What's in a Cyber Threat Intelligence sharing platform?

A mixed-methods user experience investigation of MISP

Borce Stojkovski
SnT, University of Luxembourg
Esch-sur-Alzette, Luxembourg
borce.stojkovski@uni.lu

Gabriele Lenzini
SnT, University of Luxembourg
Esch-sur-Alzette, Luxembourg
gabriele.lenzini@uni.lu

Vincent Koenig
COSA, University of Luxembourg
Esch-sur-Alzette, Luxembourg
vincent.koenig@uni.lu

Salvador Rivas
COSA, University of Luxembourg
Esch-sur-Alzette, Luxembourg
salvador.rivas@uni.lu

ABSTRACT

The ever-increasing scale and complexity of cyber attacks and cyber-criminal activities necessitate secure and effective sharing of cyber threat intelligence (CTI) among a diverse set of stakeholders and communities. CTI sharing platforms are becoming indispensable tools for cooperative and collaborative cybersecurity. Nevertheless, despite the growing research in this area, the emphasis is often placed on the technical aspects, incentives, or implications associated with CTI sharing, as opposed to investigating challenges encountered by users of such platforms. To date, user experience (UX) aspects remain largely unexplored.

This paper offers a unique contribution towards understanding the constraining and enabling factors of security information sharing within one of the leading platforms. MISP is an open source CTI sharing platform used by more than 6,000 organizations worldwide. As a technically-advanced CTI sharing platform it aims to cater for a diverse set of security information workers with distinct needs and objectives. In this respect, MISP has to pay an equal amount of attention to the UX in order to maximize and optimize the quantity and quality of threat information that is contributed and consumed.

Using mixed methods we shed light on the strengths and weaknesses of MISP from an end-users' perspective and discuss the role UX could play in effective CTI sharing. We conclude with an outline of future work and open challenges worth further exploring in this nascent, yet highly important socio-technical context.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**; • **Human-centered computing → User studies**.

ACSAC '21, December 6–10, 2021, Virtual Event, USA

ACM ISBN 978-1-4503-8579-4/21/12.
https://doi.org/10.1145/3485832.3488030

KEYWORDS

user studies, user experience, usability, cyber threat intelligence, information sharing, sharing platforms

ACM Reference Format:
Borce Stojkovski, Gabriele Lenzini, Vincent Koenig, and Salvador Rivas. 2021. What's in a Cyber Threat Intelligence sharing platform?: A mixed-methods user experience investigation of MISP. In *Annual Computer Security Applications Conference (ACSAC '21), December 6–10, 2021, Virtual Event, USA.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3485832.3488030

1 INTRODUCTION

Even before the onset of COVID-19, the scale and sophistication of malicious cyber activities by various threat actors highlighted the distressing risks posed to our increasingly digitized and interconnected societies. The pandemic only further demonstrated how cyber criminals and other actors have adapted their practices to fit the COVID-19 narrative and exploit the crisis [25]. The Colonial Pipeline [15] and SolarWinds [14] cyber attacks further illustrate the palpable disruption to business continuity of critical infrastructure and potential threats to national and global cybersecurity.

The consequences of cyber attacks are manifold, with attacked organizations often experiencing not only different kinds of out-of-pocket costs, such as investigation and remediation expenses, legal and regulatory fines, etc., but also reputation costs which can economically be much larger [38]. Furthermore, there are spillover effects where industry competitors of attacked organizations do not benefit from such cyber attacks, but in turn also experience shareholder wealth losses [38]. Thus, in order to mitigate the likelihood or impact of future incidents, organizations tend to engage in cooperative relationships with other third parties [39].

The timely and efficient gathering, analysis and, in particular, exchange of cyber threat intelligence (CTI) is therefore seen as a promising approach to countering these new generation threats. Parties that belong to a CTI sharing community can leverage the collective knowledge, experience, and capabilities to create an extensive situational awareness picture of the threats their organization may face [37]. It has been shown that CTI sharing can be effective in the mitigation of ongoing and the prevention of potential attacks, in the faster identification and detection of threats, threat

actors, and their tactics, techniques and procedures (TTPs) [71]. Furthermore, CTI sharing can be a cost-effective tool and reduce the likelihood of cascading effects across entire systems, sectors or industries [71]. Thus, there is a wide consensus on the benefits of CTI sharing in different contexts, such as financially-driven cyber criminal activities, cyberwar, hacktivism and terrorism [65].

That being said, effective CTI sharing depends on a number of dimensions and is complicated by obstacles and challenges that entail technical, organizational, legal, economical, and social aspects [21, 23, 28, 80]. These include efficient cooperation and coordination, legal and regulatory compliance, standardization, regional and international implementation, and technology integration [65]. The acknowledgement of the multi-faceted complexity of CTI exchange, motivates for a multi-disciplinary and multi-stakeholder discourse as well as mobilization of diverse expertise in the collective pursuit of defending our societies from malicious cyber activities.

In recent years there has been significant progress in terms of overcoming technical hurdles in establishing the formats and platforms for CTI exchange. Further, some attention has been devoted to uncovering and addressing challenges around organizational modalities, incentives, and implications associated with CTI sharing. For instance, in light of the persistent and increasingly sophisticated cyber attacks, a recently signed Executive Order on Improving the Nation's Cybersecurity [1] made a specific reference to removing (contractual) barriers to threat information sharing.

Many questions still remain open, however. In particular, those concerning the user experience and unique challenges faced by security professionals and other participants in CTI exchange that make use of threat intelligence sharing platforms, which have become indispensable tools for cooperative and collaborative cybersecurity.

Despite early views that security and usability are at odds with each other [17], the security world has become acutely conscious of the importance human aspects play in the overall security, use, and adoption of systems that are critical from a security and/or privacy perspective. This is recognized also in the context of CTI, where human motivation and user experience (UX) design have been highlighted as critical success factors for threat intelligence sharing platforms [58]. Yet, empirical evidence on how UX impacts the use and adoption of such platforms, and by extension the cyber incident prevention and response efforts, is largely missing.

Motivated by this research gap, in a first study of its kind, we establish a UX benchmark for a leading open source CTI sharing platform used by over 6,000 organizations [49]. Further, applying a blend of quantitative and qualitative methods in a delicate user research context, we uncover what users value about the studied platform and why, as well as, what they think could be improved in order to overcome the voiced limitations and pain points.

As the core concepts of CTI exchange are incorporated in many CTI sharing platforms, our study not only provides actionable inputs to the developers of MISP, but equally serves to highlight key findings and UX recommendations of relevance to CTI sharing platforms more generally. Besides advancing our understanding of human factors and interaction aspects within the CTI sharing context, this report also draws attention to the possible negative outcomes in terms of CTI sharing effectiveness or disclosure of sensitive information due to usability issues or overall poor UX.

It is worth mentioning that our study insights may be limited due to the challenging participant recruitment circumstances. Nevertheless, we believe that our research has an empirical and a methodological contribution. The former informs the improvement of cybersecurity in real-world systems, the latter demonstrates the utility and necessity of UX research methods applied in a new context, which is in dire need of further interdisciplinary scrutiny.

2 BACKGROUND AND RELATED WORK

2.1 Cyber Threat Intelligence (CTI)

Intelligence sharing is by no means a recent practice, in particular between nation-states, which have been utilizing shared intelligence as a means to provide decision-makers with fresh perspectives on the problems they face or with information on the effects of their decision-making and policies taken [77].

With the rapid proliferation of ICT technology, many capabilities are no longer reserved to nation-states, diffusing the power across the private sector and individual actors [16]. Thus, increasingly interconnected, different participants engage in the collection, processing, analysis, and exchange of information relevant to the protection of the physical, logical or social layers of cyber space.

Threat intelligence (TI), or in this context, Cyber Threat Intelligence (CTI) refers to evidence-based knowledge about an existing or potential threat, that can aid decision-makers in preventing an attack or accelerating the detection of compromised assets [72]. TI can come from a variety of internal and external sources in structured or unstructured formats, such as indicators of compromise (IoCs), tactics, techniques, and procedures (TTPs), security alerts, threat intelligence reports, tool configurations, etc. [37].

The factual insights based on the analysis of the TI can add value and support a number of different activities inside an organization, for instance, security operations and incident response, vulnerability and risk management, brand protection, etc. [45]. Thus, depending on the information source, the form of analysis that is used to produce it as well as the intended audience, CTI can be categorized as strategic, operational, tactical and technical [72].

2.1.1 ***Benefits and incentives for CTI sharing.*** According to NIST, organizations that engage in CTI exchange benefit from the shared situational awareness of the sharing community, enabling them to improve their security posture and achieve greater defensive agility [37]. Many other benefits have been reported in literature, classified along an operational, organizational, economic or policy dimension [80]. To a large extent these benefits overlap with the incentives as to why organizations participate in sharing activities. ENISA outlined 12 incentives to information sharing [21]. Two of those, namely, economic incentives stemming from cost savings, and incentives stemming from the quality, value and use of information shared, were considered to be of high importance.

2.1.2 ***Risks and obstacles to CTI sharing.*** Establishing (mutual) trust has been identified as a key driving factor for reliable and effective information exchange [23, 77]. Trust issues have thus been widely reported as key impediments to information sharing. Research suggests that trust is established over time and in face-to-face meetings [76], but can be undermined in a number of ways, e.g., when information sharing is not reciprocal [22]. These situations

pave way for free riding, which is considered to be an undesirable selfish behavior by certain participants in CTI exchange [50].

Contrary to common views that establishing and maintaining trust is hard and that free-riding is a problem, in a more recent survey of attitudes towards the benefits and barriers to CTI sharing, the majority of respondents did not consider trust establishment to be difficult to achieve, nor did they consider free riding to be a significant impediment [80].

Reluctance to CTI sharing is also driven by the fear of exposing the protective or detective capabilities of an organization, which can disrupt ongoing investigations or response actions as well as jeopardize information for future legal proceedings [37]. Fearing negative publicity and the risk of reputation damage, the perception that an incident is not worth sharing as well as the natural instinct not to share are other examples mentioned in literature [72].

Another significant obstacle is liability with respect to laws that regulate organizations' operations and privacy-related legislation [63]. Several studies have delved into the privacy implications of (automated) information sharing with the government, across organizations or in the context of (international) business-to-business CTI sharing [8, 26, 34, 62, 68].

