What’s in a Cyber Threat Intelligence sharing platform?
A mixed-methods user experience investigation of MISP

Borče Stojkovski  
SnT, University of Luxembourg  
borce.stojkovski@uni.lu

Gabriele Lenzini  
SnT, University of Luxembourg  
gabriele.lenzini@uni.lu

Vincent Koenig  
COSA, University of Luxembourg  
vincent.koenig@uni.lu

Salvador Rivas  
COSA, University of Luxembourg  
salvador.rivas@uni.lu

Authors are supported by the Luxembourg National Research Fund through grant PRIDE15/10621687/SPsquared
Outline

1. Introduction and Research Context
2. Use case (MISP) and User Study
3. Results and Analysis
4. Discussion and Future work
Introduction & Research Context
Growing number and sophistication of cyber attacks

Axia’s Asian operations hit in ransomware attack
French insurer’s units in Thailand, Malaysia, Hong Kong and Philippines affected

INTERNATIONAL ORGANISED CRIME THREAT ASSESSMENT 2021

In this year’s report, the impact of the COVID-19 pandemic remains visible. Cybercriminals have continued exploiting opportunities created by lockdowns and continued teleworking. Ransomware affiliate programs have increased in prominence and are tied to a multitude of high-profile attacks against healthcare institutions and services providers.

Ransomware highlights the challenges and subtleties of cybersecurity

Goverments want to defend themselves—and attack others
Growing number and sophistication of cyber attacks

Australia’s cybersecurity agency says it averted more attacks by hackers who crippled Nine

Australian Signals Directorate boss Rachel Noble says helping Nine allowed it to alert two other organisations they were targets for cyber-attacks

WORLD’S MOST DANGEROUS MALWARE EMOTET DISRUPTED THROUGH GLOBAL ACTION
27 Jan 2021

Incentives and Barriers to Information Sharing
Given the acknowledged importance of information sharing, this report sets out findings from a research project into the barriers to and incentives for information sharing in the field of network and information security, in the context of peer-to-peer groups such as Information Exchanges (IEs) and Information Sharing Analysis Centres (ISACs).

Published: September 06, 2010
Author: ENISA, RAND Europe
Language: English

Executive Order on Improving the Nation’s Cybersecurity
MAY 12, 2021 + PRESIDENTIAL ACTIONS

Sec. 2. Removing Barriers to Sharing Threat Information.
(a) The Federal Government contracts with IT and OT service providers to conduct an array of day-to-day functions on Federal Information Systems. These service providers, including cloud service providers, have unique access to and insight into cyber threat and incident information on Federal Information Systems. At the same time, current contract terms or restrictions may limit the sharing of such threat or incident information with executive departments and agencies (agencies) that are responsible for investigating or remediating cyber incidents, such as the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and other elements of the Intelligence
Cyber Threat Intelligence Sharing

• Countermeasure to the growing number and sophistication of attacks in different cyber security scenarios.
  ▶ financially-driven cyber criminal activities, cyberwar, hacktivism, terrorism, etc.
Cyber Threat Intelligence Sharing

• Countermeasure to the growing number and sophistication of attacks in different cyber security scenarios.
  ▶ financially-driven cyber criminal activities, cyberwar, hacktivism, terrorism, etc.

• However, complicated by a number of technical, organizational, legal, economical, and social barriers and challenges
  ▶ Emergence of Standards for formatting CTI information and Sharing Platforms
CTI Standards and Sharing Platforms

- STIX
- TAXII
- OTX
- IODEF
- CyBOX
- OpenTPX
- RID
- VERIS
- etc.

- Anomali
- STAXX
- CRITs
- MISP
- EclecticIQ
- OpenCTI
- Threat
- Connect
- IBM X-
- Force
- etc.
Human, cultural & organizational aspects

- Nature of the job, organizational setting, tools and workflows of IT security professionals
- Collaborative work practices in the CTI (sharing) context
- Motivation
- Skills development
- Usability and User Experience (UX)
Motivation for our work

- **Importance of UX**: empirical evidence on the usability, or perceived UX of CTI sharing platforms is scarce to non-existent.

