Determining System Requirements for Human-Machine Integration in Computer Security Incident Response

Megan Nyre-Yu
School of Industrial Engineering
Purdue University

Barrett S. Caldwell, PhD
School of Industrial Engineering
Purdue University

Incident response teams in cyber defense (CSIRTs) play a critical role in mitigating security events. Advancement in the field requires integrating approaches from social and behavioral sciences to better understand the humans in the system. This research investigates incident response (IR) tasks and the humans that perform them, and uses Human Factors methods to determine functional requirements for possible automated solutions. Findings presented in a systems engineering language will inform algorithmic development from other scientific fields currently addressing cyber defense with computational methods.

SUMMARY

PROBLEM

CYBER SECURITY IS A TOP GLOBAL THREAT¹ WITH MANY NEGATIVE INFLUENCERS

Current approaches to addressing these issues lack expertise in other areas, which limits effectiveness, validity, and generalizability of solutions.

There’s a skills gap being approached in two different (and ineffective) ways.

There’s a gap between current security science research and social and behavioral sciences. ²

BACKGROUND

Computer Security Incident Response Teams (CSIRTs) provide critical defense to companies, organizations, and countries.

CSIRTs vary in roles and expertise
Team structures vary greatly across cyber organizations
CSIRTs may perform many different services, including incident handling

Incident response is knowledge work; expertise is central to doing the job
Information sharing is a key aspect of incident response
Automation roles in incident response are not well understood

This exploratory research aims to identify the current state of expertise and automation in CSIR handoffs, determine gaps as requirements for future state automated solutions, and translate findings into actionable items.

PROPOSED METHODOLOGY

1 OBSERVATIONAL FIELD STUDIES / INTERVIEWS

- 3-4 DIFFERENT CSIRTS
- 40 HOURS PER CSIRT
  - Document context and environment
  - Identify critical information handoffs in IR
  - Map handoff process steps
  - Map information flows for handoffs
  - Identify struggle points within handoffs

2 COGNITIVE TASK ANALYSIS INTERVIEWS

- 4-6 EXPERTS 2 HOURS PER INTERVIEW
  - Identify points in IR that require expertise
  - Identify expertise areas needed for IR handoffs
  - Identify common scenarios
  - Identify cues and strategies for navigating

3 KNOWLEDGE ASSET MAPPING SURVEYS

- 3-4 CSIRTS (SAME AS STUDY 1)
  - Determine subjective expertise by area
  - Determine where certain expertise can be found on each team
  - Determine key differences across teams
  - Determine knowledge sharing patterns

4 SYSTEM REQUIREMENTS & FUNCTIONAL ARCHITECTURE

- Capture context, environment, human-driven automation needs
- Target critical handoffs & struggle points
- Convert the process / information flows to software requirements

PROCESS MODEL
  - Process flow per handoff
  - Information flow per handoff
DATA MODEL
  - Information needed per scenario
  - Existing information sources
RULE MODEL
  - Conditions per scenario
  - Cues and strategies per scenario

IMPAKT

Provides rich context and insights about CSIRTs, how they differ; Automation opportunities by team
Lays groundwork to address a major gap between Computer Science and Behavioral/Social Science
Translates findings of qualitative research into actionable results for system designers / developers
Provides methodology for additional work in InfoSec, as well as human-automation collaboration in general