Hewlett Packard
Enterprise

UX Aspects of Threat Information Sharing

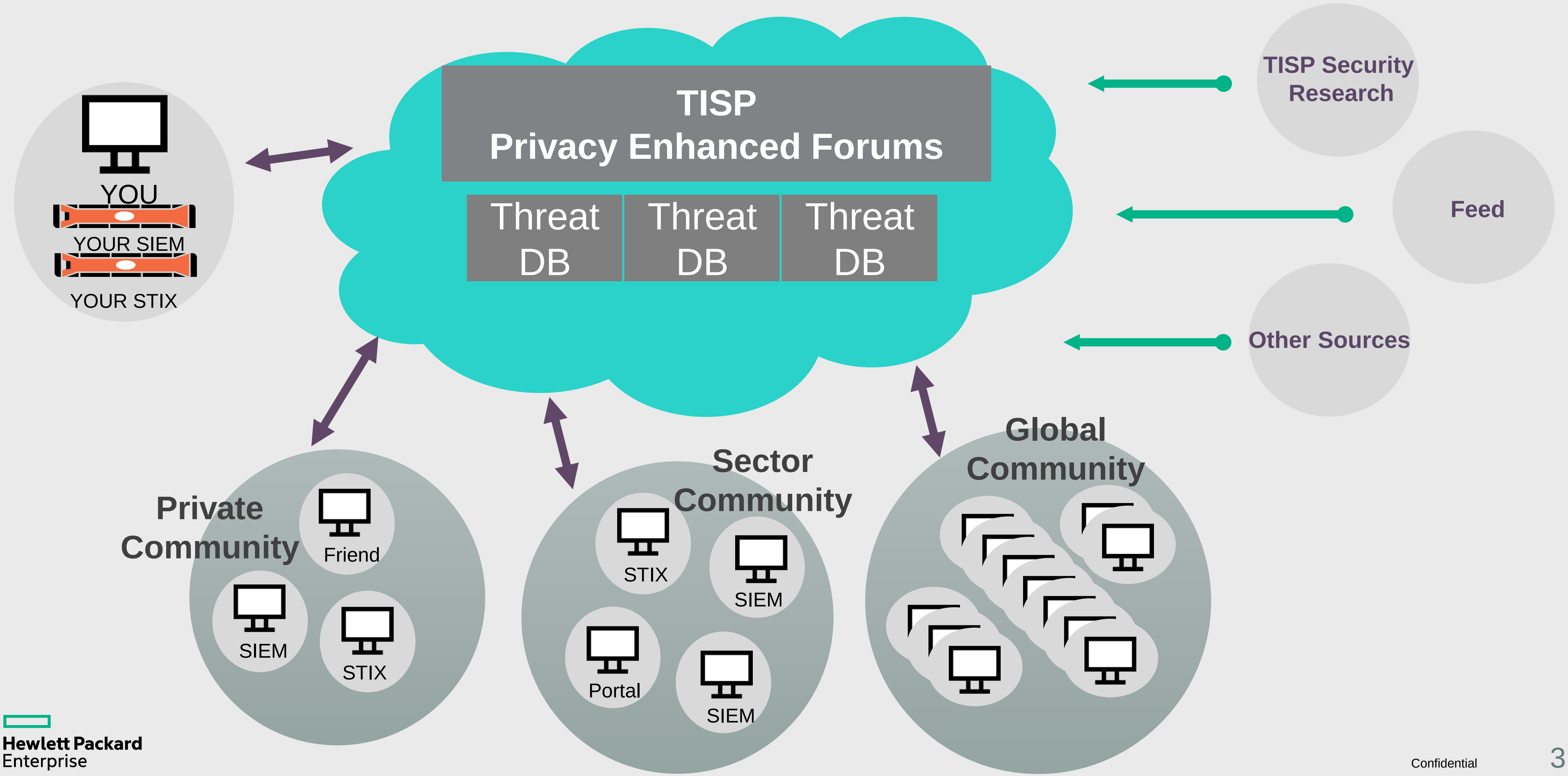
Tomas Sander
Hewlett Packard Laboratories

February 25th 2016

Starting point

Human interaction still critically important at many stages of Threat Intelligence lifecycle.

