ITEC 2019
ITEC Extended Abstract Template

SAND2018-14130C
Presentation/Panel

Human Factors Approach to Cyber Analyst Training

S. S. Adams, E. S. Fleming, S. M. Heiden and L. Kittinger
Sandia National Laboratories, Albuquerque, NM, USA
smsteve@sandia.gov

Abstract — A prominent global security threats lies in the cyber realm. To address the cybersecurity threat, a tool was developed to help novice cybersecurity analysts identify the most pertinent risks. The existing training program for the tool did not sufficiently address end-users' knowledge gaps. Thus, it was necessary to properly scaffold evidence-based training materials to support novices' needs at various stages of their learning, which was the goal of the current work. Many challenges and constraints influenced how the training was developed, which included: limited access to end-users (novice cybersecurity analysts); end-users from a variety of organizations and cultural backgrounds; end-users separated by location and time from each other and the design team; a tool that constantly changed throughout the design process; and the need for training materials to serve as both instructor-led course materials and post-training reference materials. This paper discusses how human factors approaches were applied to address the aforementioned challenges and constraints.

1 Introduction and Background

A prominent global security threats lies in the cyber realm [1]. To address the cybersecurity threat, a tool was developed to help novice cybersecurity analysts identify the most pertinent risks in internet traffic. The existing training program for the tool did not sufficiently address the end-users' knowledge gaps. Thus, it was necessary to properly scaffold evidence-based training materials to support novices' needs at various stages of their learning, which was the goal of the current work.

This work describes the development of a cohesive training program for novice cybersecurity analysts. Many challenges and constraints influenced how the training was developed, which included: limited access to end-users (novice cybersecurity analysts); end-users from a variety of organizations and cultural backgrounds; end-users separated by location and time from each other and the design team; a tool that constantly changed throughout the design process; and the need for training materials to serve as both instructor-led course materials and post-training reference materials. In this paper we describe our technical approach to designing the training and lessons learned from this project. Finally, we summarize our key takeaways and outline future continued work in this arena.

2 Technical Approach and Methods

The training design approach used an integration of human factors methods and educational design approaches, including expert elicitation, ethnographic observation, task analysis, heuristic evaluations, and iterative design. Expert elicitation includes obtaining relevant knowledge from experts about the tasks that they perform and the decisions that they make [2]. The team talked with dashboard designers to gain insight into specific features of the dashboard and how analysts might use those features. Ethnographic observation involves observing users in their natural work environment in order to understand 'things" from their perspective. As such, the team observed five expert cybersecurity analysts to understand how they performed their job and tasks from their perspective. Task analysis involved asking the expert cybersecurity analysts to explain step-by-step how they perform specific tasks [3]. The team paired this with a think-aloud protocol, in which the expert cybersecurity analysts were asked to talk aloud while they performed a given task. A heuristic evaluation consists of comparing a website or tool's format, structure and function to industry-identified 'best practices' [4]. The team performed a heuristic evaluation of the training tool and provided recommendations based on these 'best practices' principles. Finally, iterative design entailed designing the training curriculum, testing it, and then redesigning using observations and metrics gained from the testing stages. The continuous evaluation of training allowed the human factors team to better meet the needs of the users.

When available, designers immersed themselves in a training course administered prior to incorporating updates to the training. These ethnographic participant observations [5] allowed the design team to identify gaps in content and students' points of confusion.

Learning objectives for the training program were defined via analysis of previously-developed training materials and expert elicitations; then the program was scaffolded into multiple intervention types to address the varying levels of content presented. The intervention types included static slides, videos, interactive modules, embedded quizzes, and self-guided tool exploration. The training modules were delivered in a format that allowed the materials to be compatible across organizations and be accessible to students without special software.

3 Lessons Learned

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

The team faced several issues throughout the design process, including: 1) limited access to end-users; 2) dynamically changing tool; and 3) training format limitations. We address each of these separately.

3.1 Limited access to end-users

First, end users are often not technical, are geolocated around the world, and work for various organizations. Lack of access limited obtaining feedback on the usefulness of design changes. To address end-users' perspectives, the design team relied on their experiences on being new to the tool's terminology and functionality, as well as expert elicitation from cybersecurity professionals. If the design team had questions or points of confusion, it was assumed that the non-technical end users would as well. Expert elicitations extracted content details and usability issues. Sessions sometimes included recording the tool interface while the cybersecurity expert talked through task steps and rationale. The data were used to develop case scenarios.

3.2 Dynamically changing tool

The tool was constantly updated throughout training design. Most updates were minor; but one major update altered the tool's interface substantially. The changes affected not only what the user would see, but in some cases, how they would interact with the new system to accomplish tasks. Since the change took place towards the end of the design phase, the decision was made to finalize the training using the old interface, with future work entailing updating to the new interface.

3.3 Training format limitations

Finally, end-users were located within different organizations with different technical platforms, which limited software options for creating and delivering the training. This also meant users would be accessing the training at different times or days, especially if students were accessing the materials as post-training reference matter. The team chose common office processing tools, such as PowerPoint, which was accessible to all users.

4 Take-Aways and Future Work

The cybersecurity efforts are only as effective as the analysts responsible for managing those attacks, so comprehensive training is key. This project demonstrates how to build effective training using a holistic approach to understand the perspectives of end-users and experts. This training impacts diverse individuals from a variety of organizations who are new to the cybersecurity domain. The use of human factors methods supports and enables effective training design by giving designers insight to users' knowledge gaps, even with limited access to those users and with updates to the tool. Probing experts throughout the design process facilitated effective breakdown of complex information. The resulting training program design and scaffolding could be used for future courses with similar objectives. Future steps include: a workbook to support activity-based training, and improved feedback loops to better evaluate training materials and delivery.

References

[1] Coats, D.R. (2017). Worldwide Threat Assessment of the US Intelligence Community. Washington, DC, USA.

[2] O'Hagan, T., et al. (2006) *Uncertain Judgements: Eliciting Experts' Probabilities.* John Wiley & Sons Ltd, West Sussex, England.

[3] B. Kirwan, L. Ainsworth, A Guide to Task Analysis, (1992).

[4] J. Nielsen, H. Loranger, Prioritizing Web Usability (2006).

[5] DeWalt, K. M., & DeWalt, B. R. (2011). Participant Observation: A Guide for Fieldworkers. Lanham, MD: AltaMira Press.

Acknowledgements

This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Author/Speaker Biographies

Dr. Susan S. Adams is a Principle member of the Human Factors Department at Sandia National Laboratories. She obtained her degrees in Cognitive Psychology from the University of New Mexico. Her research interests include memory, team performance and decision making.

Dr. Elizabeth S. Fleming is a Senior member of the Human Factors Department at Sandia National Laboratories. She obtained her degrees in Aerospace Engineering from Georgia Tech. Her research interests include systems engineering, multidisciplinary engineering decision-making, team science, and data analysis.

Dr. Siobhan M. Heiden is a Senior member in the Human Factors Department at Sandia National Laboratories. She earned her degrees in Industrial Engineering from California Polytechnic State University (BS) and Purdue University (MS, PhD). Her research interests include process and systems analysis and design, and knowledge management.

Liza Kittinger is a Technical Systems Analyst at Sandia National Laboratories. She has a Master's degree in Industrial Psychology from the University of West Florida,

and is a Ph.D. student at the University of New Mexico. Her research interests include training, technology adoption, and social networks.