the implications for design.

6. IMPLICATIONS FOR DESIGN

Based on the presented personas, we explored what values, challenges, and personality traits existed for the highly varied target populations. From these personas, we were able to generate a series of implications for design | features, workflows, and presentations that would be extremely beneficial for usability and utility of intelligence sharing systems. Each design requirement references back to the personas with clickable indexes (e.g. **BJ.1** referencing Jacob's Bio, 1st point) Before going into detail on our design requirements, we would like to call out three high-level, we believe novel, insights gained from our investigation.

6.1 High Level Insights

First, personal motivations and incentives of end users to share information do differ from (though not necessarily contradict) the corporate motivations. In particular, end users desire the ability to advance their career, enhance their skill level, engage in networking with their peers, and generally have a "desire to belong." Thus, while sharing may be part of their job, to maximize their participation systems should also facilitate the personal motivations.

Second, our personas differ significantly in terms of the type of information and the amount of information they contribute and consume from a TISP. There is no "one" typical user of a TISP. We believe that optimizing TISPs for these different personas requires slightly different, complementary features, but will lead to best results for the quality and amount of the information being shared.

Third, with younger users getting into the field (e.g. out of undergraduate programs with degrees in computer security), the tolerance for "clunky" or "everything but the kitchen sink" interfaces has gone down. Rather, there is a large preference for younger users for not just trend user interfaces (the visual presentation), but sophisticated user experience (workflow through the interface). Further, mobile and social aspects of their personal lives are requested in their professional work. In many ways, their personal experience and standards with technology has fully permeated into the workforce. While this is not explicitly called out in the following implications for design, we wish to highlight the shift that has occurred, and how commercial software aesthetics are now expected in enterprise grade solutions.

6.2 Design Requirements

We formulated six major dimensions for how to improve TISPs: encouraging member contributions to TISPs, data enrichment and cross-correlation, driving engagement via gamification, integration with TI Management Platform (TIP), actively supporting intel requirements, and improving data visualization and UI quality. Within each dimension, we highlight a series of design requirements to

achieve the dimensions' end goal. While this set of design requirements is expansive, the authors wish to state that this list is not exhaustive.

6.2.1 Encouraging member contributions to TISPs

These design requirements focus on how to operationalize and ideally improve the contribution process for CSIRT members and thereby enhance the quality and quantity of content in a TISP.

DR1 SOC analysts (level 1 analysts) are not producers of Indicators of Compromise (IOCs). (**WP.1, FS.1**) TISP contributions that take more than a mouse click are unlikely in the time-pressured SOC environment. (**FP.2, FS.3**) Thus TISPs should be extremely easy to contribute to if not integrated directly into the SIEM tools SOC analysts are using.

DR2 SOC analysts can be producers of valuable feedback on existing indicators, e.g. down-voting false positives. This helps improve the quality of shared indicators. (**WP.1, FP.3, FP.4, WS.1**)

DR3 The capability to comment on (down- or up-) votes of indicators is valuable. (**GS.3, FS.4**)

Comments make votes more meaningful to other TISP users, as they promote a second pair of eyes and allow analysts to show their skill to peers in other organizations. This creates new opportunities to collaborate/belong in a high-pressure environment. Commenting on comments of others and alerts on changes help create a dynamic experience.

DR4 Incident Responders (IR) are the primary users of the Case feature in TISPs, e.g. to support investigations. Cases will be the main channel how IR will add IOCs and other content to TISPs. (**WP.1**) Thus, TISPs need to tie into case management tools.

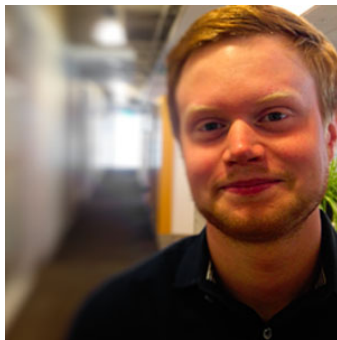
DR5 CTI analysts can provide feedback on received intel to the intel provider, however there is a high sensitivity to not disclose company internals about actual incidents or vulnerabilities. Most Threat Intelligence (TI) providers would love getting that type of feedback to improve the quality of their intelligence feeds. This raises the question how such feedback can be given in an effective, yet privacy-preserving way. (**WH.4, WH.5**)