Threat Information Sharing Platform (TISP)



Hewlett Packard Enterprise

Confidential

Key challenge for TISPs

Encouraging users to contribute content.

Guiding question:

How can we encourage users to contribute more than they currently do?

TISPs 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 TISPs for Analysts and validate potential solutions - directing development strategy.

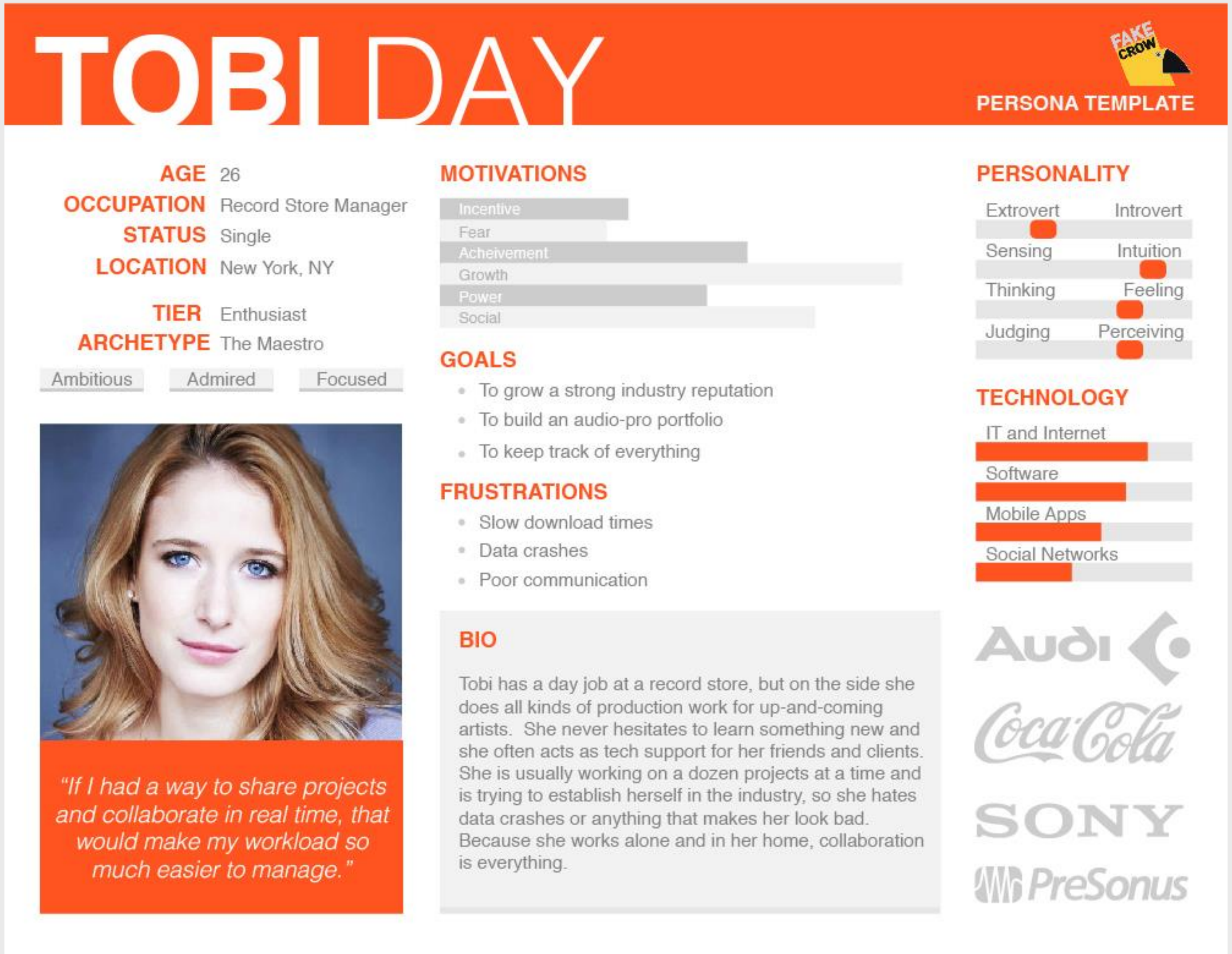
Our contribution to-date

- Initiate the systematic study of (some) UX and HCI aspects of TISPs
  - T. Sander and J. Hailpern. UX Aspects of Threat Information Sharing Platforms: An Examination & Lessons Learned Using Personas. In Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security (WISCS '15).

Key Task

Understanding TISP users

Our approach: Personas



TOBI DAY

FAKE CROW

PERSONA TEMPLATE

AGE	26
OCCUPATION	Record Store Manager
STATUS	Single
LOCATION	New York, NY
TIER	Enthusiast
ARCHETYPE	The Maestro

Ambitious Admired Focused

"If I had a way to share projects and collaborate in real time, that would make my workload so much easier to manage."

MOTIVATIONS

Incentive
Fear
Acheivement
Growth
Power
Social

GOALS

- To grow a strong industry reputation
- To build an audio-pro portfolio
- To keep track of everything

FRUSTRATIONS

- Slow download times
- Data crashes
- Poor communication