In addition to the above-mentioned organizational, economic and policy barriers to CTI sharing, operational challenges such as the lack of standardization and the necessity to achieve interoperability and automation have perhaps received the most attention. We briefly mention them in Section 2.2.

2.1.3 ***Human, cultural, and organizational aspects.*** There is a broad stream of literature that examines the nature of the job, the organizational setting, the tools and workflows of IT security professionals and operators [4, 10, 55, 66, 74]. Much of the work here is in the context of security management, security operation centers (SOCs), or incident response, where the importance of collaboration and automation has been highlighted [66, 69]. For instance, security practitioners rely on each other to see the "big picture"[9] and may resort to developing their own tools, e.g., customizable scripts, to carry out specific tasks, capture and share tacit knowledge or improve the usability of a tool [78]. Security managers and analysts in SOCs tend to agree that any cutting-edge technology at their disposal would be underutilized if it suffers from poor usability or if it is hard to learn, thereby also shifting their focus towards the tools and away from the incidents [40].

Investigating collaborative work practices in the context of CTI, Ahrend et al. found that practitioners engage in formal and informal collaborative activities, however, awareness about existing threat and defense knowledge (TDK), its availability, and correlation is impacted by the largely tacit nature of TDK, which is lost due to employee turnover or memory loss [5]. Further, the lack of formal documentation or access restrictions also played a role. A number of system circumvention activities were also reported, e.g., analysts storing TDK artifacts on local machines instead of uploading them to collaborative in-house systems due to perceived usability gains as well as perceptions that "their work is rather individualistic and not directly relevant to other analysts" [5]. When CTI is shared across borders, cultural and language barriers may also arise, thus parties engaged in CTI exchange should define a sharing language as well as understand and respect cultural differences [76].

Safa et Von Solms investigated the impact of extrinsic and intrinsic motivation on employees' attitudes toward the intention of sharing information security knowledge [57]. They found that earning a reputation, gaining promotion, and satisfying curiosity, all had positive effects on employees' attitudes, which in turn affected CTI sharing behavior. Expanding on earlier work taking economic perspectives on information security sharing [28, 30], Mermoud et al. proposed a behavioral framework theorizing how and why human behavior and sharing of security information may be associated [47]. They highlighted that human behavior may be at the core of the problem why CTI is underutilized despite being beneficial, yet cautioned not to infer that CTI sharing should be mandated as that could achieve the adverse effects of inducing compliance by sharing TI that may not be relevant, accurate, or timely [47].

The development and improvement of security professionals' skill-set is considered a key aspect of human capital management, however, recruiting and retaining security staff have been reported as major challenges [74]. Furthermore, there are high turnover rates among security analysts due to burnout, which not only leads to increased spending on frequent hiring and training of new analysts, but also impacts the team spirit and collective incident response [11]. Researchers found that operator fatigue and frustration increased significantly over the course of tactical cyber operations [20], while procedurally distinct network analysis tasks elicited differentiable effects on the cognitive stress and workload of operators [31]. As research in security practitioners and human aspects in cyber is still immature [20], the researchers encouraged further work regarding the specific needs and challenges associated with different tasks in the cyber domain, as well as the nature of the human-computer interaction and the effects of these interactions on the operators' mental states and performance capabilities [31].

2.2 CTI sharing standards and platforms

From the very beginning, organizations engaged in CTI exchange have been faced with a number of technical and operational hurdles, e.g., CTI exchange can demand a great deal of manual effort as threat information can come from a variety of sources [76]; organizations use their own terminology and data standards, which do not directly correspond to those of other organizations [63]; the utilization of meaningful threat intelligence depends on the relevance, timeliness, accuracy, and other quality aspects of CTI artifacts [60], etc.

Thus, questions such as how to automate, harmonize and standardize CTI, while keeping human judgment and control involved in sharing [6], have led to the establishment of a number of standards for structuring and sharing data as well as to the emergence of sharing platforms in an attempt to facilitate sharing and address the problems of collecting and storing threat intelligence. In recent years, a number of papers investigated the CTI sharing landscape, providing comparative analyses of the different platforms, standards, exchange formats and languages as well as the publicly available sources of threat feeds [7, 18, 54, 59].

For instance, Sauerwien et al. [59] found that most CTI sharing platforms rely on standards such as OpenIOC, STIX, and IODEF, arguing that STIX [6] can be considered as the de-facto standard for describing threat intel as it is the one most commonly used. Ramsdale et al. highlighted, however, that despite having industry

and community support, the use of STIX is not that widespread, it often suffers from poor implementation, and that recent trends indicate the use of APIs or platform-specific formats (e.g., MISP and custom JSON formats) as a better fit for the given use cases [54].

In a recent investigation, De Melo e Silva et al. established evaluation criteria for the different CTI sharing standards and platforms based on the selection of the most relevant candidates [18]. They reported that due to the different goals that CTI sharing platforms have, at the moment there is not one fully complete platform that attends to all CTI processes. Nevertheless, MISP and OpenCTI were highlighted as platforms with the most holistic approach, and applicable in a great deal of scenarios. Furthermore, MISP was ranked highest in terms of popularity and considering the compatibility with different formats it could be considered as the most flexible.

2.3 User Experience of CTI sharing platforms

The fact that human-centered design and UX aspects are of paramount importance in the CTI sharing context can also be attested by the inclusion of *usability* as a key evaluation criterion in the recently proposed frameworks for comparing CTI platforms [18]. Nevertheless, despite this recognition, the question of usability and UX remains largely unexplored in this context.

To the best of our knowledge, the only study that explicitly is motivated and investigates UX aspects is the work by Sander and Hailpern [58]. Conducting a series of interviews and ethnographic observations of security analysts and domain experts, the authors proposed a number of *personas* i.e., narrative descriptions of user archetypes reflective of the most important users of a CTI sharing platform. Furthermore, they proposed a number of design requirements, and reflected on three high level insights, grounded in their user research. These refer to: (i) the oftentimes differing personal and corporate motivations and incentives to CTI sharing; (ii) the fact that there is no one typical user, but that there are significant differences as to the type and amount of information that is consumed and contributed across the different personas; and (iii) that younger users expect CTI sharing platforms to offer a sophisticated UX. Finally, they expressed an interest in collaborating with existing solutions in an effort to try and integrate the various design requirements that they put forward, and highlighted the importance of validating them in formal user studies.

Apart from an informal inquiry into the impressions of the usability of a new decentralized CTI platform prototype [46], we are not aware of any study that has performed a formal usability or UX evaluation of an established CTI platform.

The gap in our understanding of the constraining and enabling factors of CTI sharing platforms from a UX lens poses significant challenges in terms of ensuring that our designs match the needs and capabilities of the people we are designing for in such a highly-complex cooperative environment. Furthermore, we believe that it also prevents us from identifying and addressing user misperceptions of system security and privacy, which can have adverse effects on CTI sharing effectiveness. To this end, as far as we know, we are conducting the first such UX evaluation, within the context of the MISP sharing platform.

3 MISP

Conceived within military circles as a malware information sharing platform a decade ago, MISP has in the meantime matured into a community-driven project for gathering, sharing and correlating diverse types of threats, such as indicators of compromise (IoCs), financial fraud information, counter-terrorism information, etc. [49, 75]. As previously mentioned, MISP is regarded as one of the leading OSINT platforms, used by thousands of organizations active in different domains, ranging from NATO agencies and ministries of defense, CSIRT communities, private sector actors etc. [49].

Organizations wishing to engage in CTI exchange via MISP, either need to approach i.e., be invited to an established sharing community, or initiate their own MISP instance given that the source code underpinning the platform is publicly and freely available on the MISP GitHub project page [29]. MISP can also be easily retrofitted for specific communities or objectives, such as the recent COVID-19 MISP instance dedicated to sharing medical information, cyber threats and disinformation related to COVID-19 [48].

Technical details. We invite interested readers to consult available MISP resources (e.g., [29, 49, 75]) in case they would like to better familiarize themselves with the technical details and implementation. Here, we briefly outline some main points.

A MISP instance can be considered as an independent centralized server that facilitates the consumption and contribution of CTI among a defined set of participating organizations. MISP instances can be standalone or they can connect to and exchange information with other instances via different synchronization mechanisms, pursuant to the sharing rules or negotiated terms. Connecting or syncing MISP instances allows for shared CTI to traverse between them in one or both directions, as per user-defined distribution settings. Thus, interconnecting multiple instances creates a de facto decentralized network which is able to send and receive data entries, called *events*, described with different levels of granularity of information as per the user's wish. In terms of the interface used to access MISP, a key distinction can be made between UI users (those using the web portal) and API users (those using ReST API).

Features and functionalities. In terms of supported features and functionalities, MISP seems to account for a large number of the design requirements highlighted by Sander et Hailpern [58], e.g., automatic correlations to find relationships between attributes and indicators from malware or attack campaigns, historical info for indicators and pivoting capability, non-attribution, etc.

A number of actors in the MISP user community regularly organize training sessions and community meetups in order to address training needs as well as discuss the future development of the platform. Furthermore, lots of resources, such as training materials, virtual environments and online repositories, are available to help (prospective) users experiment and test the latest updates, builds and features under development [13].

3.1 Study motivation

MISP is a technically-advanced system. If it aims to cater for a diverse set of users involved in CTI exchange, it needs to account for their distinct needs and objectives as well as their capabilities to engage in CTI sharing activities of various complexity. To date,

there appears to be no empirical evidence on UX evaluations of MISP by the different user groups, nor investigations of usability issues or challenges faced by users.

Given the wide adoption and large user base of MISP, we were motivated to shed light on UX aspects of CTI sharing platforms within this relevant context, as a representative use case. To this end, we formulated the following research questions:

(1) How do different security information workers evaluate the user experience of MISP?
(2) What do users value about MISP and what do they think could be improved?
(3) Which user needs are addressed and accounted for by MISP, and which are neglected?

4 METHODOLOGY

In line with lessons learned and taking into account the voiced difficulties getting access to participants for cybersecurity research [10, 20, 51, 52] we chose to conduct several smaller studies that had a low impact on the environment.

Recruitment. Over the course of two years, we took part in a number of events organized within the MISP user community that were facilitated by the Computer Incident Response Center Luxembourg [12], which is an organization that co-finances and resource-wise supports the development of MISP.