DR6 Automated bulk validation and cleaning of received indicators and intel would be valuable, before pumping them into a SIEM for monitoring. (E.g. utilizing feedback on how many or which indicators have been seen elsewhere.) Providing these validation and cleaning services for uploaded data provides a golden opportunity for TISPs to incentivize analysts to upload data to a sharing platform. (**FH.1, FH.2, FH.5**)

DR7 IR and CTI analysts will query intel repositories of a TISP triggered by anomalies seen in the organization. (**WP.1, WP.2**)

DR8 Sensitive data, e.g. Traffic Light Protocol (TLP)² Red marked data, are more likely to be shared with trusted individuals rather than with companies. To accommodate this TISP access control mechanisms need to allow to control access to shared data at the level of the individual, not just their organization. (**FH.6**)

²<http://www.us-cert.gov/tlp/>



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.5 Relationship: Single. Dating.
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”



BIOGRAPHIC INFORMATION

- BS.1 Age:** 25
BS.2 Education: BSc in CS
BS.3 Experience: First exposure to security.
BS.4 Housing: Renting with wife in East Bay, due to low cost
BS.5 Relationship: Married. No Children
BS.6 Hobbies: Writing apps, hiking, playing classical Indian music instruments
BS.7 Values: Learning, succeeding professionally, the well-being of his family and parents.
BS.8 Other: Grew up in Hyderabad, India and went to college in Florida. Moved into security because there's a major shortage of skilled workers.

GOALS

- GS.1** Build a successful career in IT security.
GS.2 Become a deep expert in incident response area such as forensics, malware analysis.
GS.3 Establish professional network.
GS.4 Get a green card.
GS.5 Make enough money to start a family and buy a house in the Bay Area.

WORKFLOW

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

FRUSTRATION & CHALLENGES

- FS.1** Shift rotation can make spending time with his wife who also works difficult.
FS.2 “Eyes on glass” for whole shift exhausting.
FS.3 Time pressure
FS.4 Intel without context makes triage difficult.

PERSONAL TECHNOLOGY USE

- PS.1** Uses Android products as they give him better control.
PS.2 Loves to try out new gadgets
PS.3 Goes to Quantified self meet-ups
PS.4 Less active on social media platforms both for privacy concerns and a preference for spending lots of time by himself.

Table 2: Satish Kapoor | SOC Analyst
“I really need more information to make meaningful escalation decisions. If all I have is that an IP address is “bad” that’s useless to me”



BIOGRAPHIC INFORMATION

- BP.1 Age:** 32
- BP.2 Education:** BSc in CS
- BP.3 Experience:** 4 Years in Incident Response
- BP.4 Housing:** Just bought house
- BP.5 Relationship:** Married. 2 small children
- BP.6 Hobbies:** Rock music, hiking, politics
- BP.7 Values:** Civil liberties, independence, spirituality

GOALS

- GP.1** Advance on technical track and become specialist in malware analysis.
- GP.2** Learn and improve on ongoing basis about ever-shifting attack techniques.
- GP.3** Being a valued contributor to the community of security professionals.

WORKFLOW

- WP.1** Investigate incidents that have been flagged up by SOC analysts.
- WP.2** Hunting e.g. using important IOCs or TTPs
- WP.3** Cyclical collaboration with CTI, e.g. to make attribution.
- WP.4** Work with businesses on containment and remediation. Important to articulate attack in terms of risk.
- WP.5** Multi team work to resolve incident (e.g. forensics, malware analysis etc.)

FRUSTRATION & CHALLENGES

- FP.1** Work life balance is a challenge due to being on call when a major incident happens. Also sometimes long hours.
- FP.2** Sometimes not the right tools available.
- FP.3** Sometimes information you need is not available.
- FP.4** In time-critical incident investigations multi-team efforts with interdependencies occasionally a challenge as teams have different priorities.
- FP.5** Containment and remediation often requires working with people in the businesses who may be non-technical and have difficulties of appreciating what needs to be done to remediate an incident.

