Title: Studying Usability of Expert Cybersecurity Tools

Program: OUR

Student Author(s): Toya Okey-Nwamara

Faculty Mentor(s): Prakruthi Reddy, Cori Faklaris

College: College of Computing and Informatics

According to the Verizon Data Breach Investigation Report, 68% of data breaches involved a person falling victim to a social engineering attack (What Is Social Engineering? | Definition, n.d.). According to the Cambridge Dictionary, a social engineering attack is an attempt to trick people into giving secret or personal information, especially on the internet, and using it for harmful purposes. These harmful purposes include phishing, scamming, hacking, information stealing, etc. Security experts need tools to easily analyze these attacks, known as digital forensics and incident response (DFIR). However, past research has shown that many such tools are unusable by novices and difficult for experts to use. This affects the productivity of DFIR professionals ranging from security analysts to law enforcement officers. Our research addresses this situation by gathering insights into the challenges faced by DFIR professionals and the requirements for improving their usability. In this first study, we interview DFIR professionals and review the current literature. Work to date includes compiling and analyzing prior works, recruiting and talking with twenty-five DFIR professionals on Zoom, and cleaning up and analyzing the resulting transcripts. The insights gained from our literature grid and interviews will inform a research agenda that aims to improve the usability of DFIR tools. This

will aid in developing better heuristics for the design of these tools, ultimately enhancing the efficiency and effectiveness of DFIR professionals in analyzing cybersecurity attacks.