Human Factors Approach to Cyber Analyst Training

Susan Adams, Elizabeth Fleming, Siobhan Heiden and Liza Kittinger

Presented by: Elaine Raybourn

Sandia National Laboratories, United States of America

The Team

Susan Adams, PhD
Principal technical staff member

Specializations: Experimental design, task analysis, decision making

Scottie Fleming Lindsley, PhD
Senior technical staff member

Specializations: Engineering design processes, collaborative decision making

Siobhan Heiden, PhD
Senior technical staff member

Specializations: Process and systems analysis and design, knowledge management

Liza Kittinger, MA
Technical staff member

Specializations: Training, technology adoption, organizational development

Sandia's Cyber Mission Area

Sandia's research efforts in cybersecurity are focused in three broad areas:

1. Trusted hardware, software, and systems;
2. Networks and systems architectures and analysis; and
3. Effective cyber defense systems

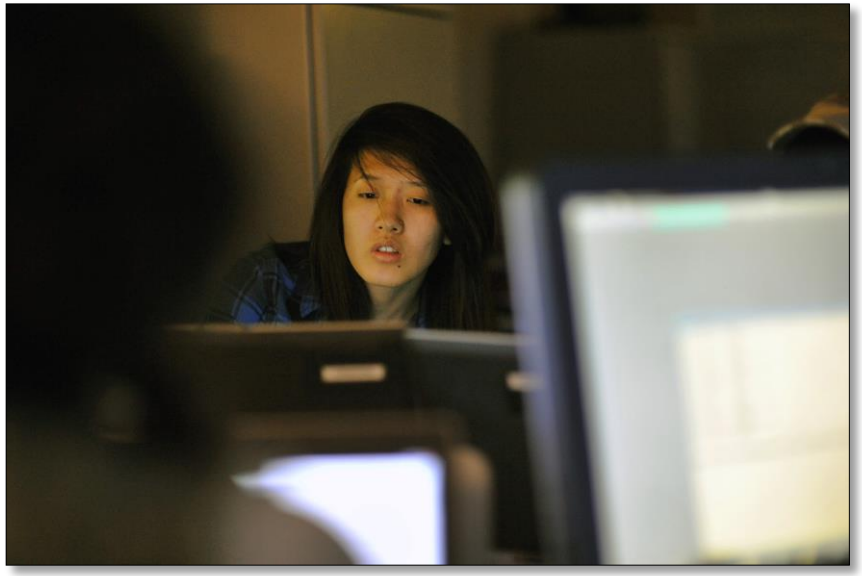
Sandia built a network intrusion detection tool that helps cyber analysts detect:

- Cyber attacks
- Data exfiltration
- System compromise
- Data manipulation
- Insider threat

Background

Motivation: Current training for tool to help cyber analysts' identify pertinent risks did not sufficiently address their knowledge gaps

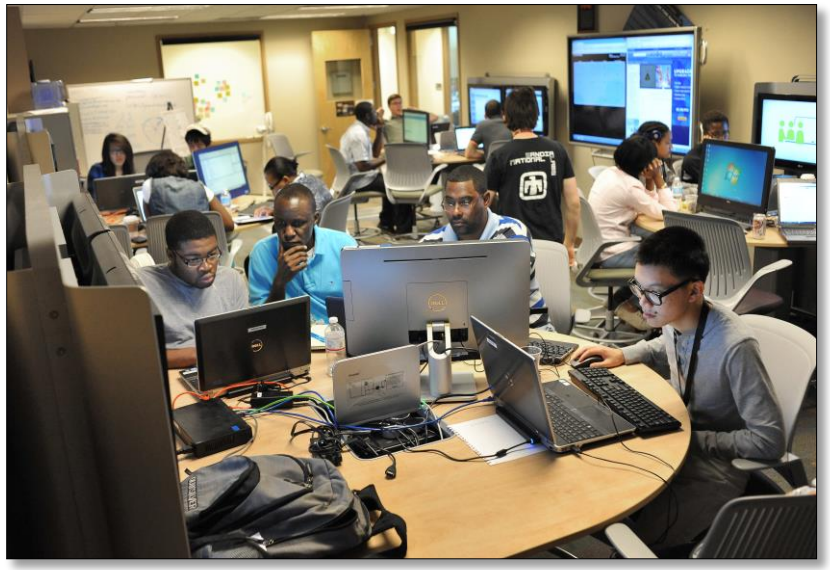
Goal: Create evidence-based training materials to support novice cyber analysts' needs at various stages of their learning