BIO

Tobi has a day job at a record store, but on the side she does all kinds of production work for up-and-coming artists. She never hesitates to learn something new and she often acts as tech support for her friends and clients. She is usually working on a dozen projects at a time and is trying to establish herself in the industry, so she hates data crashes or anything that makes her look bad. Because she works alone and in her home, collaboration is everything.

PERSONALITY

TECHNOLOGY

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.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.

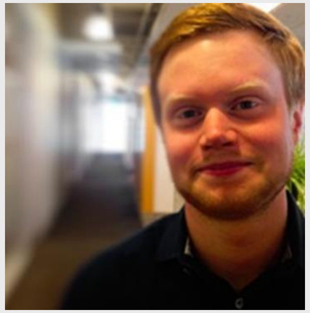
PC.3 Shares his photos via Instagram.

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”

3 Groups, 5 Personas



Chris, SOC Analyst

Satish, SOC Analyst

Phil, Incident Responder

Jacob, Incident Responder

Hal, CTI Analyst

Based on 9h of interviews and 20h of ethnographic observation of CSIRTs and SOCs

Findings: TISP contributions differ by role

SOC Analysts

- Feedback on specific indicators
- Annotations

Incident Responders

- New IOCs, cases, malware samples
- Tools and practices how they solved certain problems

CTI Analysts

- Gatekeeper
- Enable automated sharing
- Detailed feedback on received intel

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.