PERSONAL TECHNOLOGY USE

- PP.6** Uses technology where it's useful, but also likes to turn it off if not. Doesn't want to spend his whole life in front of screens or with gadgets.

Table 3: Phil Baker | Incident Responder
"I love solving the intricate puzzles that sophisticated attacks pose"

DR9 Well-tailored TISP responses can save IR work as well as encourage data contributions. (Ex: A button for receiving YARA rules for malware samples that have been provided to TISP by the analyst would incentivize him to upload malware samples, whenever these rules could help him in an investigation.) (**WP.1, WP.2**)

6.2.2 Data enrichment and cross-correlation

These design requirements focus on the value-add of adding more context to information that has been shared with the TISP.

DR1 While the value added by basic TISP data enrichment (Whois, geo location, etc.) is minimal, if well done it can keep analysts on TISPs as a preferred tool. (**FP.1**). Thus TISPs need to be thought of as more than just a raw information sharing platform.

DR2 Automated cross-correlation of data across different sources with consolidated opinions from the different sources (perhaps highlighting differences in opinion) provides a large amount of value and saves analysts time. (**FH.1, FH.2**) Moreover, if different TISP services or communities can collaborate and share some of their feeds and data, the goal of broad security awareness can be more easily achieved.

6.2.3 Driving engagement via gamification

These design requirements focus on documenting personal growth and motivation for continued high-quality contributions.

DR1 Badges can provide meaningful feedback and motivation during normal work (age group: **BC.1** & **BS.1**, education: **BC.2, BS.2**)

DR2 Early career analysts benefit from badges as it helps their professional qualifications. They can progress from "Newbie" to "TISP Master." This can provide a professional ranking independent of their growth in their company (career aspirations: **GC.1, GS.1**)

These goals and achievements should contain both raw activity, verified activity by the community, and community impact allowing individual contributors to demonstrate their depth, breath and impact of their skills

DR3 Leaderboards may not be an ideal feature as they would need to make sure not to add additional pressure in what is already a high-pressure environment (**FC.2, FS.3**). For example, feedback should be positive (suppress 'losers' from the leaderboard ranking).

6.2.4 Integration with TI Management Platform (TIP)

These design requirements focus on automation of Threat Intelligence (TI) handling and higher-level data management. Organizations that consume a variety of threat intelligence feeds benefit from a platform that handles the management and fusion of this data. Data can also originate from internal sources, e.g. to compare them against external feeds. We call this a TI management platform (TIP). A TIP also allows an organization to assign its own confidence and relevancy scores to its sources. TIPs can be distinguished from TISPs which are primarily focused on enabling (bi-



BIOGRAPHIC INFORMATION

- BJ.1 Age:** 23
BJ.2 Education: Recent college graduate with BSc in Computer Security & Forensics
BJ.3 Experience: Internship
BJ.4 Housing: Renting alone
BJ.5 Relationship: Single. Dating casually
BJ.6 Hobbies: Sports plane pilot, travel, adventures
BJ.7 Values: Social and civic values, ecology, and fitness

GOALS

- GJ.1** Get valuable real life work experience after school.
GJ.2 Eventually do a Master or Ph.D. in CS or Computer Security Programs.
GJ.3 Loves technological cutting edge and might eventually wish to join security start-up
GJ.4 Happy to work hard, as long as he feels he's progressing.
GJ.5 Loves the rush of resolving incidents.
GJ.6 Enjoys opportunities for human collaboration in his job.

WORKFLOW

- WJ.1** Investigates incidents that have been flagged up by SOC analysts.
WJ.2 Hunting e.g. using important IOCs or TTPs.
WJ.3 Analyzes network and other logs.

FRUSTRATION & CHALLENGES

- FJ.1** There's always too much to do and to learn. Unclear boundaries between job and private life.
FJ.2 Gets annoyed by the many clunky UIs from security and intra company tools.
FJ.3 Slow and cumbersome access to information. Breaks his state of flow when working.
FJ.4 Hates to be glued to a desk for hours on end and would love to use mobile technologies to work while walking around or being on the treadmill at the company fitness center.
FJ.5 Loves learning from his older colleagues but is weary that he's assigned a high proportion of dull jobs as the young one.