These events represented in Figure 1 – Study overview, refer to: two in-person training sessions, indicated as Study 1 and Study 4; an annual summit of the MISP user community, indicated as Study 2; and one regional community event, indicated as Study 3.

Survey. Data collection for Studies 1, 3 and 4 took place in person, whereas for Study 2 via an online form.

Ethics. The study was approved by our organization's ethics review panel, and consent was obtained through voluntary participation, which was not financially compensated.

4.1 Study components and Methods

Information and Consent. At the beginning of the studies, the participants were informed that the survey aims to assess the UX of MISP and learn more about the needs of its users. They were informed that participation was voluntary and anonymous as well as that they can withdraw their consent to participate at any time without giving reasons and without negative consequences.

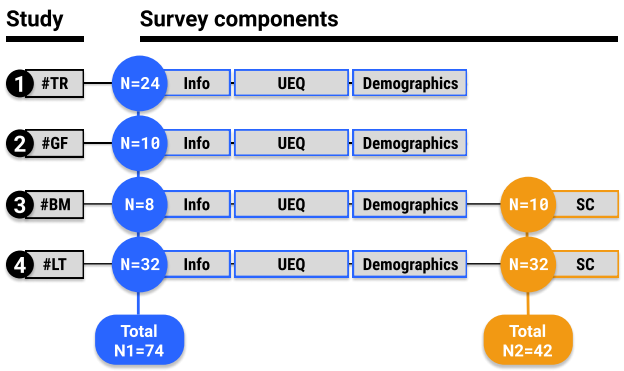


Figure 1: Study overview

UEQ - User Experience Questionnaire. The UEQ is a validated instrument for measuring UX [44] and it is the most widely used standardized UX questionnaire in recent years [19]. It contains 6 scales with a total of 26 items in the form of semantic differentials: (i) *attractiveness* measures users' overall impression of a system or technology; (ii) *perspicuity* measures the degree of ease of learning how to use a system; (iii) *efficiency* measures whether users have to put unnecessary effort into solving a task; (iv) *dependability* measures whether users feel they can rely on the system; (v) *stimulation* measures the level of excitement or motivation to use the system; (vi) *novelty* measures how innovative or creative do users perceive the system to be i.e., whether it triggers their interest [61].

Through the *perspicuity*, *efficiency*, and *dependability* scales, the UEQ investigates the pragmatic, goal-directed, quality aspects. The *stimulation* and *novelty* scales investigate the hedonic aspects, which are not goal-directed, but appeal to sensations. The *attractiveness* scale is considered as a pure valence dimension [61].

Demographics. After the UEQ, there was a demographics section where we sought to learn more about our participants, their education, technical background as well as prior experience and engagement with MISP. This was the last section in Studies 1 & 2.

SC - Sentence completion. SC is a semi-structured projective technique that can be deployed to understand user needs and values by providing only a sentence stimulus to research participants who are free to interpret it and respond to it from their own frame of reference [41]. Complementing UX questionnaires, SC is a practical method for obtaining qualitative inputs and a quick overall understanding of how users interpret their experiences with a system, in a structured way and in a fraction of the time in comparison to interviews [41]. For our investigation, we tailored the stems used by Kujala et al. [41] to our context, represented in Table 2. SC was the final section of the survey in Studies 3 and 4.

5 RESULTS AND ANALYSIS

5.1 Participants

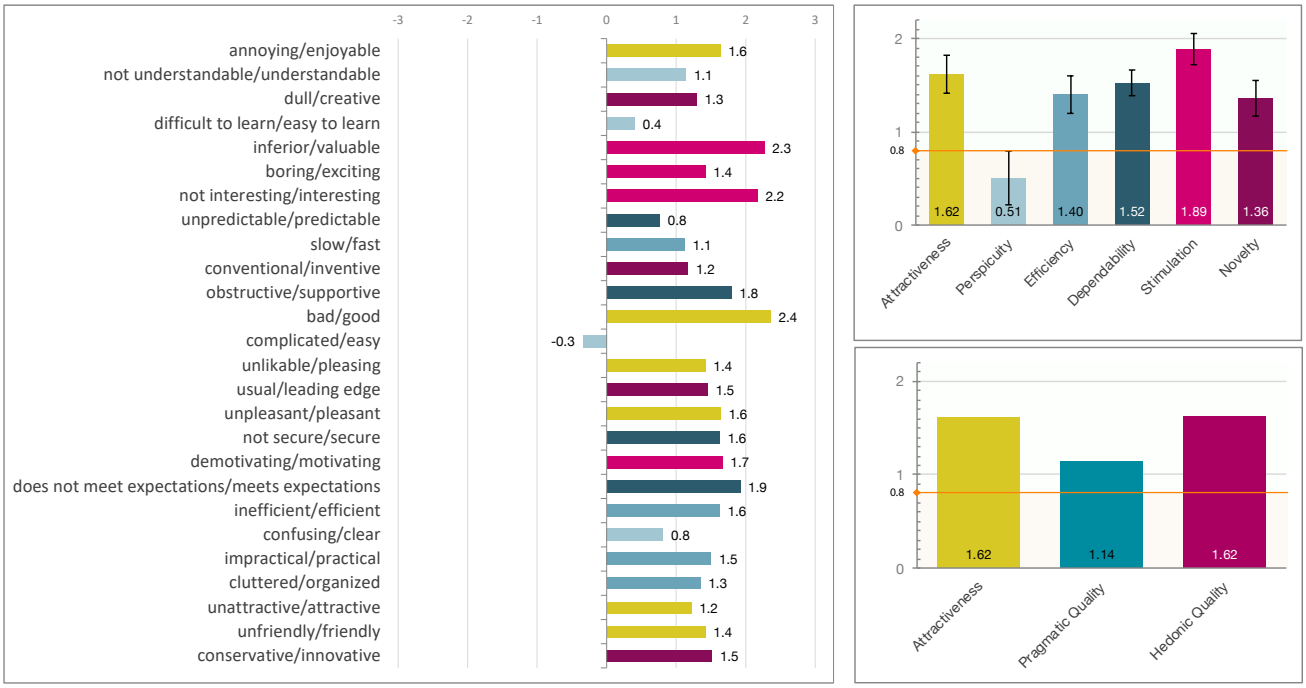
Table 4 in Appendix C presents the main participant demographics.

Out of the 74 participants, 70 (95%) were male. 66 participants (89%) had an engineering or computer science background. 63 of them (85%) had a Bachelor's degree or higher.

There were 32 participants (43%) in the age span of 26 – 35 years, and the second largest age group consisted of 27 participants (37%) in the range 36 – 45. In terms of prior experience with MISP, the largest subgroups consisted of those that had never used MISP before their training session and those that had used MISP between 6 – 12 months, which in both cases was 24%. Less than 25% of the participants had used MISP for more than 12 months.

28 participants (38%) saw themselves as having more than one role, with *Security Analyst* being the most frequent role indicated by 53 participants (72%). The most represented group in terms of industry was *ICT Consulting/Advisory* with 20 participants (27%).

It was the first training session for 61 attendees (82%), and 45% of our participants indicated that they had used the training materials and MISP virtual machine before. 30% indicated that they had used the PyMISP API before, 42% had cloned a MISP repository, whereas 18% had contributed to any of the MISP repositories.



(a) Mean values per scale item

(b) Mean values per scale (above) and quality (below)

Figure 2: Main UEQ results.

5.2 Quantitative section (UEQ)

All responses were collected for preparatory coding and analysis using the UEQ data analysis tool (ver. 8) [73] and with the statistical software SPSS. Inconsistent responses were identified and removed whenever more than 3 subscales contained inconsistent response patterns, leading to 74 responses available for further analysis.

Data grouping. To investigate the possibility of grouping our responses from the four studies into a single data set, we performed tests of homogeneity of variance, and an ANOVA with post hoc tests using bootstrapping of 1,000 samples to determine any statistically significant differences between the means of the 6 UEQ scales from our four studies. This led to the exclusion of the 10 responses from Study 2. No statistically significant differences were obtained for Studies 1, 3 and 4, which we grouped for subsequent analyses.

5.2.1 ***UEQ Results.*** Table 1 and Figure 2 show the main results of the combined UEQ analysis for studies 1, 3 and 4. The mean values per individual scale item can be found in Table 5 in Appendix C.

According to the standard interpretation of the UEQ, values for the scale means that are < -0.8 represent a negative evaluation, values in the range -0.8 to 0.8 represent a neutral evaluation, and values > 0.8 represent a positive evaluation. Our results denote an overall *positive* evaluation of MISP across all scales, except for *Perspicuity* where the scale mean belongs to the range -0.8 to 0.8, thus evaluated as *neutral*.

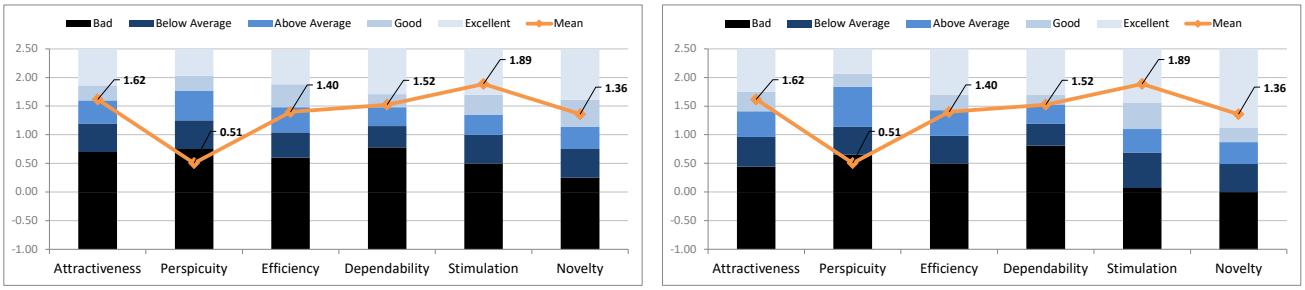
5.2.2 ***Benchmark comparison.*** As this is the first study of its kind, there is no baseline to qualify the observed measurements within the CTI context. However, these results can be compared to other studies that deploy the UEQ.

Table 1: Main UEQ results. N = 64.

