Visualization for Cyber Security and Security Analysts' Use of Visualizations: Is There a Gap?

Noëlle Rakotondravony* Lane Harrison†

Worcester Polytechnic Institute

ABSTRACT

Many research threads in visualization for cybersecurity aim to equip practitioners with novel visualization techniques and systems to facilitate the exploration and analysis of data in their organizations. It is not clear, however, the extent to which security practitioners are directly or indirectly benefiting from current research efforts in data visualization and visualization for cybersecurity. To explore this question, we propose an interview study protocol, adapted from previous works that identified gaps and opportunities between visualization research and practitioner workflows and tools. Our interview targets security practitioners who use visualizations as part of their daily work, focusing on considerations behind their visualization-related choices, preferences, and constraints within their organizations. Initial results from a pilot study with this protocol suggest that organizational constraints and specific technical properties of novel visualization tools might discourage analysts from adopting newer visualization practices, techniques, and systems. We conclude with our plans for refining the current interview protocol and expanding the study population and findings.

Index Terms: Data—Visualization—Analysis—

1 INTRODUCTION

Security visualization tools help security analysts in different areas explore their data in more effective ways and achieve their tasks faster. For example, *APT-hunter* [9] helps security analysts detect malicious logins in an enterprise by visualizing patterns from login data. The tool *OwlSight* [2] offers large companies a platform for real-time detection of cyber threats and attacks that affect organizations, through the analysis of real-time alerts from multiple sources and insightful visualizations. In many cases, researchers involve the target end-users, security analysts, during design, prototyping, development, and evaluation phases to guarantee better adequacy and effectiveness of the proposed visualization tools and techniques.

While security analysts rely more and more on visualizations in their daily tasks, little is known about how the tools, techniques, or prototypes are adopted within the workflow of practitioners. It is difficult to evaluate to what extent security analysts are directly or indirectly benefiting from the research community's efforts. In the visualization for data science field, researchers worked with data science practitioners to identify future directions for addressing the *visualization gap*. The *visualization gap* in data science is characterized by the research community believing that advanced visualizations will improve data science workflows whereas data scientists using visualizations mostly only for disseminating results [1, 8].

In this poster, we propose an interview study protocol to explore possible gaps similar to the "visualization gap" in the cybersecurity visualization domain. We adapt protocols from previous interviews by Kandel *et al.* [6] and Hong *et al.* [5] to identify comparable trends in the adoption of data visualization tools and techniques by security analysts within their organizations. Direct exchanges with practitioners help understand the constraints and challenges arising from their tasks or organizational contexts that impede their choice of data visualization tools and techniques, and thus helping future research address important needs through realistic and practical solutions.

*e-mail: ntrakotondravony@wpi.edu

†e-mail: ltharrison@wpi.edu

2 MOTIVATION AND BACKGROUND

Reflecting on the extent to which targeted users benefit directly or indirectly from research results is essential to measure the impact of scientific research. In the visualization and data science community, interviews with analysts have allowed researchers to develop a better understanding of the practical use of visualization within their actual organizational contexts [6]. Recent studies that addressed the "interactive visualization gap" [1] also helped researchers come up with different design suggestions towards better integration of interactive visualization techniques in data science workflows [8].

In the cybersecurity visualization field, recent user-centered design methodologies have helped create visualization tools that could be successfully deployed to the target users [7], and help security experts and cyber operators answer analytic questions from real-world scenarios they work in [3]. Evaluation studies identified the trends in evaluation methodologies and provided an understanding of how the effectiveness of the cybersecurity visualization techniques, systems, models, and tools that are proposed is measured in the research community [10]. Although such works are important to highlight trends and future directions for building effective tools, they do not allow to estimate how research results and techniques find their applications in real-world settings.

In our study, we aim to gain an overview of the uptake and uses of proposed visualization systems and techniques beyond the publication and prototyping phases. Our work is based on prior studies in the visualization field that analyze analysts' ecosystems from a variety of sectors to understand the impact of their organizations on the visualization processes. We adapt Kandel *et al.* [6]'s interview protocol to the cybersecurity domain and target security analysts from different industries and areas. Interviews are very used qualitative method in the cybersecurity visualization field [4], and given the dynamic security landscape, we believe that a broad, direct exchange with security analysts within their working contexts may lead to new perspectives and outcomes such as a better characterization of the practical considerations of analysts' workflow within their organizations and an identification of the motivations, challenges, or constraints behind the visualization-related choices of practitioners.

3 PROPOSED INTERVIEW METHODOLOGY

To explore the potential visualization gaps in cybersecurity visualization domain, we adapt prior qualitative methodologies into a visualization focused interview for cyber security domain. We describe the methodology we follow to design, conduct the interviews and to analyze the collected data.

Figure 1: Sample questions for the themes in the proposed interview. The full protocol is available as supplemental material.