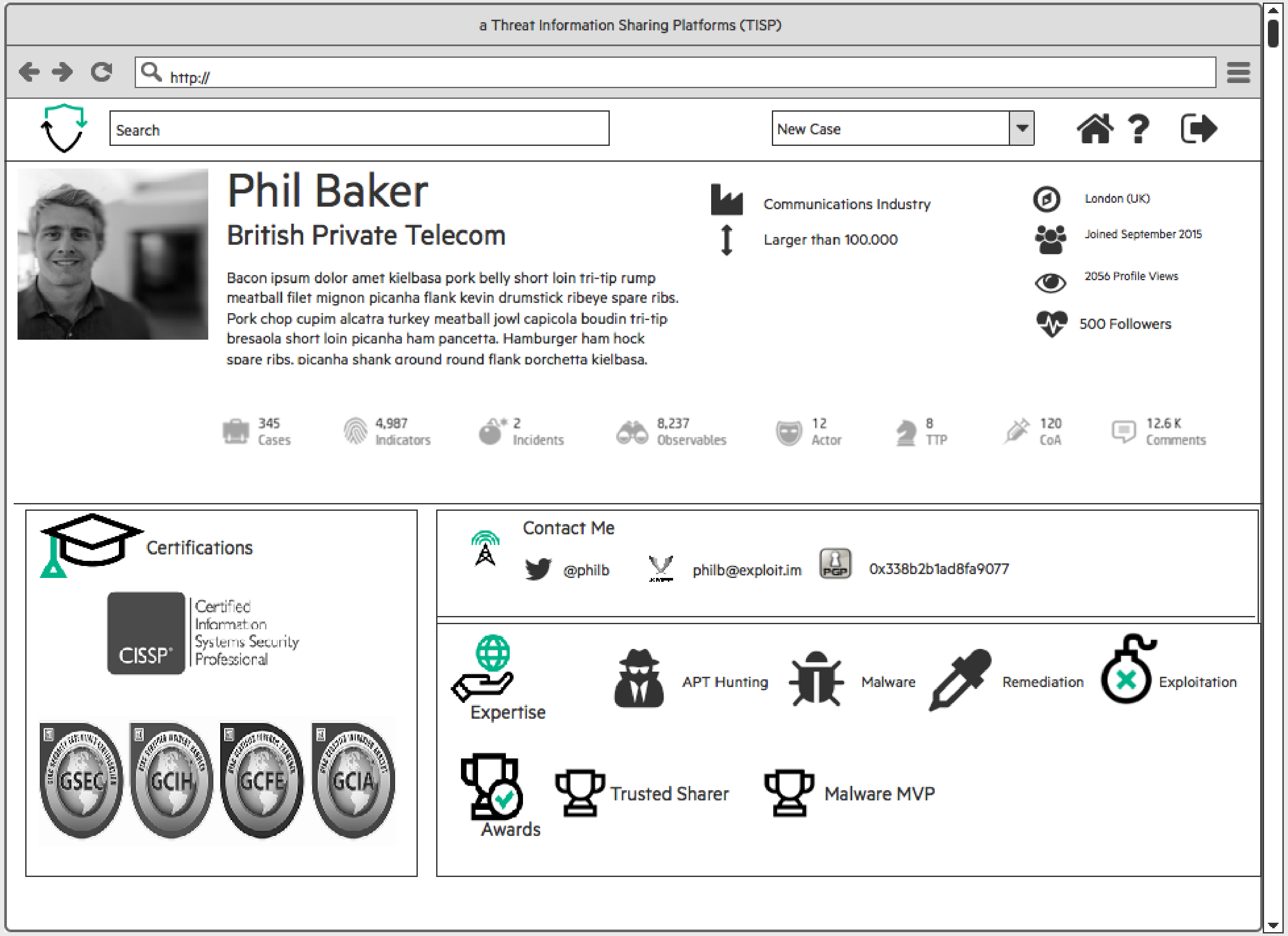
– What helps to add to the trustworthiness for received information

– 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



a Threat Information Sharing Platforms (TISP)

http://

Search

New Case

Phil Baker

British Private Telecom

Bacon ipsum dolor amet kielbasa pork belly short loin tri-tip rump meatball filet mignon picanha flank kevin drumstick ribeye spare ribs. Pork chop cupim alcatra turkey meatball jowl capicola boudin tri-tip bresaola short loin picanha ham pancetta. Hamburger ham hock spare ribs. picanha shank ground round flank porchetta kielbasa.

Communications Industry

Larger than 100.000

London (UK)