Scale	Evaluation	Mean	Std. Dev.	MoE	5% CI
Attractiveness	Positive	1.62	0.83	0.203	[1.41, 1.82]
Perspicuity	Neutral	0.51	1.18	0.288	[0.21, 0.79]
Efficiency	Positive	1.40	0.82	0.201	[1.20, 1.60]
Dependability	Positive	1.52	0.56	0.138	[1.39, 1.66]
Stimulation	Positive	1.89	0.68	0.167	[1.72, 2.05]
Novelty	Positive	1.36	0.78	0.191	[1.17, 1.55]

Setting the measured scale means from Table 1 in relation to a benchmark dataset that contains evaluations from 20,190 persons across 452 studies (as per version 8 of the UEQ handbook and data analysis tools [61]), we can estimate the relative UX quality of MISP compared to other systems. Figure 3a provides a comparison to the general benchmark consisting of the whole data set, whereas Figure 3b shows the comparison against a specialized benchmark of 85 product evaluations of websites and web services. Appendix C contains the benchmark comparison tables 6 and 7.

In both cases, MISP's *perspicuity* aspect is categorized as *bad* i.e., in the range of the 25% worst results. This is in contrast to the other 5 scales, which are categorized at least as *above average*. In both benchmark comparisons, the hedonic aspects of MISP are evaluated higher than in 75% of the investigated products, with *stimulation* categorized as *excellent* i.e., in the range of the 10% best results.



(a) Comparison to a general benchmark.

(b) Comparison to a specialized benchmark of websites and web services.

Figure 3: Comparison to benchmark values from UEQ evaluations of other systems.

5.2.3 ***Demographic differences.*** To investigate differences in the evaluation of MISP based on distinct participant profiles and characteristics, we performed a number of group comparisons. Details on how we split the sample, the statistical tests and results can be found in Appendix B, which we discuss further in Section 6.

5.3 Qualitative section (SC)

Table 2: Overview of Sentence completion stems and corresponding response rates *(N=42).*

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

As visible in Table 2, across the two sessions where the SC activity was administered, 42 participants completed 211 out of possible 336 sentence stems (63%). In our analysis, we used a theoretically-driven inductive approach [70], in which, the coding system was generated inductively, but we drew from the theoretical perspectives of psychological needs [64], positive and negative emotions [53], as well as UX [32], when identifying and naming themes.

The thematically-driven stems were used as a guide for the creation of first level codes (user-related and system-related aspects) by which to assign all participant input. Inductive coding was then used to produce second level codes and to draw further insights on the guiding research questions. Preliminary coding from one session was undertaken by the lead researcher. This was then independently verified by a second researcher, so as to ensure consensus across the identified coding categories, and to drive discussion and further refining where coding disagreements arose. The rest was then coded by the lead researcher, in consultation where necessary. Table 3 outlines the main themes identified per SC stem.

Table 3: Overview of the most frequent themes emerging from the data during the qualitative analysis.

Themes	Theme frequency per sentence stem								
	S1	S2	S3	S4	S5	S6	S7	S8	T
User-related aspects									
Needs and values	9	0	0	0	11	2	4	6	**32**
Emotion evocation	34	2	0	4	1	3	0	0	**44**
- Positive emotions	*22*	*2*	*0*	*0*	*0*	*2*	*0*	*0*	*26*
- Negative emotions	*12*	*0*	*0*	*4*	*1*	*1*	*0*	*0*	*18*
User characteristics	0	1	7	1	0	6	13	0	**28**
System-related aspects									
MISP characteristics	1	0	0	0	12	6	1	7	**27**
UX qualities	16	34	12	39	31	25	2	21	**180**
- Attractiveness	*0*	*0*	*0*	*16*	*0*	*0*	*0*	*6*	*22*
- Lack of attractiveness	*0*	*0*	*0*	*5*	*0*	*2*	*0*	*0*	*7*
- Pragmatic qualities	*3*	*34*	*0*	*7*	*29*	*0*	*2*	*10*	*85*
- Lack of pragmatic q.	*10*	*0*	*12*	*7*	*0*	*23*	*0*	*0*	*52*
- Hedonic qualities	*3*	*0*	*0*	*0*	*2*	*0*	*0*	*5*	*10*
- Lack of hedonic q.	*0*	*0*	*0*	*4*	*0*	*0*	*0*	*0*	*4*

5.3.1 ***User-related aspects.***

Needs and values. As a major source of positive UX, the following themes were voiced as dominant psychological needs and values accounted for by MISP: *competence*, *control*, *autonomy*, and in particular, *relatedness*.

As exemplified by the following verbatims, users feel capable and effective in their work, they value that MISP supports their routines and habits, as well as their control over options.

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

S5 "*… its flexibility allows me to solve my problems and I do not have to change my way of working*" (BM18)

The support in fulfilling the psychological need of *relatedness / belongingness* was raised most often, suggesting that MISP is perceived particularly well along its core objective of connecting parties interested in CTI sharing.

S1 "*… 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)

S5 "*... its aim is to promote sharing (cyber information); it includes a lot of users/contributors*" (LT28)
S5 "*... it is a community-based sharing platform*" (BM10)

Evocation of emotions. Besides need-related aspects, participants also expressed their emotional experiences with MISP.

Overall, positive emotions dominated, with *satisfaction*, *confidence*, *pride*, and *courage* being most reported.

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 suppliment [sic] to the documentation*" (BM14)

On the other hand, *confusion* was denoted as the most prominent negative emotion evoked, as hinted by these verbatims.

S1 "*When I use MISP, I feel overwhelmed with the amount and type of data*" (BM12)
S4 "*I think the appearance of MISP is causing confusion*" (BM10)
S6 "*The problem with MISP is its integration, this is confusing for me*" (LT27)

Some participants highlighted *boredom* as well as *frustration*.

S1 "*When I use MISP, I feel a bit lost, need to search a lot to find what I need*" (BM7)

User characteristics. Another significant portion of user-related codes focused on the profile and characteristics of users, in particular the role of technical expertise and experience with MISP and CTI sharing in general.

S7 "*People who use MISP are typically experts on security*" (LT11)
S3 "*MISP is not suitable for non techies*" (BM11)
S3 "*... not suitable for quick ad-hoc analysis by non IT professionals*" (LT25)
S3 "*... not suitable for inactive organizations/users*" (LT22)

The opportunity to address an unmet user need of *relatedness* can be identified through the following statement.

S6 "*The problem with MISP is lack of a public community that new users can join when starting out*" (LT3)

5.3.2 *System-related aspects.*

MISP characteristics. A number of SC stems triggered participants to express what system characteristics they value. Participants had a particularly high opinion of MISP's *freeness* and *openness*.

S5 "*I am happy with MISP because it is open (source)*" (LT30)
S5 "*... has potential to integrate with other tools and is open-source*" (LT16)
S8 "*Compared to other TI sharing platforms, MISP is free, open-source and not managed by big companies*" (BM20)
S8 "*... far more open*" (LT19)

MISP's *adaptation* properties were also much appreciated.

S5 "*I am happy with MISP because it just works 95% of the time and it's enormously flexible as a tool*" (BM14)
S5 "*... can be used in different ways*" (LT31)

UX qualities. The largest proportion of user inputs described UX qualities (or lack thereof) grouped along three main dimensions.

Attractiveness. Our participants did not provide a homogeneous response regarding the *attractiveness* of MISP, in particular the *aesthetics* of the platform, as evident by these opposing verbatims.

S4 "*I think the appearance of MISP is quite pleasing*" (BM7)
S4 "*I think the appearance of MISP is very good*" (LT27)
S4 "*the appearance of MISP [is] has room for improvement*" (BM18)
S6 "*The problem with MISP is [its] look and feel*" (LT19)

Pragmatic aspects. The ability for MISP to support the effective and efficient achievement of CTI tasks i.e., the *instrumental* quality of the platform was the most frequent theme in our data. MISP was perceived as useful along both utility and usability dimensions.

S5 "*... it has a lot of features*" (LT6)
S8 "*...well-maintained and good feature set*" (LT16)
S8 "*...complete, simple and free*" (LT16)

Participant statements reveal how MISP supports them in *searching*, *organizing*, *correlating* and *contextualizing* indicators of compromise (IoCs) and other CTI data.

S5 "*... the API allows easy access to filter the data needed*" (BM12)
S2 "*MISP is best for analysing and validating security incidents*" (LT7)
S2 "*MISP is best for identifying events, their sources, and their attributes*" (LT7)

The core functionality of *collaboration* and *sharing* (technical) threat intelligence was particularly emphasized.

S5 "*I am happy with MISP because it allows actionable information sharing*" (LT12)
S2 "*MISP is best for exchanging IOC*" (LT13)
S2 "*MISP is best for documenting malware and incidents and sharing that information*" (LT12)
S2 "*MISP is best for having a centralized place to store and collaborate on data*" (LT8)

Participants did, however, also raise a number of pragmatic issues. On the utilitarian side, these ranged from the lack of applicability in certain sectors to the lack of suitability for specific CTI workflows.

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*" (LT3)
S3 "*... not suitable for use out of the box (complex, needs deep integration into workflow)*" (LT30)
S3 "*... not suitable for full IR management process*" (LT8)

As regards usability, which was much more commented, participants emphasized the *lack of clarity and efficiency* as well as the *complexity*, or more generally the *lack of perspicuity*, of MISP.

S4 "*I think the appearance of MISP is chaotic at times*" (BM6)
S6 "*The problem with MISP is it that it requires too much time*" (LT13)
S6 "*The problem with MISP is finding the balance between good enough information and time invested*" (LT12)
S6 "*The problem [...] is many tools/features (good problem)*" (LT9)

The *lack of learnability* and difficulty to cut through the complexity of MISP was a major concern:

S6 "*...that is huge and kind of hard to start with* " (LT11)
S6 "*...it has a steep learning curve*" (LT16)

S4 "*...needs to be explained to be more used*" (LT28)
S6 "*...it is hard to get started adding events if you never saw an example*" (LT6)

Hedonic aspects. While less frequent, users also mentioned hedonic aspects related to their experience with MISP, in particular, *novelty* and *stimulation*, or lack thereof.

