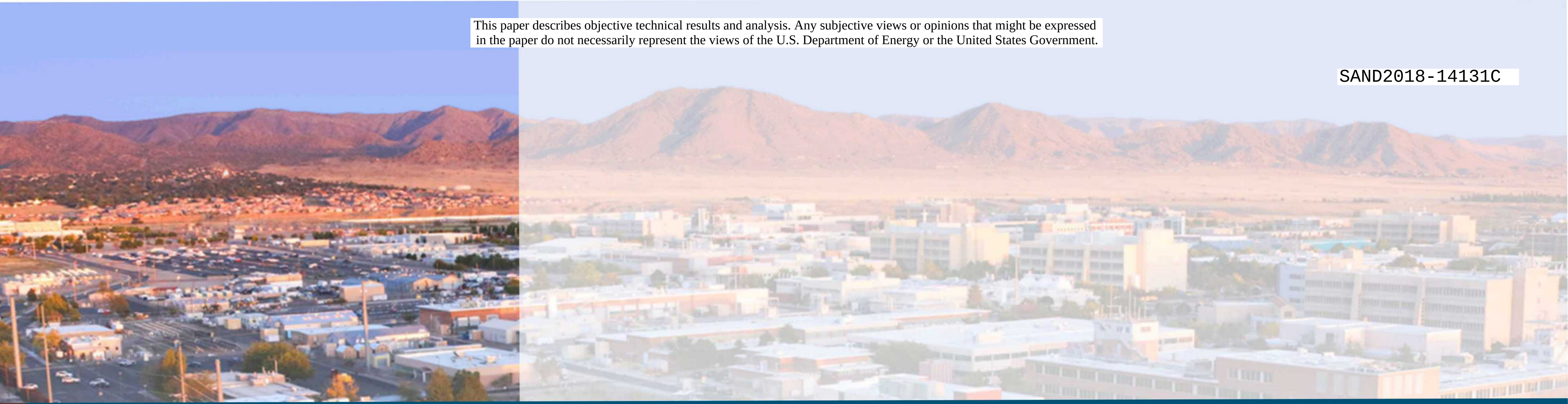
This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2018-14131C



Human Factors Approach to Cyber Analyst Training

Susan Adams, Elizabeth Fleming, Siobhan Heiden and Liza Kittinger

Sandia National Laboratories

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.

Background

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

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

Challenges

Limited access to end-users

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

Human Factor Approaches Used

Expert Elicitations

Task Analysis

Heuristic Evaluations

Ethnographic Observations

Iterative Design

Expert Elicitations

Approach

- Selected our experts: Engineers and designers of the tool
- Refined issues: Focused on issues of learning and usability for the end user
- Explained the context: Described our purpose for the meeting and expected outcomes
- Elicitation: 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 allowed the design team to:

- 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

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

Heuristic Evaluation

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 were given to the tool's point of contacts
- Note: Our design team had little influence on what would be implemented, only that our recommendations would enable an analyst to learn the tool faster and be more effective at their job.
- Interface limitations influenced some aspects of how we designed training

Ethnography: Participant Observations

Approach

- Participated in training sessions as though we were the 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

- More data and information that allowed the design team to identify gaps in the learning process, where information became too advanced too quickly, helped identify assumptions instructors had of their students

Iterative Design

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

The "ideal situation" is not always realistic – constraints, barriers and changes are inherent

Feedback and evaluation are key to a successful training program

Acknowledgements

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 multimission 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.