Source: Sandia Labs (CC BY-NC-ND 2.0)

Challenges

- Limited access to end-users (i.e., cyber 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
- Tool is constantly updated and modified
- Need for both instructor-led training and post-training reference materials



Source: Sandia Labs (CC BY-NC-ND 2.0)

Human Factor Approaches Used

Expert Elicitations

Definition: A process of obtaining judgements and knowledge from experts to a particular problem or scenario

Approach

Select Experts	Refined Issues	Explained the Context	Elicitation
•Engineers and designers of the tool	•Focused on issues of learning and usability •for the end user	•Described the purpose of the meeting and expected outcomes	•Used task-oriented exercises with standardized question sets to elicit their conceptual understanding, technical reasoning, and mental organization of the information most relevant for solving a particular issue.

Findings

- Understand the decisions and reasons for solving particular cyber issues
- Identify commonalities and differences expert analysts might take
- Begin identifying locations where scaffolding would be appropriate

Task Analysis

Definition: A process of breaking a job task into smaller parts

Approach

- Used a general task analysis method where we focused on identifying the relationships one task had with another task in addition to terminology used
- Think-Aloud-Protocol: Experts were asked to talk while performing a given task

Findings

- Allowed for the design team to observe aspects of the analyst's behavior with various levels of detail and at various stages of the task
- Allowed the design team to understand sequential steps in completing tasks

Attribution

Heuristic Evaluation

Definition: An analysis of the computer interface to ensure it is "user friendly"

Approach

- Used usability standards to evaluate how easy the interface was to use
- Considerations were given around: learnability, efficiency, memorability, errors and satisfaction

Findings

- Results and recommendations for modern tool enhancements were given to developers (e.g. interface organization, features, search, etc.)
- Interface limitations influenced some aspects of how team designed training

Ethnography: Participant Observation

Definition: A strategy of observation and direct participation to understand the trainee's perspective

Approach

- Participated in training sessions similar to an end user of the tool
- Completed readings and exercises a new analyst would experience
- Tried triaging cyber issues the way a new analyst is expected to do

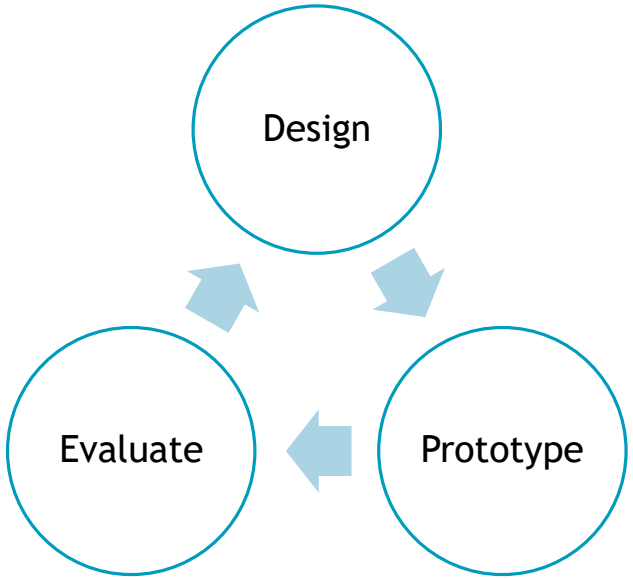
Findings

- Identified gaps in the learning process and where information became too advanced too quickly
- Identified assumptions instructors had of their students

Iterative Design

Definition: A method of prototyping, testing, analyzing and refining, then restarting the process.

- Non-linear process which involved continuous evaluation and feedback from users and designers to identify opportunities for improvement
- Training was updated multiple times



Lessons Learned

- Understanding the end user is key to any training design
- Experts in the field are great resources, but effort is needed to scale down their level of knowledge to be appropriate for novice learners
- Anticipate small and big changes to software to occur throughout the development of training

Conclusions

- Designing a learning program takes time
- Some enhancements suggested by Human Factors may be beyond the scope of training (e.g., tool functionality)
- The "ideal situation" is not always realistic – constraints, barriers and changes are inherent
- Feedback and evaluation are key to a successful training program
- Partnering with experts who were accessible was crucial to our success

Acknowledgements

Special thanks to the subject matter experts who participated in the design and development of this training.

This presentation 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 multi-mission laboratory managed and operated by National Technology and 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. SAND2019-5167 C.

Questions?

Susan Adams – smsteve@sandia.gov