PERSONAL TECHNOLOGY USE

- PJ.1** Extensive user of mobile devices and social platforms for everything from shopping to socializing.
PJ.2 Used to making many decisions by consulting friends and others.

Table 4: Jacob Cook | Incident Responder
"Computer Security is one of the most exciting fields to be in these days"



BIOGRAPHIC INFORMATION

- BH.1 Age:** 34
BH.2 Education: BSc in EE
BH.3 Experience: 4 years in Incident Response, 5 years in Intelligence. Background from DOD.
BH.4 Housing: Homeowner in Atlanta.
BH.5 Relationship: Married. Two children.
BH.6 Hobbies: Baseball, running and keeping fit as he "ages"
BH.7 Values: Freedom, self-reliance, global thinking
BH.8 Other: Grew up in Charleston, SC

GOALS

- GH.1** Be the leader in the creation of emerging field of threat intelligence driven security.
GH.2 Trusted, reciprocal relationships with industry peers. Creating trusted networks.
GH.3 Keep abreast of the highly dynamic, constantly changing threat landscape.

WORKFLOW

- WH.1** Monitor threat landscape
WH.2 Gateway for incoming and outgoing intel
WH.3 Disseminating intel to right places in organization
WH.4 Counsel for incident response investigations
WH.5 Vetting intel
WH.6 Engage with sharing communities.

FRUSTRATION & CHALLENGES

- FH.1** Constantly having to cut and paste data manually between different tools.
FH.2 Cross-correlation is hard.
FH.3 Indicators frequently outdated.
FH.4 Lack of well-defined collection criteria leads to "fog of more".
FH.5 Benefit (to him) of outgoing sharing not clear.
FH.6 Not possible to disclose sensitive information (e.g. if it allows to conclude company has been under an APT attack)

PERSONAL TECHNOLOGY USE

- PH.1** Fan of computer games (MMOGs like WoW) at nights after the kids go to bed.

Table 5: Hal Brady | Threat Intelligence Analyst
"You can achieve better security through leading with intel and aligning your assets accordingly"

directional) sharing. Whereas TISPs can be naturally implemented as a cloud service a TIP would typically reside locally.

DR1 A 'one-stop-shop' for TI would make CTI a lot more effective. **(FH.1)**

Far too much time is spent with integrating various sources (via cutting and pasting), checking a number of web sites, cross-correlating the data etc.

What's needed is effective, unified management of internal and external TI data. Thus adding TIP functionality to TISPs or alternatively a good integration between a TISP and TIP solution would deliver more value than a TISP alone. Whether this is a data pull from or push to TISPs is an open question.

DR2 Simplicity of upload of data to TISP key. Upload should ideally be done in two phases: 1) uploading and review and 2) sharing. **(FH.1, FH.5)**. This could even have an internal check as a third phase within a company before public sharing.

DR3 Non-attribution (i.e. hiding who contributed data to TISPs) often essential for sharing, as well as using Traffic Light Protocol (TLP) to control onward sharing. **(FH.6)**

There is a tension between the requirement of non-attribution and the desire of an analyst to gain a professional reputation via his sharing activities. Badges and pseudonyms are one way of striking a balance between these conflicting requirements. However the privacy protection badges offer in real life scenarios need to be better explored before implemented, and will likely depend on the granularity of the badge system and the distribution of attributes that earn badges within a community.

DR4 Automated outward sharing of indicators from TIPs into TISPs would be beneficial to enhance sharing. **(FH.1, FH.5)**. To better protect companies, this can be done as aggregates, e.g. over a time period, rather than raw occurrences.

DR5 Unified management of sharing relationships with different groups would be a beneficial as there is a significant cost to maintaining these relationships. **(WH.6)**

6.2.5 Actively support intel requirements

These design requirements focus on the requirements for the data itself that is being shared.

DR1 Providing minimal context is essential for indicators. **(FS.4)**

For IPs minimal context would be: related ports, URLs, sample packets. For domains, context such as C&C, scanning, concern about ingress or egress activity etc.