- **Knowledge gap** regarding users’ perceptions of key tasks
  - enabling and constraining factors of security information sharing
  - how much effective CTI sharing is impacted by usability problems or UX
Contribution

• Empirical
  ▶ First UX benchmark for a leading CTI sharing platform
  ▶ Key findings and UX recommendations of relevance to CTI sharing platforms in general
  ▶ Possible negative outcomes in terms of security and adoption related to UX

• Methodological
  ▶ Demonstration of the utility and necessity of UX research methods in cybersecurity
Use case (MISP) & User study
MISP

- A leading open-source CTI sharing platform
  - Inception within military circles 15 years ago
  - Used by over 6,000 organizations worldwide
  - UI and API users
  - Characterized as holistic and applicable in diverse scenarios (De Melo e Silva et al., 2020)

- More info: https://www.misp-project.org
Research Questions

• How do different security information workers evaluate the UX of MISP?
• What do users value about MISP and what do they think could be improved?
• Which user needs are addressed and accounted for by MISP, and which are neglected?
Methodology

Study | Survey components
--- | ---
1 #TR | N=24 Info, UEQ, Demographics
2 #GF | N=10 Info, UEQ, Demographics
3 #BM | N=8 Info, UEQ, Demographics
4 #LT | N=32 Info, UEQ, Demographics

N=10 SC

N=32 SC

Total N1=74

Total N2=42
Methodology

User Experience Questionnaire

Please complete the sentences below. There are no wrong replies, respond rather quickly without thinking too long. You can leave a sentence without an answer if you feel that it is not suitable for your situation.

When I use MISP, I feel …

____________________________________________________________________

MISP is best for …

____________________________________________________________________

MISP is not suitable for …

____________________________________________________________________

I think the appearance of MISP is …

____________________________________________________________________

I am happy with MISP because …

____________________________________________________________________

The problem with MISP is …

____________________________________________________________________

People who use MISP are typically …

____________________________________________________________________

Compared to other threat information sharing platforms, MISP is …

____________________________________________________________________

MISP Users - Questionnaire

The purpose of this questionnaire is to better understand the types of users and their respective needs on the MISP platform. Participation is voluntary.

1. Which of the following roles best describes how you (intend to) use MISP?
   - ☐ Malware reverser: e.g. willing to share indicators of analysis with respective colleagues
   - ☐ Security analyst: e.g. searching, validating and using indicators in operational security
   - ☐ Intelligence analyst: e.g. gathering information about specific adversary groups
   - ☐ Fraud analyst: e.g. willing to share financial indicators to detect financial frauds
   - ☐ Risk analyst: e.g. willing to know about the new threats, likelihood and occurrences
   - ☐ Law enforcer: e.g. relying on indicators to support or bootstrap DFIR cases
   - ☐ Academic researcher
   - ☐ Other: __________________________________________________

2. Which of the following categories best describes the organization you work in?
   - ☐ National or Governmental CSIRT
   - ☐ Military
   - ☐ Energy
   - ☐ Law enforcement agency
   - ☐ Banking and Finance
   - ☐ Insurance
   - ☐ Computer hardware manufacturer
   - ☐ Software company
   - ☐ ICT Consulting / Advisory
   - ☐ Public Health
   - ☐ Telecommunications
   - ☐ Transportation
   - ☐ Academic institution
   - ☐ Other: ______________________________

3. How long have you been using MISP?
   - ○ I have never used MISP before
   - ○ < 1 month
   - ○ 1 - 6 months
   - ○ 6 - 12 months
   - ○ 1 - 2 years
   - ○ > 2 years

4. If applicable, how often do you use MISP?
   - ○ Less than once a week
   - ○ Between once and three times a week
   - ○ Between three times a week & every day
   - ○ Every day

5. Have you attended a training session on MISP before?
   - ○ No
   - ○ Yes

6. Have you used the MISP training materials before?
   - ○ No
   - ○ Yes

7. Have you used the MISP virtual machine before?
   - ○ No
   - ○ Yes

8. Have you used PyMISP - the Python library to access MISP via the API before?
   - ○ No
   - ○ Yes

Sentence Completion

When I use MISP, I feel …

____________________________________________________________________

MISP is best for …

____________________________________________________________________

I think the appearance of MISP is …

____________________________________________________________________

I am happy with MISP because …

____________________________________________________________________

The problem with MISP is …

____________________________________________________________________

People who use MISP are typically …

____________________________________________________________________

Compared to other threat information sharing platforms, MISP is …

____________________________________________________________________
Methodology - User Experience Questionnaire

For the assessment of the MISP platform, please fill out the following questionnaire, which consists of pairs of contrasting attributes that may apply to the platform. You can express your agreement with the attributes by ticking the circle that most closely reflects your impression.