Joined September 2015

2056 Profile Views

500 Followers

345 Cases

4,987 Indicators

2 Incidents

8,237 Observables

12 Actor

8 TTP

120 CoA

12.6 K Comments

Certifications

CISSP® Certified Information Systems Security Professional

GSEC GCIH GCFE GCIA

Contact Me

@philb

philb@exploit.im

0x338b2b1ad8fa9077

Expertise

APT Hunting

Malware

Remediation

Exploitation

Awards

Trusted Sharer

Malware MVP

Findings: Privacy

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

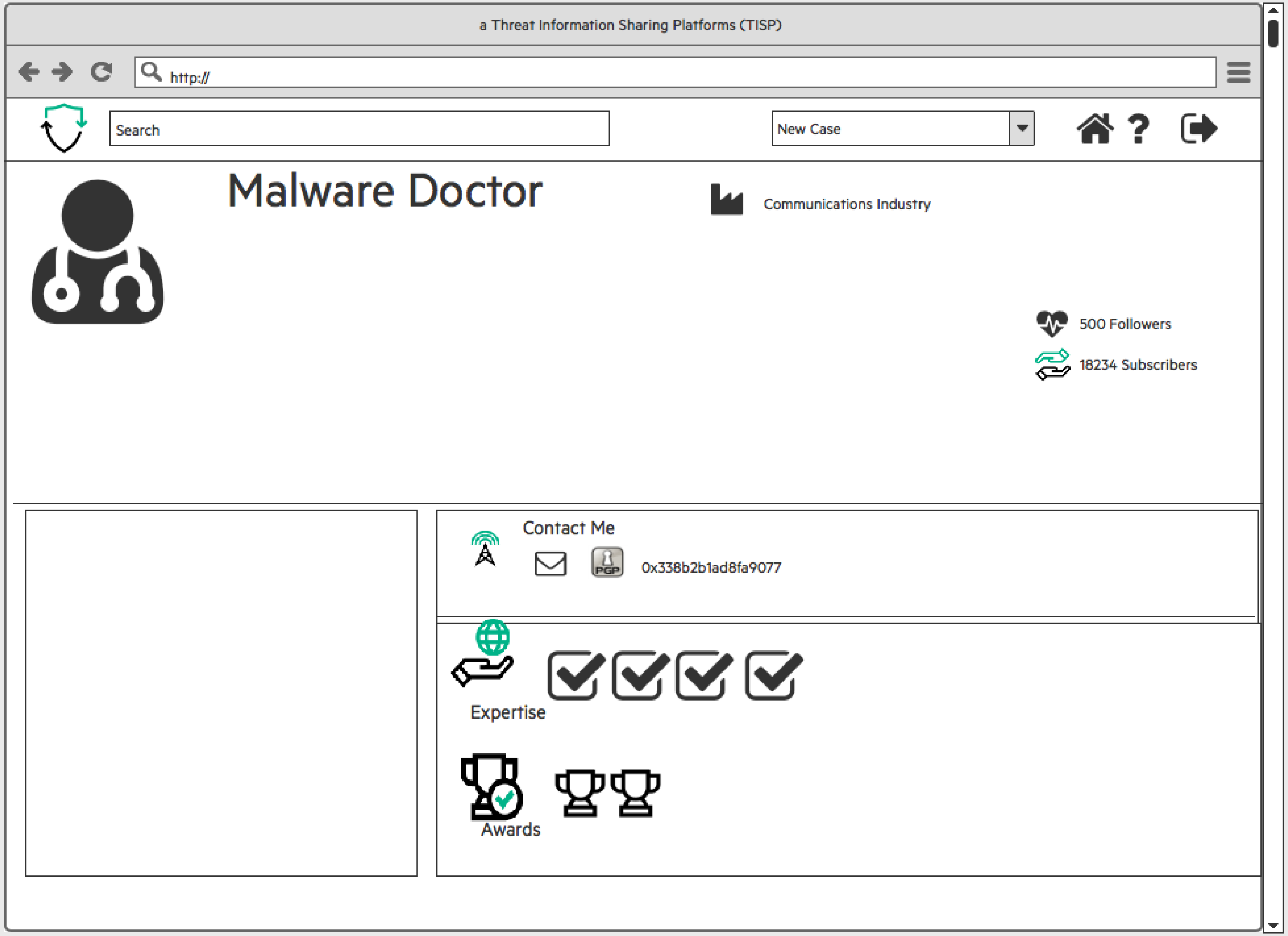
– Concerns about social engineering, job poaching.

– 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



a Threat Information Sharing Platforms (TISP)

Malware Doctor

Communications Industry

500 Followers

18234 Subscribers

Contact Me

0x338b2b1ad8fa9077

Expertise

Awards

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