DR2 More context is better also for SOC analysts to help with their triage decisions **(FC.1, FS.1)**

Info about kill-chain phase, associated actors and campaigns helps to determine severity and if events should be escalated to an investigations team. For example indicators associated to later phases in the kill chain imply greater risk.

*Including carefully chosen Time To Live (TTL) fields with intel is key to avoiding false positives. **(FC.4)***

DR3 Intel should be validated where possible, ideally by another analyst or the CTI function. High false positive rates will ruin the credibility of a platform. **(FC.3)**

This can be enhanced by taking an analysts' history and reputation into account when distributing intel, or if the credibility is too low, waiting until a second or third report is received. This could be achieved in parallel by using an ensemble learning approach.

DR4 IR benefits from a broad range of intel. **(WP.1, WP.2)**

DR5 Provide IOCs to support detection in an environment **(WP.2)**

DR6 Provide contextual information (actors, targets, motivations, campaigns, mitigations) that informs investigation, containment and mitigation. **(WP.2, WH.4)**

DR7 Kill chain data is very helpful to reconstruct unknown attack paths. **(WP.1, WP.2, WP.3)**

DR8 Beyond basic indicators, specialists need more detailed IOCs to support their in depth investigations. **(WP.4)**

DR9 Providing historical info for indicators is also important to CTI as it is known that attackers reuse resources over time. **(WH.4)**

DR10 Pivoting capability (i.e. being able to follow the chain of associated information of an indicator such as other indicators, threat actors etc.) is a much sought after functionality. **(WH.4)**

6.2.6 Multi-team support

These design requirements focus on the collaborative/team environment inside of SOCs.

DR1 Investigations often require collaboration between different individuals and teams in the organization due to complementary expertise. This raises the question if/how a sharing and intel management platform can best support multi-team work. **(WP.4, FP.4, WH.3, WH.4)**

When a case is shared between different teams relevant intel should be shared as well, including visualizations and results from pivoting and analysis. Teams should not have to duplicate efforts.

6.2.7 Training opportunities and needs

These design requirements focus on training and career growth beyond one individual company.

DR1 Only need to provide limited training for the TISPs contribution of giving feedback on indicators **(FC.3, FS.3)**

In essence: A SOC Analyst needs to understand when indicators and feedback should NOT be added to TISPs based on company policy. Training videos and regular quizzes are a scalable delivery vehicle for much of the training needed. Should be well-accepted by targeted junior employees.

DR2 Provide more complex training for parties that receive and contribute more complex data from TISPs, such as IR and CTI. **(WP.2, WP.3)**

As issuers of cases and complex TISP queries they need an advanced understanding when not to share information.

Ex: malware samples that appear to be part of a targeted campaign against Acme Inc. will not be shared as they may contain Acme Inc. specific data, e.g. relating to Acme Inc. networks.

In addition trainees should learn criteria that help their decision-making when they should share, and how to do it most effectively for their own and the recipient's benefit.

DR3 Create 3 paths on which users can advance. **(GC.1, GC.4, GS.1, GP.2, GP.3, FP.6, GH.1, FH.6)**

1. TISPs User Path | system issues badges that reward TISPs contributions.

2. Training Path | analysts/responders can take specific trainings.

3. Certification Path for intel management and sharing.(Could be delivered in partnership with an organization like SANS.)

DR4 Badges and certifications gained on the 3 paths can be part of the profiles of TISPs users. Tagging contributions with these badges helps analysts to determine how much to trust contributions, even while the exact identity of the contributor is hidden. Non-attribution key requirement (**FH.6**).

6.2.8 Data Visualization, UI Quality

These design requirements focus on the presentation layer in TISPs.

DR1 Visualization of intel, as well as interactive querying and pivoting capabilities help CTI in analyzing data. (**FH.2**)

The work by Edward Tufte (eg. [12]) should be deeply consulted by visualization designers, as a launching point for creating meaningful visual representations of data. Ex: visualization can link a number of entities and their relationships in a graph. For example: malware samples, domains, IPs, email addresses, whois info. You may also wish to visualize malware info.

A challenge for visualization is to figure out what kind exactly helps analysts in their work. There is a concern that there are too many visualizations that are only eye candy.