Example:
This response would mean that you rate the application as more attractive than unattractive.

Please decide spontaneously. Don’t think too long about your decision to make sure that you convey your original impression. Sometimes you may not be completely sure about your agreement with a particular attribute or you may find that the attribute does not apply completely to the platform. Nevertheless, please tick a circle in every line. It is your personal opinion that counts. Please remember: there is no wrong or right answer!

Source: User Experience Questionnaire Handbook (Version 8)
Methodology - Sentence Completion

When I use MISP, I feel …

MISP is best for …

MISP is not suitable for …

I think the appearance of MISP is …

I am happy with MISP because …

The problem with MISP is …

People who use MISP are typically …

Compared to other threat information sharing platforms, MISP is …

Adapted from: Kujala et al. (2014)
Results and Analysis
Participants

Gender

- Male: 70
- Female: 2
- Not specified: 2

N=74
Participants

Engineering / Tech Background

No 8
Yes 66

N=74
Participants

Education

N=73

- Less than a Bachelor's degree: 10
- Bachelor's degree: 32
- Master's degree: 28
- Doctoral degree: 3
Participants

Age Group

- 18 - 25 years: 11 participants
- 26 - 35 years: 32 participants
- 36 - 45 years: 27 participants
- 46 - 55 years: 4 participants

N=74
Participants

Role (multiple possible)

N=74
Participants

Industry (multiple possible)

N=74
Participants

Prior experience with MISP

- I have never used MISP before: 18
- Less than 1 month: 11
- 1-6 months: 18
- 6-12 months: 10
- 1-2 years: 6
- More than 2 years: 11

N=74
Participants

MISP usage frequency

- Less than once a week: 11
- Between 1 and 3 times per week: 19
- Between 3 times per week & every day: 18
- Every day: 10

N=52
Participants

Previously attended a MISP training

N=74
Participants

Previously used MISP training materials

N=74
Participants

Previously used MISP virtual machines

N=74
UEQ Results

N=64
### UEQ Results

<table>
<thead>
<tr>
<th>Rating</th>
<th>Unhappy</th>
<th>Neutral</th>
<th>Happy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annoying/Enjoyable</td>
<td>0.4</td>
<td>1.1</td>
<td>1.6</td>
</tr>
<tr>
<td>Not Understandable/Understandable</td>
<td>0.8</td>
<td>1.4</td>
<td>2.3</td>
</tr>
<tr>
<td>Dull/Creative</td>
<td>0.8</td>
<td>1.1</td>
<td>2.2</td>
</tr>
<tr>
<td>Difficult to learn/Easy to learn</td>
<td>1.2</td>
<td>1.2</td>
<td>1.8</td>
</tr>
<tr>
<td>Inferior/Valuable</td>
<td>1.2</td>
<td>1.4</td>
<td>2.4</td>
</tr>
<tr>
<td>Boring/Exciting</td>
<td>1.1</td>
<td>1.5</td>
<td>2.4</td>
</tr>
<tr>
<td>Not Interesting/Interesting</td>
<td>1.1</td>
<td>1.5</td>
<td>2.4</td>
</tr>
<tr>
<td>Unpredictable/Predictable</td>
<td>1.1</td>
<td>1.5</td>
<td>2.4</td>
</tr>
<tr>
<td>Slow/Fast</td>
<td>1.1</td>
<td>1.5</td>
<td>2.4</td>
</tr>
<tr>
<td>Conventional/Inventive</td>
<td>1.1</td>
<td>1.5</td>
<td>2.4</td>
</tr>
<tr>
<td>Obstructive/Supportive</td>
<td>1.1</td>
<td>1.5</td>
<td>2.4</td>
</tr>
<tr>
<td>Bad/Good</td>
<td>1.1</td>
<td>1.5</td>
<td>2.4</td>
</tr>
<tr>
<td>Complicated/Easy</td>
<td>1.1</td>
<td>1.5</td>
<td>2.4</td>
</tr>
<tr>
<td>Unlikely/pleasing</td>
<td>1.1</td>
<td>1.5</td>
<td>2.4</td>
</tr>
<tr>
<td>Usual/Leading edge</td>
<td>1.1</td>
<td>1.5</td>
<td>2.4</td>
</tr>
<tr>
<td>Unpleasant/Pleasant</td>
<td>1.1</td>
<td>1.5</td>
<td>2.4</td>
</tr>
<tr>
<td>Not secure/Secure</td>
<td>1.1</td>
<td>1.5</td>
<td>2.4</td>
</tr>
<tr>
<td>Demotivating/Motivating</td>
<td>1.1</td>
<td>1.5</td>
<td>2.4</td>
</tr>
<tr>
<td>Does not meet expectations/Meets expectations</td>
<td>1.1</td>
<td>1.5</td>
<td>2.4</td>
</tr>
<tr>
<td>Inefficient/efficient</td>
<td>1.1</td>
<td>1.5</td>
<td>2.4</td>
</tr>
<tr>
<td>Confusing/Clear</td>
<td>1.1</td>
<td>1.5</td>
<td>2.4</td>
</tr>
<tr>
<td>Impractical/Practical</td>
<td>1.1</td>
<td>1.5</td>
<td>2.4</td>
</tr>
<tr>
<td>Cluttered/organized</td>
<td>1.1</td>
<td>1.5</td>
<td>2.4</td>
</tr>
<tr>
<td>Unattractive/Attractive</td>
<td>1.1</td>
<td>1.5</td>
<td>2.4</td>
</tr>
<tr>
<td>Unfriendly/Friendly</td>
<td>1.1</td>
<td>1.5</td>
<td>2.4</td>
</tr>
<tr>
<td>Conservative/Innovative</td>
<td>1.1</td>
<td>1.5</td>
<td>2.4</td>
</tr>
</tbody>
</table>