S4 "*... good, but a little old fashioned*" (BM9)
S8 "*Compared to other threat information sharing platforms, MISP is a breath of fresh air*" (BM14)
S5 "*I am happy with MISP because it is an awesome tool*" (LT27)

6 DISCUSSION

Summary of key findings. The UEQ scores from Section 5.2 show an overall positive UX evaluation across the three main system quality aspects i.e., *attractiveness*, *pragmatic* and *hedonic* qualities. This finding is arguably not unexpected, as it would be challenging for MISP to achieve such widespread utilization if its UX was largely perceived as negative. At the same time, we cannot exclude the possibility that the obtained results are skewed towards more positive as the majority of our study participants were recruited around training events, which might imply active interest in the platform. Further, their level of experience both with the tool and in the industry may not fully reflect the body of actual users of MISP, potentially narrowing the scope of our findings.

Nevertheless, taking into account the shortage of security specialists [27], the high turnover rates among security analysts and their needs for adequate training [11], and the increased interest in CTI sharing beyond the security community, we can assume that the number of users who experience the system for the first time or are still novice is not insignificant. Understanding their UX needs and challenges is crucial to fully onboarding them as adopters who are confidently participating in CTI exchange. In this regard our research brings greater granularity and clarity regarding the different aspects that impact the experience.

The lower mean value for the *pragmatic* quality (1.14) is mainly due to the low *perspicuity* evaluation of MISP (0.51), which is the only aspect rated below the positive threshold. One should not directly conclude, however, that MISP has a low utilitarian value. The qualitative insights obtained using the sentence completion method (Section 5.3), provide further understandings behind the quantitative ratings of the UEQ. Furthermore, investigating the user experience more holistically, rather than solely through a usability-focused prism (as discussed later), allowed us to capture user needs more comprehensively.

The results presented earlier point to the complex relationship many users have with MISP. On the one hand, the platform is praised for being useful, valuable, and empowering, on the other hand, it is also perceived as overwhelming. As regards the threat intelligence aspect of the system, users value the flexibility and adaptation offered by MISP. Nonetheless, they express concerns about the difficulty to learn the system and its complexity. Our results also highlight the importance of the user community, which in the case of MISP strongly values the openness, open-source nature of the platform and contributors. However, our findings also suggest that there might be a gap to be bridged among novice users until they feel onboarded. Furthermore, the sentence completion responses indicate that the platform is very much technology-oriented, which might be a negative association for certain beginners or non-technical users that MISP attempts to onboard in different verticals or areas of interest (e.g., COVID research, misinformation, dark patterns etc.).

Our findings are of relevance beyond MISP. As reported in literature, many approaches to user-centered design rely on measures of the quality of interactive systems, such as benchmarking against usability measured for competitors' systems [35]. In this respect, similar investigations of other CTI platforms could estimate how those systems fare against MISP along the different UX dimensions. Further, many of the positive and negative accounts that our study participants reported transcend MISP as a system and relate to user needs that were either fulfilled or neglected. Thus, much can be learnt as to what users find important in this context and why, which can be of use to designers of other CTI sharing platforms as well as researchers of socio-technical security in general.

Implications. The user concerns highlighted above, such as the complexity of the platform, the steep learning curve as well as the perceived lack of support or community for novice users, opens potential problems both in terms of errors, as well as under-utilization i.e., adoption problems. Thus, designers of CTI sharing platforms should also take into account many of the base findings and assumptions coming from the field of computer-supported cooperative work (CSCW) [2], to narrow the gap between the social requirements and the technical feasibility in CTI exchange.

For instance, access control systems should accommodate the nuanced behavior that people have with respect to how and with whom they share information, their concerns about sharing specific pieces of information at a particular time, or the effects of information disclosure [2]. Awareness about who else is present in a "shared space" and allowing for low-level monitoring of others' activities as well as making information exchange visible is important both for guiding people's work and actions [24] as well as enabling learning and greater efficiencies [36]. However, making people's work visible may also open them to scrutiny or criticism, which can impact their willingness to share information [2].

Both of the afore-mentioned aspects are very important in particular for novice and non-expert users. In this respect, MISP offers plenty of distribution options, meaning different pieces of information can reach different entities within the same and/or connected MISP instances. Furthermore, a *delegation* feature allows users to entrust another party on the MISP instance to share a CTI event and remove the binding between the information shared and the reporting organization. However, not knowing about these options due to the cognitive overload new users are faced with as they get started with MISP, or having a misperception about the core functioning of such a security system due to a poor UX, can have serious consequences.

To illustrate, even if a shared CTI event refers to Indicators of Compromise (IoCs) only, certain organizations might perceive the information as sensitive because its (premature) disclosure could impede a successful response to a cyber attack. Or it could be sensitive as the shared information might imply that the organization disclosing the event is a potential victim of a specific attack, which

in itself can have negative reputation consequences. Thus, performing this core activity without knowing or disregarding who the (intended) recipients of the shared information are, can lead to both *oversharing* i.e., accidental leakage of sensitive information to parties beyond what was initially planned, as well as to *undersharing* i.e., to lower preparedness levels of the sharing community as vital pieces of information would not be reaching the other members. Both can play a role in the perception of the platform's efficiency, usefulness, and added value, ultimately impacting the future use and adoption, where no adoption in essence means lower overall cyber preparedness and security.

Beyond usability. We can also pose the question: Why would someone start or continue using a certain CTI sharing platform even though it is hard to learn? Just as traditional models of rational choice disregard the numerous factors that impact actual privacy and security decision-making [3], so are narrow usability investigations unable to provide much insights in this direction. A typical usability study would normally focus on task-related efficiency and effectiveness, which would omit other equally important aspects that impact the overall impression, appeal and intention to use a system [33, 42, 79]. Our study shows that the psychological need of *relatedness / belongingness* [56] can play a key role here.

This is not to say that investigating pure functionality aspects is less important, especially in such an expert domain where *fun* is not the main design objective of the system. However, disregarding factors such as people's affective reactions before, during or after using a specific system, the emotional relationships they build with specific technology, or the fulfillment of psychological needs that can be mediated via technology, can pose major shortcomings during the design as well as evaluation stages of a system's lifecycle. Far too often, core security and privacy research takes an overly simplistic approach to investigating the human role or how to make systems usable. We hope that our study brings to the fore the importance of approaching UX in a holistic manner and that the deployed methods and approach taken can serve as a blueprint to the wider security community when investigating not only other CTI sharing platforms, but security tools and systems in general.

Future Work. While we do not have compelling evidence of the relationship between the evaluation of MISP and the expertise level of the users, the results from Section 5.2.3 (see Appendix B) prod us to investigate whether users that, in one way or another, are more involved with the platform, are able to recognize more the different UX qualities in MISP. For instance, those that had used MISP in multiple roles, those that had used the system for more than one year, or those that had used the training materials, found MISP more *stimulating* to use. These assumptions and the other findings stemming from this baseline UX evaluation, would require further validation. To this end, replication studies are strongly encouraged.

More research is needed not only to establish UX as a standard criterion when assessing different CTI platforms, but also in terms of how UX design can help users cut through the complexity as they learn to use the system for different CTI activities. In light of the afore-mentioned adoption and security implications, future research could explore: *(i)* whether users have a correct understanding of how far does CTI information travel when it is shared in a platform like MISP; *(ii)* how are users supported in this core activity e.g., are there user interface mechanisms, documentation, or is training required; *(iii)* how does end-user feedback loop back to the designers of a CTI sharing platform and whose responsibility is the UX in open-source, community-driven projects like MISP?

Eliciting and incorporating representative views that reflect the different user groups of the platforms under investigation is of paramount importance. To this end, future work could also experiment with different user research methods and recruitment strategies as well as propose and explore how integrated avenues within the CTI sharing platforms themselves could seek to solicit UX feedback that could potentially reach a wider and more diverse user segment.

Limitations. Our work comes with certain limitations that should be considered when interpreting the results and analysis of our study. Despite our best efforts to collect inputs from a larger sample of MISP users, we also experienced difficulties recruiting and getting access to larger numbers of participants from our target population. Thus, the given sample size, the profile of the participants, and the recruitment circumstances limit the generalizability of the different UX evaluations. Further, our sample was skewed towards novice users, who were mostly male and with a technical background. Thus, we risk omitting important under-represented views.

As our study was conducted over a period of two years, different users were not working with exactly the same version of MISP, as it is a system that is in continuous development. Nevertheless, no radical changes were introduced to the system with respect to activities covered during the MISP training sessions.

Lastly, while we deployed standardized and validated methods for evaluating the UX, every context is specific and the methods are not a perfect fit for every situation [43]. For instance, we do not make a distinction between different components of MISP and consequently we do not know which aspect of the user interaction or experience was reported by the participants or dominated their evaluation. Similarly, it is hard to discern whether certain evaluations (e.g., stimulation) are restricted to MISP as a system or to the activity of CTI exchange via MISP more broadly.

7 CONCLUSION

The exchange of CTI is a crucial element in the fight against the increasing number and complexity of cyber attacks. To date, research in this field has mainly overlooked UX aspects, which are essential for the successful deployment and utilization of CTI sharing platforms. Through the use case of MISP, we highlighted what novice users perceive to be the strengths and weaknesses of a leading system of this kind. Furthermore, by specifying appropriate metrics and performing a benchmark UX evaluation of MISP, we not only aspired to contribute to the improvement in the quality of cybersecurity in real-world systems, but also to enrich the discourse on CTI sharing with new UX perspectives. These contributions provide much needed insights into an understudied facet of the CTI sharing problematic. Our study also demonstrated that many user and system-related needs can remain hidden unless we take an expanded notion of the UX and go beyond usability studies which look at task-related aspects only. This has implications beyond CTI, and should be taken into account in the investigations of security tools and systems in general.

We hope that the reported findings also help the designers and developers of other CTI platforms, who can take into account what users value about MISP and why, as well as how they could aim to overcome identified shortcomings from an aesthetic, pragmatic, or hedonic perspective. Through the presented methods and our accounts of conducting user research in this context, we also aim to inspire further studies, investigating both CTI sharing systems as well as different user groups. Further work is needed to incorporate additional views which we were unable to account for in this study, and to uncover a plethora of user related challenges and opportunities in the service of securing organizations and communities.

ACKNOWLEDGMENTS

We would like to thank the Computer Incident Response Center Luxembourg (CIRCL) for their collaboration and for facilitating this research. We would also like to thank Michel van Eeten as well as the anonymous reviewers for their useful comments and suggestions on how to improve this paper. Authors are supported by the Luxembourg National Research Fund through grant PRIDE15/10621687/SPsquared.