Cross-correlation and aggregation of data tends to lead to even more data to cognitively process for an analyst. Clever visualization would be quite advantageous to deal with over a twenty page text print-out to represent such data.

DR2 The typically clunky UIs of traditional security tools are much less tolerated by the new generation of incoming analysts and incident responders and should be replaced by state of the art UIs that match the sophistication of consumer technology. (Chris' quote **Table 1, FJ.2**)

DR3 Offer key functions of intel work and sharing such as pivoting, drill down, cross-correlation, commenting etc. on tablets to support mobility and unchain analyst from the desk. (**FJ.4**)

7. FUTURE WORK

While it is outside the scope of this one paper to build a TISP with these design requirements and validate end-user reactions, the next logical progression is to work with one of the existing solutions and attempt to integrate some if not all of these design recommendations. Once implemented, this will allow a formal user study to validate their role on user data sharing, and even present quantitative data to support or refute the design recommendations proposed.

8. CONCLUSIONS

This paper created a set of personas for what we believe are the most important users of a TISP. It would be useful to develop additional personas in the future. We suggest e.g. to develop personas for CISOs. As we confirmed in initial interviews their needs are broadly related to creating useful dashboards that allow them to get a high level view of the threat landscape for their organization. They also wish to see metrics that allow them to evaluate the effectiveness of information sharing and its impact on their organization. In addition it may be useful to develop personas for IR experts in areas such as malware analysis and forensics.

We believe this work demonstrates the usefulness and richness of investigating the human elements of information sharing. More research should address other important human aspects such as how TISPs can help to build up trust among members of the sharing community.

We also recommend to develop training programs and certifications for information sharing and more generally for using and creating threat intelligence.

Ultimately we are hopeful that well-designed technical platforms combined with these “soft” measures can help establish a culture of sharing among security professionals that give defenders a new edge against their adversaries.

9. ACKNOWLEDGMENTS

The authors would like to thank the members of a major corporate CSIRT for their willingness to freely share their observations and insights with us. We'd also like to thank HP Security Research for creating the case content of the Threat Central screen shots and we would like to thank Ted Ross, head of HP Security Research, for his support of this research.

10. REFERENCES

- [1] S. Barnum. Standardizing cyber threat intelligence information with the structured threat information expression (STIX). *MITRE Corporation*, page 11, 2012.
- [2] Å. Blomquist and M. Arvola. Personas in action: ethnography in an interaction design team. In *Proceedings of the second Nordic conference on Human-computer interaction*, pages 197–200. ACM, 2002.
- [3] D. Broschinsky and L. Baker. Using persona with xp at landesk software, an avocent company. In *Agile, 2008. AGILE'08. Conference*, pages 543–548. IEEE, 2008.
- [4] A. Cooper et al. *The inmates are running the asylum:[Why high-tech products drive us crazy and how to restore the sanity]*, volume 261. Sams Indianapolis, 1999.
- [5] R. Danyliw, J. Meijer, and Y. Demchenko. The incident object description exchange format. *IETF*, 2007.
- [6] M. Helander, T. Landauer, and P. Prabhu. *Handbook of Human-Computer Interaction*. Elsevier, 1997.
- [7] E. M. Hutchins, M. J. Cloppert, and R. M. Amin. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, 1:80, 2011.
- [8] C. Johnson, L. Badger, and D. Waltermire. *Guide to Cyber Threat Information Sharing [draft]*. NIST Special Publication 800-150, October 2014.
- [9] J. J. McGinn and N. Kotamraju. Data-driven persona development. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1521–1524. ACM, 2008.
- [10] E. McKay. *Enhancing learning through human computer interaction*. Igi Global, 2007.
- [11] K. M. Moriarty. Real-time inter-network defense (RID). *IETF*, 2012.
- [12] E. R. Tufte and P. Graves-Morris. *The visual display of quantitative information*, volume 2. Graphics press Cheshire, CT, 1983.
- [13] M. J. West-Brown, D. Stikvoort, K.-P. Kossakowski, G. Killcrece, and R. Ruefle. Handbook for computer security incident response teams (csirts). Technical report, DTIC Document, 2003.