**N=64**
# UEQ Results

### N=64

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>annoying/enjoyable</td>
<td>1.6</td>
</tr>
<tr>
<td>not understandable/understandable</td>
<td>1.1</td>
</tr>
<tr>
<td>dull/creative</td>
<td>1.3</td>
</tr>
<tr>
<td>difficult to learn/easy to learn</td>
<td>0.4</td>
</tr>
<tr>
<td>inferior/valuable</td>
<td>2.3</td>
</tr>
<tr>
<td>boring/exciting</td>
<td>1.4</td>
</tr>
<tr>
<td>not interesting/interesting</td>
<td>1.4</td>
</tr>
<tr>
<td>unpredictable/predictable</td>
<td>1.1</td>
</tr>
<tr>
<td>slow/fast</td>
<td>1.1</td>
</tr>
<tr>
<td>conventional/inventive</td>
<td>1.2</td>
</tr>
<tr>
<td>obstructive/supportive</td>
<td>1.8</td>
</tr>
<tr>
<td>bad/good</td>
<td>2.4</td>
</tr>
<tr>
<td>annoying/enjoyable</td>
<td>1.6</td>
</tr>
<tr>
<td>not understandable/understandable</td>
<td>1.1</td>
</tr>
<tr>
<td>dull/creative</td>
<td>1.3</td>
</tr>
<tr>
<td>difficult to learn/easy to learn</td>
<td>0.4</td>
</tr>
<tr>
<td>inferior/valuable</td>
<td>2.3</td>
</tr>
<tr>
<td>boring/exciting</td>
<td>1.4</td>
</tr>
<tr>
<td>not interesting/interesting</td>
<td>1.4</td>
</tr>
<tr>
<td>unpredictable/predictable</td>
<td>1.1</td>
</tr>
<tr>
<td>slow/fast</td>
<td>1.1</td>
</tr>
<tr>
<td>conventional/inventive</td>
<td>1.2</td>
</tr>
<tr>
<td>obstructive/supportive</td>
<td>1.8</td>
</tr>
<tr>
<td>bad/good</td>
<td>2.4</td>
</tr>
</tbody>
</table>

### Dimensions

- **Attractiveness**
  - Mean: 1.62
- **Pragmatic Quality**
  - Mean: 1.42
- **Dependability**
  - Mean: 1.52
- **Stimulation**
  - Mean: 1.89
- **Novelty**
  - Mean: 1.26
# UEQ Results