REFERENCES

[1] 2021. Executive Order No. 14,028 of May 12, 2021, 86 FR 26633. , 26633–26647 pages. https://www.federalregister.gov/executive-order/14028

[2] Mark S. Ackerman. 2000. The Intellectual Challenge of CSCW: The Gap between Social Requirements and Technical Feasibility. *Hum.-Comput. Interact.* 15, 2 (Sept. 2000), 179–203. https://doi.org/10.1207/S15327051HCI1523_5

[3] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. 2017. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Comput. Surv.* 50, 3, Article 44 (Aug. 2017), 41 pages. https://doi.org/10.1145/3054926

[4] Enoch Agyepong, Yulia Cherdantseva, Philipp Reinecke, and Pete Burnap. 2020. Challenges and performance metrics for security operations center analysts: a systematic review. *Journal of Cyber Security Technology* 4, 3 (July 2020), 125–152. https://doi.org/10.1080/23742917.2019.1698178

[5] Jan M. Ahrend, Marina Jirotka, and Kevin Jones. 2016. On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit Threat and Defence Knowledge. *2016 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2016* (2016). https://doi.org/10.1109/CyberSA.2016.7503279

[6] Sean Barnum. 2012. Standardizing cyber threat intelligence information with the structured threat information expression (stix). *Mitre Corporation* 11 (2012), 1–22.

[7] Sara Bauer, Daniel Fischer, Clemens Sauerwein, Simon Latzel, Dirk Stelzer, and Ruth Breu. 2020. Towards an Evaluation Framework for Threat Intelligence Sharing Platforms. In *53rd Hawaii International Conference on System Sciences, HICSS 2020, Maui, Hawaii, USA, January 7-10, 2020*. ScholarSpace, 1–10. http://hdl.handle.net/10125/63978

[8] Jaspreet Bhatia, Travis D. Breaux, Liora Friedberg, Hanan Hibshi, and Daniel Smullen. 2016. Privacy risk in cybersecurity data sharing. *WISCS 2016 - Proceedings of the 2016 ACM Workshop on Information Sharing and Collaborative Security, co-located with CCS 2016* (2016), 57–64. https://doi.org/10.1145/2994539.2994541

[9] David Botta, Kasia Muldner, Kirstie Hawkey, and Konstantin Beznosov. 2011. Toward understanding distributed cognition in IT security management: The role of cues and norms. *Cognition, Technology and Work* 13, 2 (2011), 121–134. https://doi.org/10.1007/s10111-010-0159-y

[10] David Botta, Rodrigo Werlinger, André Gagné, Konstantin Beznosov, Lee Iverson, Sidney Fels, and Brian Fisher. 2007. Towards understanding IT security professionals and their tools. *ACM International Conference Proceeding Series* 229 (2007), 100–111. https://doi.org/10.1145/1280680.1280693

[11] Sathya Chandran, Xinming Ou, Alexandru G. Bardas, Jacob Case, Michael Wesch, John McHugh, and S. Raj Rajagopalan. 2019. A human capital model for mitigating security analyst burnout. *SOUPS 2015 - Proceedings of the 11th Symposium on Usable Privacy and Security* (2019), 347–359.

[12] CIRCL. 2021. CIRCL – Computer Incident Response Center Luxembourg. Retrieved September 15, 2021 from https://www.circl.lu

[13] CIRCL. 2021. MISP - Malware Information Sharing Platform and Threat Sharing - Training Materials. Retrieved September 15, 2021 from https://www.circl.lu/services/misp-training-materials/

[14] CISA. 2020. Alert (AA20-352A) Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations. https://us-cert.cisa.gov/ncas/alerts/aa20-352a.

[15] CISA. 2021. Alert (AA21-131A) DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks. Retrieved September 15, 2021 from https://us-cert.cisa.gov/ncas/alerts/aa21-131a

[16] Dave Clemente. 2013. Cybersecurity. In *Routledge Companion to Intelligence Studies*. Routledge. https://doi.org/10.4324/9780203762721.ch26

[17] Lorrie Cranor and Simson Garfinkel. 2005. *Security and Usability: Designing Secure Systems that People Can Use.* O'Reilly Media, Inc.

[18] Alessandra de Melo e Silva, João José Costa Gondim, Robson de Oliveira Albuquerque, and Luis Javier García Villalba. 2020. A methodology to evaluate standards and platforms within cyber threat intelligence. *Future Internet* 12, 6 (2020), 1–23. https://doi.org/10.3390/fi12060108

[19] Ignacio Díaz-Oreiro, Gustavo López, Luis Quesada, and Luis A. Guerrero. 2019. Standardized Questionnaires for User Experience Evaluation: A Systematic Literature Review. *Proceedings* 31, 1 (2019). https://doi.org/10.3390/proceedings2019031014

[20] Josiah Dykstra and Celeste Lyn Paul. 2018. Cyber Operations Stress Survey (COSS): Studying fatigue, frustration, and cognitive workload in cybersecurity operations. *11th USENIX Workshop on Cyber Security Experimentation and Test, CSET 2018, co-located with USENIX Security 2018* (2018).

[21] ENISA. 2010. *Incentives and Challenges for Information Sharing in the Context of Network and Information Security.* Technical Report. European Union Agency for Network and Information Security, Heraklion.

[22] ENISA. 2013. *Detect, SHARE, Protect: Solutions for Improving Threat Data Exchange among CERTs.* Technical Report. European Union Agency for Network and Information Security, Heraklion.

[23] ENISA. 2015. *Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches (ISBN 978-92-9204-131-1).* Technical Report December. European Union Agency for Network and Information Security, Heraklion. 1–64 pages.

[24] Thomas Erickson, David N. Smith, Wendy A. Kellogg, Mark Laff, John T. Richards, and Erin Bradner. 1999. Socially Translucent Systems: Social Proxies, Persistent Conversation, and the Design of "Babble". In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Pittsburgh, Pennsylvania, USA) *(CHI '99)*. Association for Computing Machinery, New York, NY, USA, 72–79. https://doi.org/10.1145/302979.302997

[25] Europol. 2020. *Internet Organised Crime Threat Assessment (IOCTA) 2020.* Technical Report. European Union Agency for Law Enforcement Cooperation. 64 pages.

[26] Gina Fisk, Calvin Ardi, Neale Pickett, John Heidemann, Mike Fisk, and Christos Papadopoulos. 2015. Privacy principles for sharing cyber security data. *Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015* (2015), 193–197. https://doi.org/10.1109/SPW.2015.23

[27] Steven Furnell, Pete Fischer, and Amanda Finch. 2017. Can't get the staff? The growing need for cyber-security skills. *Computer Fraud & Security* 2017, 2 (2017), 5–10. https://doi.org/10.1016/S1361-3723(17)30013-1

[28] Esther Gal-Or and Anindya Chose. 2005. The economic incentives for sharing security information. *Information Systems Research* 16, 2 (2005), 186–208. https://doi.org/10.1287/isre.1050.0053

[29] GitHub. 2021. GitHub - MISP/MISP/ MISP (core software) - Open Source Threat Intelligence and Sharing Platform. Retrieved September 15, 2021 from https://github.com/MISP/MISP

[30] Lawrence Gordon, Martin Loeb, and William Lucyshyn. 2003. Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy* 22, 6 (2003), 461–485.

[31] Eric T. Greenlee, Gregory J. Funke, Joel S. Warm, Ben D. Sawyer, Victor S. Finomore, Vince F. Mancuso, Matthew E. Funke, and Gerald Matthews. 2016. Stress and workload profiles of network analysis: Not all tasks are created equal. *Advances in Intelligent Systems and Computing* 501 (2016), 153–166. https://doi.org/10.1007/978-3-319-41932-9_13

[32] Marc Hassenzahl, Sarah Diefenbach, and Anja Göritz. 2010. Needs, affect, and interactive products – Facets of user experience. *Interacting with Computers* 22, 5 (September 2010), 353–362. https://doi.org/10.1016/j.intcom.2010.04.002

[33] Marc Hassenzahl, Axel Platz, Michael Burmester, and Katrin Lehner. 2000. Hedonic and ergonomic quality aspects determine a software's appeal. *Conference on Human Factors in Computing Systems - Proceedings* 2, 1 (2000), 201–208. https://doi.org/10.1145/332040.332432

[34] Martin Horák, Václav Stupka, and Martin Husák. 2019. GDPR compliance in cybersecurity software: A case study of DPIA in information sharing platform. *ACM International Conference Proceeding Series* (2019). https://doi.org/10.1145/3339252.3340516

[35] Kasper Hornbæk. 2006. Current practice in measuring usability: Challenges to usability studies and research. *International Journal of Human-Computer Studies*

