

Work in Progress: A preliminary user experience evaluation of MISP

Anonymous Authors

1 Introduction

MISP is an open source threat intelligence platform used by more than 6000 organizations worldwide, ranging from NATO to national CSIRTs and private sector actors [1]. Conceived within military circles as a malware information sharing platform, the project has in the meantime matured into a community-driven project for gathering, sharing and correlating diverse threats e.g. indicators of compromise (IoC), financial fraud information or counter-terrorism information [1, 7]. The project is co-financed and resource-wise supported by CIRCL, the Computer Incident Response Center Luxembourg, which operates a number of MISP instances comprising over 950 organizations with more than 2400 users [2].

As a technically-advanced information sharing platform that caters for a diverse set of security information workers with distinct needs and objectives, MISP has to pay an equal amount of attention to the user experience in order to maximize and optimize the amount of threat information that is contributed and consumed by the different user groups. As highlighted by [6] attending to the UX design and human motivations is paramount to the success of a threat information sharing platform. Here, we present the first step of our ongoing research that aims to quantify and qualify the user experience of MISP.

2 Methodology

Interested in how MISP users evaluate the usability and user experience of the platform i.e. how they perceive both the pragmatic and hedonic qualities of the system, we administered i) a User Experience Questionnaire (UEQ), ii) a Demographics questionnaire, and iii) a System Usability Scale (SUS) questionnaire to 50 attendees at the end of a 2-day training session on MISP, organized by CIRCL in March 2019.

3 Participants

Out of the 50 participants, 25 (24 male, 1 female) filled out and returned the questionnaires. 20 of them (80%) had an engineering or computer science background. 19 of them had a Bachelor's degree or higher. 12 (48%) were in the age span of 26 - 35 years. In terms of prior experience with MISP, the largest subgroup (32%) consisted of those that had used MISP 1 - 6 months. 18 participants (72%) would best describe their role as Security analysts. The most represented subgroup in terms of industry was banking with 6 participants (24%). While it was the first training session for all attendees, over 50% of the them had used the training materials or MISP virtual machine prior to the training.

4 Results

UEQ contains 6 scales with a total of 26 items, investigating the attractiveness, perspicuity, efficiency, dependability, stimulation and novelty of interactive products [5]. Based on 24 UEQ responses, MISP was positively evaluated along all scales except for perspicuity. Comparing the mean values (1.611, 0.681, 1.448, 1.583, 1.906, 1.448, respectively) against benchmark values provided with the UEQ analysis tools [3] we can see that MISP scores well along the non-goal directed, hedonic aspects, such as stimulation, where it is in the range of 10% best results. On the other hand, when it comes to how easy it is to learn the system, MISP is among the 25% worst results. Based on 22 SUS responses, the raw SUS score for MISP is 64.5, which generally is considered to be below average.

5 Future work

Using mixed methods, we are motivated to further identify and qualify the presence of usability and UX issues, in particular with respect to the different types of information security workers using MISP.

References

- [1] MISP - Malware Information Sharing Platform and Threat Sharing - The Open Source Threat Intelligence Platform. <https://www.misp-project.org/>. Accessed 2019-05-31.
- [2] MISP - Malware Information Sharing Platform and Threat Sharing - Training Materials. <https://www.circl.lu/services/misp-training-materials/>. Accessed 2019-05-31.
- [3] User Experience Questionnaire. <https://www.ueq-online.org/>. Accessed 2019-05-31.
- [4] John Brooke. *"SUS-A quick and dirty usability scale."* *Usability evaluation in industry*. CRC Press, 1996. ISBN: 9780748404605.
- [5] Bettina Laugwitz, Theo Held, and Martin Schrepp. Construction and Evaluation of a User Experience Questionnaire. In Andreas Holzinger, editor, *HCI and Usability for Education and Work*, pages 63–76, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.
- [6] Tomas Sander and Joshua Hailpern. 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*, pages 51–59, New York, NY, USA, 2015. ACM. <http://doi.acm.org/10.1145/2808128.2808136>.
- [7] Cynthia Wagner, Alexandre Dulaunoy, Gérard Wagener, and Andras Iklody. MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform. *Workshop on Information Sharing and Collaborative Security (WISCS)*, pages 49–56, 2016. <http://dl.acm.org/citation.cfm?doid=2994539.2994542>.