<table>
<thead>
<tr>
<th>Scale</th>
<th>Evaluation</th>
<th>Mean</th>
<th>Std Dev.</th>
<th>MoE</th>
<th>5% CI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attractiveness</td>
<td>Positive</td>
<td>1.62</td>
<td>0.83</td>
<td>0.203</td>
<td>[1.41, 1.82]</td>
</tr>
<tr>
<td>Perspicuity</td>
<td>Neutral</td>
<td>0.51</td>
<td>1.18</td>
<td>0.288</td>
<td>[0.21, 0.79]</td>
</tr>
<tr>
<td>Efficiency</td>
<td>Positive</td>
<td>1.40</td>
<td>0.82</td>
<td>0.201</td>
<td>[1.20, 1.60]</td>
</tr>
<tr>
<td>Dependability</td>
<td>Positive</td>
<td>1.52</td>
<td>0.56</td>
<td>0.138</td>
<td>[1.39, 1.66]</td>
</tr>
<tr>
<td>Stimulation</td>
<td>Positive</td>
<td>1.89</td>
<td>0.88</td>
<td>0.167</td>
<td>[1.72, 2.05]</td>
</tr>
<tr>
<td>Novelty</td>
<td>Positive</td>
<td>1.36</td>
<td>0.78</td>
<td>1.191</td>
<td>[1.17, 1.55]</td>
</tr>
</tbody>
</table>

N=64
# UEQ Results

Comparison of the MISP results to a general UEQ benchmark  
(452 product evaluations)

<table>
<thead>
<tr>
<th>Scale</th>
<th>Mean</th>
<th>Comparison</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attractiveness</td>
<td>1.62</td>
<td>Good</td>
<td>10% of results better, 75% of results worse</td>
</tr>
<tr>
<td>Perspicuity</td>
<td>0.51</td>
<td>Bad</td>
<td>In the range of the 25% worst results</td>
</tr>
<tr>
<td>Efficiency</td>
<td>1.40</td>
<td>Above average</td>
<td>25% of results better, 50% of results worse</td>
</tr>
<tr>
<td>Dependability</td>
<td>1.52</td>
<td>Good</td>
<td>10% of results better, 75% of results worse</td>
</tr>
<tr>
<td>Stimulation</td>
<td>1.89</td>
<td>Excellent</td>
<td>In the range of the 10% best results</td>
</tr>
<tr>
<td>Novelty</td>
<td>1.36</td>
<td>Good</td>
<td>10% of results better, 75% of results worse</td>
</tr>
</tbody>
</table>

![Comparison of the MISP results to a general UEQ benchmark](image-url)
UEQ Results

Comparison of the MISP results to a UEQ benchmark of websites and web services
(85 product evaluations)

<table>
<thead>
<tr>
<th>Scale</th>
<th>Mean</th>
<th>Comparison</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attractiveness</td>
<td>1.62</td>
<td>Good</td>
<td>10% of results better, 75% of results worse</td>
</tr>
<tr>
<td>Perspicuity</td>
<td>0.51</td>
<td>Bad</td>
<td>In the range of the 25% worst results</td>
</tr>
<tr>
<td>Efficiency</td>
<td>1.40</td>
<td>Above average</td>
<td>25% of results better, 50% of results worse</td>
</tr>
<tr>
<td>Dependability</td>
<td>1.52</td>
<td>Above average</td>
<td>25% of results better, 50% of results worse</td>
</tr>
<tr>
<td>Stimulation</td>
<td>1.89</td>
<td>Excellent</td>
<td>In the range of the 10% best results</td>
</tr>
<tr>
<td>Novelty</td>
<td>1.36</td>
<td>Excellent</td>
<td>In the range of the 10% best results</td>
</tr>
</tbody>
</table>
## SC Results

### Overview of Sentence completion stems and corresponding response rates

<table>
<thead>
<tr>
<th>Sentence stems</th>
<th>Responses</th>
<th>No answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1: When I use MISP, I feel ...</td>
<td>29 (69%)</td>
<td>13 (31%)</td>
</tr>
<tr>
<td>S2: MISP is best for ...</td>
<td>29 (69%)</td>
<td>13 (31%)</td>
</tr>
<tr>
<td>S3: MISP is not suitable for ...</td>
<td>19 (45%)</td>
<td>23 (55%)</td>
</tr>
<tr>
<td>S4: I think the appearance of MISP is ...</td>
<td>31 (74%)</td>
<td>11 (26%)</td>
</tr>
<tr>
<td>S5: I am happy with MISP because ...</td>
<td>32 (76%)</td>
<td>10 (24%)</td>
</tr>
<tr>
<td>S6: The problem with MISP is ...</td>
<td>27 (64%)</td>
<td>15 (36%)</td>
</tr>
<tr>
<td>S7: People who use MISP are typically ...</td>
<td>20 (48%)</td>
<td>22 (52%)</td>
</tr>
<tr>
<td>S8: Compared to other threat information sharing platforms, MISP is ...</td>
<td>24 (57%)</td>
<td>18 (43%)</td>
</tr>
<tr>
<td><strong>Total:</strong></td>
<td><strong>211 (63%)</strong></td>
<td><strong>125 (37%)</strong></td>
</tr>
</tbody>
</table>
# SC Results