3.1 Participants

We target security professionals doing some or all of the high-level tasks suggested by Kandel *et al.* [6] as part of their data-driven security workflow. To ensure that our sample is representative of security analysts' works and the different organizational structures, we target practitioners working in organizations of different sizes ranging from individual, to large institutions making security products, and data-driven businesses who heavily rely on secure information systems.

3.2 Interview

Figure 1 shows a sample of the interview protocol with the goals for the four themes that we cover: the analyst's job and role within the organization, their experience with data, with data visualization concepts, best practices or tools, and their familiarity with (security) visualization research. The challenges in identifying effective interview questions are that we address different types of security roles, of which some might not require advanced visualizations (even then we still want to hear about how current analysis could be supported), experts might not be familiar with the visualizations or human-computer interaction terminologies. To analyze the interview data, an open-coding scheme is applied in which the authors will regularly meet to adjust the coding scheme as we gather more data.

4 Early findings

We conducted a pilot study with 3 participants working in security industry, as threat intelligence analysts (2), and digital forensics investigator (1). The interviewees are affiliated to different companies and had seven years of experience in average. Following the proposed methodology, our initial results highlight the analysts' organizational contexts, the ever-changing landscape of the cyber security job, challenging characteristics of the security data, which all impact the analysts' choice of visualisation tools and techniques.

Organizational rules applicable to the context of their work do not always allow analysts to freely adopt the best practices for data visualization. One interviewee said: ''I usually make no choices [of color] because there's a standard corporate template."

Privacy disclosure considerations also impacts analysts' choice of visualization techniques as one interviewee said: "*in this particular graph, we don't have an X Y axis because this is our own data. We don't want to give away what would be competitive information and customer information*." Added to that, cloud-based visualization systems are generally avoided due to the privacy of the data, and in some cases analysts are required to analyze a tool's source code to identify vulnerabilities that could leak sensitive data.

The **target audience** of analysts' results also impact their visualization practices. An essential part of today's security expertise is reporting security analysis to other experts who are neither security nor data visualization practitioners. For such tasks, our interviewees reported that complex visualization techniques are often not helpful as they require extra effort and training.

The tool configurations such as the limitation on supported data formats, the requirement to install and set up the tools *vs.* plug-and-play model also impacts analysts' choice of visualization tools.

5 Conclusion and future work

We propose an interview-study with security analysts to identify the different aspects behind their choice of data visualization tools and the best-practices that they apply in their workflows. Early results indicate how the organizational guidelines, the target audience of analysts, the sensitive characteristics of working data, and the technical configurations of proposed tools impact the way analysts choose and adopt specific visualizations systems and techniques. By extending the interview to more security analysts in different domains, we hope to highlight research opportunities to address analysts' challenges in adopting researched visualization methodologies and tools; for example exploring raising topics like privacy preserving visualizations in cyber security or including support for easy vulnerability checks in published visualization tools.

References

[1] A. Batch and N. Elmqvist. The interactive visualization gap in initial exploratory data analysis. *IEEE transactions on visualization and computer graphics*, 24(1):278–287, 2017.

[2] V. S. Carvalho, M. J. Polidoro, and J. P. Magalhães. Owlsight: Platform for real-time detection and visualization of cyber threats. In *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, pp. 61–66, 2016.

[3] A. D'Amico, L. Buchanan, D. Kirkpatrick, and P. Walczak. Cyber operator perspectives on security visualization. In *Advances in Human Factors in Cybersecurity*, pp. 69–81. Springer, 2016.

[4] D. Fujs, A. Mihelič, and S. L. Vrhovec. The power of interpretation: Qualitative methods in cybersecurity research. In *Proceedings of the 14th International Conference on Availability, Reliability and Security*, pp. 1–10, 2019.

[5] S. R. Hong, J. Hullman, and E. Bertini. Human factors in model interpretability: Industry practices, challenges, and needs. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW1):1–26, 2020.

[6] S. Kandel, A. Paepcke, J. M. Hellerstein, and J. Heer. Enterprise data analysis and visualization: An interview study. *IEEE Transactions on Visualization and Computer Graphics*, 18(12):2917–2926, 2012.

[7] S. McKenna, D. Staheli, and M. Meyer. Unlocking user-centered design methods for building cyber security visualizations. In *2015 IEEE Symposium on Visualization for Cyber Security (VizSec)*, pp. 1–8. IEEE, 2015.

[8] J. Schmidt. Usage of visualization techniques in data science workflows. In *VISIGRAPP (3: IVAPP)*, pp. 309–316, 2020.

[9] H. Siadati, B. Saket, and N. Memon. Detecting malicious logins in enterprise networks using visualization. In *2016 IEEE Symposium on Visualization for Cyber Security (VizSec)*, pp. 1–8. IEEE, 2016.

[10] D. Staheli, T. Yu, R. J. Crouser, S. Damodaran, K. Nam, D. O'Gwynn, S. McKenna, and L. Harrison. Visualization evaluation for cyber security: Trends and future directions. In *Proceedings of the Eleventh Workshop on Visualization for Cyber Security*, pp. 49–56, 2014.