64, 2 (2006), 79–102. https://doi.org/10.1016/j.ijhcs.2005.06.002
[36] E Hutchins. 1995. (1995b). How a cockpit remembers its speeds. Cognitive Science, 19, 265-288. (1995).
[37] Christopher S. Johnson, Mark Lee Badger, David A. Waltermire, Julie Snyder, and Clem Skorupka. 2016. *Guide to Cyber Threat Information Sharing*. Technical Report NIST Special Publication (SP) 800-150, October, 2016. National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-150
[38] Shinichi Kamiya, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis, and René M Stulz. 2021. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics* 139, 3 (2021), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019
[39] Mazaher Kianpour, Harald Øverby, Stewart James Kowalski, and Christopher Frantz. 2019. Social Preferences in Decision Making Under Cybersecurity Risks and Uncertainties. In *HCI for Cybersecurity, Privacy and Trust*, Abbas Moallem (Ed.). Springer International Publishing, Cham, 149–163.
[40] Faris Bugra Kokulu, Yan Shoshitaishvili, Ananta Soneji, Ziming Zhao, Gail Joon Ahn, Tiffany Bao, and Adam Doupé. 2019. Matched and mismatched SOCs: A qualitative study on security operations center issues. *Proceedings of the ACM Conference on Computer and Communications Security* (2019), 1955–1970. https://doi.org/10.1145/3319535.3354239
[41] Sari Kujala, Tanja Walsh, Piia Nurkka, and Marian Crisan. 2014. Sentence completion for understanding users and evaluating user experience. *Interacting with Computers* 26, 3 (2014), 238–255. https://doi.org/10.1093/iwc/iwt036
[42] Mike Kuniavsky. 2007. User Experience and HCI. In *The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies, and Emerging Applications (Human Factors and Ergonomics Series)*, Andrew Sears and Julie A. Jacko (Eds.). L. Erlbaum Associates Inc., USA, 897–916.
[43] Carine Lallemand and Vincent Koenig. 2017. How Could an Intranet Be Like a Friend to Me? Why Standardized UX Scales Don't Always Fit. In *Proceedings of the European Conference on Cognitive Ergonomics 2017* (Umeå, Sweden) *(ECCE 2017)*. Association for Computing Machinery, New York, NY, USA, 9–16. https://doi.org/10.1145/3121283.3121288
[44] Bettina Laugwitz, Theo Held, and Martin Schrepp. 2008. Construction and Evaluation of a User Experience Questionnaire. In *HCI and Usability for Education and Work*, Andreas Holzinger (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 63–76.
[45] Jeff May. 2020. *The Security Intelligence Handbook: How to disrupt adversaries and reduce risk with security intelligence.* CyberEdge Group, LLC.
[46] Florian Menges, Benedikt Putz, and Günther Pernul. 2020. DEALER: decentralized incentives for threat intelligence reporting and exchange. *International Journal of Information Security* (2020). https://doi.org/10.1007/s10207-020-00528-1
[47] Alain Mermoud, Marcus Matthias Keupp, Kévin Huguenin, Maximilian Palmié, and Dimitri Percia David. 2019. To share or not to share: A behavioral perspective on human participation in security information sharing. *Journal of Cybersecurity* 5, 1 (2019), 1–13. https://doi.org/10.1093/cybsec/tyz006
[48] MISP. 2021. COVID-19 MISP Information Sharing Community. Retrieved September 15, 2021 from https://www.misp-project.org/covid-19-misp/
[49] MISP. 2021. MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing. Retrieved September 15, 2021 from https://www.misp-project.org/
[50] Aziz Mohaisen, Omar Al-Ibrahim, Charles Kamhoua, Kevin Kwiat, and Laurent Njilla. 2017. Rethinking Information Sharing for Threat Intelligence. In *Proceedings of the Fifth ACM/IEEE Workshop on Hot Topics in Web Systems and Technologies* (San Jose, California) *(HotWeb '17)*. Association for Computing Machinery, New York, NY, USA, Article 6, 7 pages. https://doi.org/10.1145/3132465.3132468
[51] Sean Oesch, Robert Bridges, Jared Smith, Justin Beaver, John Goodall, Kelly Huffer, Craig Miles, and Dan Scofield. 2020. An Assessment of the Usability of Machine Learning Based Tools for the Security Operations Center. *Proceedings - IEEE Congress on Cybermatics: 2020 IEEE International Conferences on Internet of Things, iThings 2020, IEEE Green Computing and Communications, GreenCom 2020, IEEE Cyber, Physical and Social Computing, CPSCom 2020 and IEEE Smart Data, SmartData 2020* (2020), 634–641. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics50389.2020.00111
[52] Celeste Lyn Paul. 2014. Human-centered study of a network operations center: Experience report and lessons learned. *Proceedings of the ACM Conference on Computer and Communications Security* 2014-November, November (2014), 39–42. https://doi.org/10.1145/2663887.2663899
[53] Desmet Pieter and Hekkert Paul. 2007. Framework of Product Experience. *International Journal of Design* 1, 1 (2007), 57–66. http://www.ijdesign.org/ojs/index.php/IJDesign/article/viewFile/66/7
[54] Andrew Ramsdale, Stavros Shiaeles, and Nicholas Kolokotronis. 2020. A comparative analysis of cyber-threat intelligence sources, formats and languages. *Electronics (Switzerland)* 9, 5 (2020). https://doi.org/10.3390/electronics9050824
[55] Lena Reinfelder, Robert Landwirth, and Zinaida Benenson. 2019. Security managers are not the enemy either. *Conference on Human Factors in Computing Systems - Proceedings* (2019), 1–7. https://doi.org/10.1145/3290605.3300663
[56] Richard M Ryan and Edward L Deci. 2000. Self-Determination Theory and the Facilitation of Intrinsic Motivation, Social Development, and Well-Being. *The American psychologist* 55, 1 (2000), 68–78.
[57] Nader Sohrabi Safa and Rossouw Von Solms. 2016. An information security knowledge sharing model in organizations. *Computers in Human Behavior* 57 (2016), 442–451. https://doi.org/10.1016/j.chb.2015.12.037
[58] Tomas Sander and Joshua Hailpern. 2015. UX Aspects of Threat Information Sharing Platforms: An Examination and Lessons Learned Using Personas. In *Proceedings of the 2Nd ACM Workshop on Information Sharing and Collaborative Security (WISCS '15)*. ACM, New York, NY, USA, 51–59. https://doi.org/10.1145/2808128.2808136 http://doi.acm.org/10.1145/2808128.2808136.
[59] Clemens Sauerwein, Christian Sillaber, Andrea Mussmann, and Ruth Breu. 2017. Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives. *The 13th International Conference on Wirtschaftsinformatik* (2017), 837–851.
[60] Daniel Schlette, Fabian Böhm, Marco Caselli, and Günther Pernul. 2021. Measuring and visualizing cyber threat intelligence quality. *International Journal of Information Security* 20, 1 (2021), 21–38. https://doi.org/10.1007/s10207-020-00490-y
[61] Martin Schrepp. 2019. User Experience Questionnaire Handbook (Version 8). Version 8 (31.12.2019).
[62] Ari Schwartz, Sejal C Shah, Matthew H MacKenzie, Sheena Thomas, Tara Sugiyama Potashnik, and Bri Law. 2016. Automatic threat sharing: how companies can best ensure liability protection when sharing cyber threat information with other companies or organizations. *U. Mich. JL Reform* 50 (2016), 887.
[63] Oscar Serrano, Luc Dandurand, and Sarah Brown. 2014. On the Design of a Cyber Security Data Sharing System. In *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security* (Scottsdale, Arizona, USA) *(WISCS '14)*. Association for Computing Machinery, New York, NY, USA, 61–69. https://doi.org/10.1145/2663876.2663882
[64] Kennon M Sheldon, Andrew J Elliot, Youngmee Kim, and Tim Kasser. 2001. What Is Satisfying About Satisfying Events? Testing 10 Candidate Psychological Needs. *Journal of personality and social psychology* 80, 2 (2001), 325–339.
[65] Florian Skopik, Giuseppe Settanni, and Roman Fiedler. 2017. The Importance of Information Sharing and Its Numerous Dimensions to Circumvent Incidents and Mitigate Cyber Threats. In *Collaborative Cyber Threat Intelligence : Detecting and Responding to Advanced Cyber Attacks at the National Level*, Florian Skopik (Ed.). Auerbach Publishers, Incorporated.
[66] Jessica Staddon and Noelle Easterday. 2019. 'It's a generally exhausting field' A Large-Scale Study of Security Incident Management Workflows and Pain Points. *2019 17th International Conference on Privacy, Security and Trust, PST 2019 - Proceedings* (2019). https://doi.org/10.1109/PST47121.2019.8949012
[67] Borce Stojkovski, Gabriele Lenzini, Vincent Koenig, and Salvador Rivas. 2021. What's in a Cyber Threat Intelligence sharing platform? - Appendix [Data set]. https://doi.org/10.5281/zenodo.5531990
[68] Clare Sullivan and Eric Burger. 2017. "In the public interest": The privacy implications of international business-to-business sharing of cyber-threat intelligence. *Computer Law and Security Review* 33, 1 (2017), 14–29. https://doi.org/10.1016/j.clsr.2016.11.015
[69] Sathya Chandran Sundaramurthy, John McHugh, Xinming Ou, Michael Wesch, Alexandru G. Bardas, and S. Raj Rajagopalan. 2016. Turning Contradictions into Innovations or: How We Learned to Stop Whining and Improve Security Operations. (June 2016), 237–251. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/sundaramurthy
[70] Moin Syed and Sarah C. Nelson. 2015. Guidelines for Establishing Reliability When Coding Narrative Data. *Emerging Adulthood* 3, 6 (2015), 375–387. https://doi.org/10.1177/2167696815587648
[71] Wiem Tounsi. 2019. What is Cyber Threat Intelligence and How is it Evolving? In *Cyber-Vigilance and Digital Trust*. John Wiley & Sons, Ltd, Chapter 1, 1–49. https://doi.org/10.1002/9781119618393.ch1 arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781119618393.ch1
[72] Wiem Tounsi and Helmi Rais. 2018. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers and Security* 72 (2018), 212–233. https://doi.org/10.1016/j.cose.2017.09.001
[73] UEQ. 2021. User Experience Questionnaire. Retrieved September 15, 2021 from https://www.ueq-online.org/
[74] Manfred Vielberth, Fabian Bohm, Ines Fichtinger, and Gunther Pernul. 2020. Security Operations Center: A Systematic Study and Open Challenges. *IEEE Access* (2020), 1–25. https://doi.org/10.1109/ACCESS.2020.3045514
[75] Cynthia Wagner, Alexandre Dulaunoy, Gérard Wagener, and Andras Iklody. 2016. MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform. *Workshop on Information Sharing and Collaborative Security (WISCS)* (2016), 49–56. https://doi.org/10.1145/2994539.2994542 http://dl.acm.org/citation.cfm?doid=2994539.2994542.
[76] Thomas D. Wagner, Khaled Mahbub, Esther Palomar, and Ali E. Abdallah. 2019. Cyber threat intelligence sharing: Survey and research directions. *Computers & Security* 87 (2019), 101589. https://doi.org/10.1016/j.cose.2019.101589

[77] James Igoe Walsh. 2013. Intelligence Sharing. In *Routledge Companion to Intelligence Studies*. Routledge. https://doi.org/10.4324/9780203762721.ch30
[78] Rodrigo Werlinger, Kasia Muldner, Kirstie Hawkey, and Konstantin Beznosov. 2010. Preparation, detection, and analysis: The diagnostic work of IT security incident response. *Information Management and Computer Security* 18, 1 (2010), 26–42. https://doi.org/10.1108/09685221011035241
[79] Ping Zhang and Na Li. 2005. The Importance of Affective Quality. *Commun. ACM* 48, 9 (Sept. 2005), 105–108. https://doi.org/10.1145/1081992.1081997
[80] Adam Zibak and Andrew Simpson. 2019. Cyber threat information sharing: Perceived benefits and barriers. *ACM International Conference Proceeding Series* (2019). https://doi.org/10.1145/3339252.3340528

A APPENDIX - DATA

The surveys and datasets with raw participant responses from the studies can be downloaded from the following link: https://doi.org/10.5281/zenodo.5531990 [67].