## Overview of most frequent themes (1/2)

<table>
<thead>
<tr>
<th>Themes</th>
<th>Theme frequency per sentence stem</th>
<th>S1</th>
<th>S2</th>
<th>S3</th>
<th>S4</th>
<th>S5</th>
<th>S6</th>
<th>S7</th>
<th>S8</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User-related aspects</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Needs and values</td>
<td></td>
<td>9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>11</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>32</td>
</tr>
<tr>
<td>Emotion evocation</td>
<td></td>
<td>34</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>44</td>
</tr>
<tr>
<td>- Positive emotions</td>
<td></td>
<td>22</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>26</td>
</tr>
<tr>
<td>- Negative emotions</td>
<td></td>
<td>12</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>18</td>
</tr>
<tr>
<td><strong>User characteristics</strong></td>
<td></td>
<td>0</td>
<td>1</td>
<td>7</td>
<td>1</td>
<td>0</td>
<td>6</td>
<td>13</td>
<td>0</td>
<td>28</td>
</tr>
</tbody>
</table>
## SC Results

### Overview of most frequent themes (2/2)

<table>
<thead>
<tr>
<th>Themes</th>
<th>Theme frequency per sentence stem</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>S1</td>
</tr>
<tr>
<td>System-related aspects</td>
<td></td>
</tr>
<tr>
<td>MISP characteristics</td>
<td>1</td>
</tr>
<tr>
<td>UX qualities</td>
<td>16</td>
</tr>
<tr>
<td>- Attractiveness</td>
<td>0</td>
</tr>
<tr>
<td>- Lack of attractiveness</td>
<td>0</td>
</tr>
<tr>
<td>- Pragmatic qualities</td>
<td>3</td>
</tr>
<tr>
<td>- Lack of pragmatic qualities</td>
<td>10</td>
</tr>
<tr>
<td>- Hedonic qualities</td>
<td>3</td>
</tr>
<tr>
<td>- Lack of hedonic qualities</td>
<td>0</td>
</tr>
</tbody>
</table>
User-related aspects

Needs and values: competence, control, autonomy, relatedness/belongingness

S1 “When I use MISP, I feel confident about my ability to find bad guys” (BM11)

S5 “I am happy with MISP because its flexibility allows me to solve my problems and I do not have to change my way of working” (BM18)

S1 “When I use MISP, I feel I’m part of a community” (LT19)

S5 “I am happy with MISP because I’m a part of a community, I can help people like me” (BM9)
User-related aspects

Evocation of positive emotions: satisfaction, confidence, pride, courage

S1 “When I use MISP, I feel like a genius” (LT16)

S2 “MISP is best for people who aren’t afraid of digging through Github issues as a supplement [sic] to the documentation” (BM14)
User-related aspects

Evocation of negative emotions: confusion, boredom, frustration

S1 “When I use MISP, I feel overwhelmed with the amount and type of data” (BM12)

S6 “The problem with MISP is its integration, that is confusing for me” (LT27)

S1 “When I use MISP, I feel a bit lost, need to search a lot to find what I need” (BM7)
User-related aspects

Profile and characteristics of MISP users

S7 “People who use MISP are typically experts on security”  (LT11)

S3 “MISP is not suitable for non techies”  (BM11)

S3 “MISP is not suitable for quick ad-hoc analysis by non IT professionals”  (LT25)

S6 “The problem with MISP is a lack of a public community that new users can join when starting out”  (LT3)
System-related aspects

MISP characteristics: freeness, openness, adaptation

S5 “I am happy with MISP because it has potential to integrate with other tools and is open-source” (LT16)

S8 “Compared to other threat intelligence sharing platforms, MISP is free, open-source and not managed by big companies” (BM20)

S5 “I am happy with MISP because it just works 95% of the time and it’s enormously flexible as a tool” (BM14)

S5 “I am happy with MISP because it can be used in different ways” (LT31)
System-related aspects

UX qualities: Attractiveness and lack thereof

S4 “I think the appearance of MISP is quite pleasing”  
(BM7)

S4 “I think the appearance of MISP is very good”  
(LT27)

S4 “I think the appearance of MISP [is] has room for improvement”  
(BM18)

S6 “The problem with MISP is [its] look and feel”  
(LT19)
System-related aspects

UX qualities: Pragmatic aspects

S8 “Compared to other threat intelligence sharing platforms, MISP is well-maintained and good feature set”  

S2 “MISP is best for identifying events, their sources, and their attributes”  

S2 “… best for documenting malware and incidents and sharing that information”  

S2 “… best for having a centralized place to store and collaborate on data”
System-related aspects

UX qualities: Pragmatic issues

S6 “The problem with MISP is it is too IOC-centered / IOC-oriented” (BM2)

S3 “MISP is not suitable for long term analysis or assessment” (LT13)

S4 “I think the appearance of MISP is chaotic at times” (BM6)

S6 “The problem with MISP is finding the balance between good enough information and time invested” (LT12)
System-related aspects

UX qualities: Pragmatic issues

S6 “The problem with MISP is that it is huge and kind of hard to start with”

S6 “The problem with MISP is it has a steep learning curve”

S4 “I think the appearance of MISP needs to be explained to be more used”

S6 “The problem with MISP is it is hard to get started adding events if you never saw an example”
System-related aspects

UX qualities: Hedonic aspects

S4 “I think the appearance of MISP is good, but a little old fashioned” (BM9)

S8 “Compared to other threat intelligence sharing platforms, MISP is a breath of fresh air” (BM14)

S4 “I am happy with MISP because it is an awesome tool” (LT27)
Discussion and Future Work
Summary of key findings

• Overall positive UX evaluation across the three main system quality aspects: attractiveness, pragmatic and hedonic qualities
  ▸ Lower pragmatic evaluation due to low perspicuity score

• Complex relationship users have with MISP:
  ▸ useful, valuable, and empowering, but also overwhelming
  ▸ flexibility, adaptation, openness, community
Implications

• Highlighted concerns open potential problems in terms of errors and under-utilization
  ▪ people have nuanced behavior with respect to how, with whom, when, and why they share sensitive information

• Sharing without knowing who the (intended) recipients are, can lead to:
  ▪ **oversharing** i.e. leakage of sensitive information to parties beyond those intended
  ▪ **undersharing** i.e. lower cyber preparedness levels of the sharing community
  ▪ both impact the future use and adoption, where no adoption means lower security
Beyond usability

- Why start/continue using a CTI platform even though it is hard to learn?
  - Narrow usability-focused studies focus on task-related efficiency and effectiveness, but omit other equally important aspects.
UEQ Results

versus
Beyond usability

• **Why start/continue using a CTI platform even though it is hard to learn?**
  
  ▪ Narrow usability-focused studies focus on task-related efficiency and effectiveness, but omit other equally important aspects.

• Affective reactions before, during, or after use, emotional relationships people build with products, fulfillment of psychological needs
  
  ▪ Psychological need of **relatedness / belongingness** can play a key role here

• Importance of approaching UX in a holistic manner
Limitations

• Difficulties recruiting and getting access to larger numbers of participants
  ▶ Sample skewed towards novice users, mostly male, with a tech background
  ▶ Study period of two years, not exactly the same version of MISP, however, no radical
    changes introduced w.r.t. activities covered during MISP training sessions

• Limitations of deployed methods, as every context is specific and the methods are not a
  perfect fit for every situation
Future Work

• Further validation of obtained results and assumptions e.g. impact of expertise and experience with the platform on the evaluation

• More research on UX aspects and how UX design can help
  ▸ Do users have a correct understanding of how far CTI information travels when shared?
  ▸ How are users supported in core activities (e.g. UI mechanisms, docs, training)?
  ▸ How does end-user feedback loop back to the designers and developers and whose responsibility is the UX in open-source, community-driven projects like MISP?
Conclusion

• CTI exchange is a crucial element in the fight against increasing cyber attacks and threats

• Through the use case of MISP, we have highlighted what novice users perceive to be the strengths and weaknesses of a leading CTI sharing platform
  ▪ Specified appropriate metrics and performed a benchmark UX evaluation

• We demonstrated that many user and system-related needs can remain hidden unless we take an expanded notion of the UX and go beyond narrow usability studies
Thank you for your attention! Any questions?