B APPENDIX - GROUP COMPARISON TESTS

As indicated in Section 5.2.3, the following tests report on the differences found in the UEQ evaluation of MISP based on the demographic characteristics of our study participants.

Role. A statistically significant difference in the UEQ evaluation of MISP was observed in the *Dependability* and *Stimulation* scales between users that reported multiple roles and users that reported a single role in terms of how they (intend to) use MISP.

Dependability: $(M_{mul} - M_{sin})$ = 1.80 − 1.40 = 0.40, 95% CI [0.11, 0.69], d = 0.75, 95% CI [0.20, 1.29]; $t(62)$ = 2.78, p = .007.

Stimulation: $(M_{mul} - M_{sin})$ = 2.19 − 1.75 = 0.44, 95% CI [0.08, 0.79], d = 0.67, 95% CI [0.12, 1.21]; $t(62)$ = 2.47, p = .016.

Industry. Participants who indicated working for an ICT consulting/advisory company, expressed significantly lower UEQ scores regarding the platform's *Attractiveness*, *Perspicuity*, and *Efficiency* in comparison to those working in other industries.

Attractiveness: $(M_{cons} - M_{oth})$ = 1.20 − 1.77 = -0.57, 95% CI [-1.02, -0.12], d = -0.72, 95% CI [-1.29, -0.15]; $t(62)$ = -2.54, p = .013.

Perspicuity: $(M_{cons} - M_{oth})$ = -0.13 − 0.74 = -0.87, 95% CI [-1.50, -0.23], d = -0.78, 95% CI [-1.34, -0.20]; $t(62)$ = -2.74, p = .008.

Efficiency: $(M_{cons} - M_{oth})$ = 0.853 − 1.596 = -0.74, 95% CI [-1.17, -0.31], d = -0.98, 95% CI [-1.56, -0.40]; $t(62)$ = -3.47, p = .001.

Experience. The planned contrast between study participants that had used MISP for less than one year (*novice* users) and those that had used MISP for more than one year (*experienced* users) suggests that the latter group finds MISP more *stimulating*.

$(M_{exp} - M_{nov})$ = 2.3 − 1.81 = 0.49, 95% CI [0.02, 0.96], d = 0.73, 95% CI [0.35, 1.42]; $t(58)$ = 2.105, p = .04.

Use of Training materials. The platform's *dependability* and *stimulation* were the two UX aspects evaluated significantly higher among participants that had used the MISP training materials before in comparison to those that had never used them.

Dependability: $(M_{yes} - M_{no})$ = 1.78 − 1.37 = 0.41, 95% CI [0.14, 0.68], d = 0.78, 95% CI [0.25, 1.30]; $t(62)$ = 3.001, p = .004.

Stimulation: $(M_{yes} - M_{no})$ = 2.21 − 1.69 = 0.51, 95% CI [0.18, 0.84], d = 0.80, 95% CI [0.28, 1.33]; $t(62)$ = 3.114, p = .003.

Use of PyMISP. The planned contrast between study participants that had used the PyMISP API and those that had not, revealed a statistically significant difference regarding three UX aspects. The results denote that participants with PyMISP experience gave lower scores across all three aspects, namely:

Attractiveness: $(M_{yes} - M_{no})$ = 1.09 − 1.77 = -0.68, 95% CI [-1.31, -0.05], d = -0.83, 95% CI [-1.6, -0.06]; $t(38)$ = -2.191, p = .035.

Efficiency: $(M_{yes} - M_{no})$ = 0.86 − 1.52 = 0.66, 95% CI [-1.21, -0.10], d = -0.90, 95% CI [-1.67, -0.13]; $t(38)$ = -2.384, p = .022.

Novelty: $(M_{yes} - M_{no})$ = 0.72 − 1.48 = -0.75, 95% CI [-1.30, -0.21], d = -1.07, 95% CI [-1.84, -0.28]; $t(38)$ = -2.816, p = .008.

Cloning a MISP repo. The planned contrast between study participants that had cloned a MISP repository and those that had not, revealed a statistically significant difference in the evaluation of the platform's *dependability*.

Dependability: $(M_{yes} - M_{no})$ = 1.73 − 1.37 = 0.36, 95% CI [0.01, 0.70], d = 0.71, 95% CI [0.26, 1.39]; $t(38)$ = 2.107, p = .042.

No statistically significant differences were observed following planned contrasts between participants split according to the following characteristics: age, education, frequency of use of MISP, and use of the MISP virtual machines.

C APPENDIX - TABLES

Table 4: Participant demographics.

N	Demographic	Count	Percent
74	Gender		
	• *Female*	2	2.7 %
	• *Male*	70	94.6 %
74	Age group		
	• *18–25*	11	14.9 %
	• *26–35*	32	43.2 %
	• *36–45*	27	36.5 %
	• *46–55*	4	5.4 %
73	Education		
	• *Less than a Bachelor's degree*	10	13.7 %
	• *Bachelor's degree*	32	43.8 %
	• *Master's degree*	28	38.4 %
	• *Doctoral degree*	3	4.1 %
74	Engineering or Tech Background	66	89.2 %
74	Role (multiple possible)		
	• *Security Analyst*	53	71.6 %
	• *Intelligence Analyst*	25	33.8 %
	• *Malware Researcher*	14	18.9 %
	• *Risk Analyst*	13	17.6 %
	• *Law Enforcement*	3	4.1 %
	• *Academic Researcher*	3	4.1 %
	• *Fraud Analyst*	2	2.7 %
	• *Other*	5	6.7 %
74	Industry (multiple possible)		
	• *ICT Consulting/Advisory*	20	27.0 %
	• *National or Governmental CSIRT*	12	16.2 %
	• *Telecommunications*	9	12.2 %
	• *Bank*	8	10.8 %
	• *Software company*	7	9.5 %
	• *Public Health*	6	8.1 %
	• *Military*	3	4.1 %
	• *Other*	12	16.2 %
74	Prior experience with MISP		
	• *I have never used MISP before*	18	24.3 %
	• *Less than 1 month*	11	14.9 %
	• *1 – 6 months*	18	24.3 %
	• *6 – 12 months*	10	13.5 %
	• *1 – 2 years*	6	8.1 %
	• *More than 2 years*	11	14.9 %
52	MISP usage frequency		
	• *Less than once a week*	11	21.2 %
	• *Between 1 and 3 times per week*	19	36.5 %
	• *Between 3 times per week & every day*	11	21.2 %
	• *Every day*	11	21.2 %
74	Previously attended a MISP training	13	17.6 %
74	Previously used MISP training materials	33	44.6 %
74	Previously used MISP virtual machines	33	44.6 %

Table 5: Overview of the UEQ evaluation of MISP, mean values per scale item

Item	Mean	Variance	Std. Dev.	No.	Left	Right	Scale
1	1.6	1.2	1.1	63	annoying	enjoyable	Attractiveness
2	1.1	1.6	1.3	63	not understandable	understandable	Perspicuity
3	1.3	1.7	1.3	64	creative	dull	Novelty
4	0.4	2.1	1.4	64	easy to learn	difficult to learn	Perspicuity
5	2.3	0.9	1.0	63	valuable	inferior	Stimulation
6	1.4	1.2	1.1	64	boring	exciting	Stimulation
7	2.2	0.7	0.9	64	not interesting	interesting	Stimulation
8	0.8	1.2	1.1	64	unpredictable	predictable	Dependability
9	1.1	1.4	1.2	64	fast	slow	Efficiency
10	1.2	1.0	1.0	64	inventive	conventional	Novelty
11	1.8	0.7	0.8	64	obstructive	supportive	Dependability
12	2.4	0.7	0.9	64	good	bad	Attractiveness
13	-0.3	1.9	1.4	64	complicated	easy	Perspicuity
14	1.4	0.8	0.9	64	unlikable	pleasing	Attractiveness
15	1.5	1.1	1.1	64	usual	leading edge	Novelty
16	1.6	0.9	0.9	64	unpleasant	pleasant	Attractiveness
17	1.6	1.0	1.0	64	secure	not secure	Dependability
18	1.7	0.9	1.0	63	motivating	demotivating	Stimulation
19	1.9	0.6	0.7	63	meets expectations	does not meet expectations	Dependability
20	1.6	1.1	1.0	64	inefficient	efficient	Efficiency
21	0.8	2.1	1.4	64	clear	confusing	Perspicuity
22	1.5	1.4	1.2	64	impractical	practical	Efficiency
23	1.3	2.1	1.4	63	organized	cluttered	Efficiency
24	1.2	2.6	1.6	64	attractive	unattractive	Attractiveness
25	1.4	2.1	1.4	64	friendly	unfriendly	Attractiveness
26	1.5	1.3	1.2	64	conservative	innovative	Novelty

Table 6: Comparison of the MISP results to a general UEQ benchmark (452 product evaluations)

Scale	Mean	Comparison to general benchmark	Interpretation
Attractiveness	1.62	Good	10% of results better, 75% of results worse
Perspicuity	0.51	Bad	In the range of the 25% worst results
Efficiency	1.40	Above average	25% of results better, 50% of results worse
Dependability	1.52	Good	10% of results better, 75% of results worse
Stimulation	1.89	Excellent	In the range of the 10% best results
Novelty	1.36	Good	10% of results better, 75% of results worse

Table 7: Comparison of the MISP results to a UEQ benchmark of websites and web services (85 product evaluations)

Scale	Mean	Comparison to specialized benchmark	Interpretation
Attractiveness	1.62	Good	10% of results better, 75% of results worse
Perspicuity	0.51	Bad	In the range of the 25% worst results
Efficiency	1.40	Above average	25% of results better, 50% of results worse
Dependability	1.52	Above average	25% of results better, 50% of results worse
Stimulation	1.89	Excellent	In the range of the 10% best results
Novelty	1.36	Excellent	In the range of the 10% best results