EPiC Series in Computing

Volume 102, 2024, Pages 44–53

Proceedings of Conference on Cognitive and Computational Aspects of Situation Management 2023

Exploring Cognition and Proficiency in Cybersecurity Incident Response: Description of a Subject-Matter Expert Interview

David Schuster[1*], Crystal M. Fausett[2], Jenna Korentsides[2], Sabina Mitesh Patel[2], Elizabeth H. Lazzara[2], and Joseph R. Keebler[2]

[1] San José State University, California, U.S.

[2] Embry-Riddle Aeronautical University, Florida, U.S.

david.schuster@sjsu.edu, fausetc1@my.erau.edu, korentsj@my.erau.edu, patels77@my.erau.edu, lazzarae@erau.edu, keeblerj@erau.edu

Abstract

Cybersecurity incident response presents significant challenges, exacerbated by a limited understanding of the cognitive processes employed by cybersecurity professionals. Cognitive task analysis (CTA) is a valuable tool to address this knowledge gap and inform evaluation, training, and design of cybersecurity systems. However, the required access and cost have limited the number and scope of CTAs in cybersecurity. Therefore, a need exists for CTA-derived insights about incident response and methodology of CTA to support data collection in this rapidly evolving domain. In this paper, we explore some of the challenges specific to CTA in the context of incident response, present an example demonstrating how CTA facilitates insights by examining results obtained from a single subject matter expert (SME), and describe the role of CTA in our ongoing mixed methods research program. The application of CTA in supporting quantitative research holds promise for advancing cyber defense strategies.

1 Introduction

1.1 The Work of Cybersecurity Professionals

The cybersecurity of organizations, especially corporations, presents an ongoing and costly challenge, with potentially devastating impacts when cybersecurity is poor. The quality and sophistication of cyber-attacks continue to rise at an alarming rate. In 2021, Accenture reported an

* Corresponding author

K. Baclawski, M. Kozak, K. Bellman, G. D'Aniello, A. Ruvinsky and C. Da Silva Ferreira Barreto (eds.), CogSIMA 2023 (EPiC Series in Computing, vol. 102), pp. 44–53

average of 270 attacks per company per year, reflecting a 31% increase over 2020 [1]. Further, the global average cost of a data breach within an organization stands at $4.35M [2]. To address this escalating threat, organizations allocate a significant portion of their budget toward security measures, accounting for about 15% of total information technology spending [3]. Beyond financial impacts are consequences that impact health and safety concerns and affect supply chains and critical infrastructure. In a notable case, University Hospital Dusseldorf alleged that a ransomware-caused network outage led to the death of a patient [4].

Considering the potential gravity of the consequences, cybersecurity requires professional expertise to effectively manage the cognitive demands. Agyepong and colleagues [5] identified several recurrent challenges faced by cybersecurity analysts, including the difficulty of detecting rapidly evolving threats amidst high workload scenarios—a difficult signal detection problem in which relevant events must be detected and understood out of a rapid stream of irrelevant information. Incident management and response, the process of investigating and planning a resolution to cybersecurity incidents, is particularly critical and complex because it is intimately tied to the organization's business. For example, consider the differences in the response of a hospital to a malware attack compared to that of a retail store. Therefore, incident response is frequently assigned to more experienced professionals. Even though experienced individuals often assume these roles, there is a lack of sufficient knowledge of the cognition of cybersecurity professionals and how their cognition supports proficiency in demanding roles like incident response. This is a problem because incident responders are at the end of an already-insufficient workforce pipeline. With better knowledge of cognition and proficiency development, improved training and recruitment could support a greater number of incident responders who are better able to perform this cognitively challenging and critical work.

1.2 Utility of Mixed Methods Research

To better understand the complexities inherent in cybersecurity, there is a need to leverage mixed methodological approaches. Mixed methods research, which combines quantitative and qualitative aspects, is well suited to improve understanding of the cognitive aspects of cybersecurity incidents. Quantitative research offers the ability to test falsifiable, *a priori* hypotheses and provide generalizable evidence [see 6]. One challenge to quantitative research is that hypotheses and measurement must be specified *a priori*. Researchers need to know what to measure and how to quantify it. Quantitative research also requires isolation of variables of interest, which can obscure or remove important context. These are meaningful barriers to research on cognition in cybersecurity. Qualitative research provides a complementary piece through its ability to derive explanations of the *how* and *why* of phenomena while incorporating environmental context. It lacks the descriptive power and generalizability of quantitative research, however. In a domain where cognition is only starting to be understood, qualitative research can be used to generate theory, hypotheses, and measurement strategies that can be tested more directly using quantitative research.

1.3 Cognitive Task Analysis

Cognitive task analysis (CTA) offers a valuable approach. CTA is a collection of qualitative research methods used to understand cognition in specific contexts and improve performance [7]. As a qualitative research methodology, CTA can support and complement quantitative research, such as laboratory experimentation, by elucidating the cognitive components that support the goal of a successfully managed incident response. As another example, we can identify knowledge elements at the three levels of Endsley's model of situational awareness (SA; i.e., perception, comprehension, and projection) using goal-oriented task analysis [8], [9].

Although CTA can be beneficial, CTA is resource intensive. In the context of aviation, another complex and intensive field of work, Seamster and colleagues suggested that a four-hour data collection

could cost between $2,400 and $16,400 depending on the methods used and hourly rates [10]. Beyond expense, CTA in the context of incident response poses specific challenges that must be addressed. One such challenge is the shortage of cybersecurity professionals, which creates a high demand for their time and expertise. CTA methods often require multiple long sessions with experts, which makes it difficult to apply to operational cybersecurity settings [11], [12]. Additionally, cybersecurity is inherently a secretive industry. This is adaptive, because secrecy is aligned with the goal of security, and maladaptive; Coldebella and White identified structural disincentives that act as barriers to information sharing, hindering the exchange of valuable insights in cybersecurity investigations [13]. This privacy and security emphasis means that comprehensive access to a security operations center (SOC) by a CTA researcher is unlikely, let alone a researcher conducting the analysis for public benefit. Despite this, researchers have conducted and published a variety of CTAs over the past few decades [14]–[17]. These are valuable but are too few and too far between.

To maximize the value and impact of CTA efforts, it is crucial to publish and share lessons learned from research endeavors. Because of the value CTA offers to theory and hypothesis development, even limited-access CTAs and small samples may provide value. Through sharing these findings, methodologies, and insights gained from CTA studies, researchers and cyber professionals can benefit from this knowledge, accelerating and updating cognitive processes and strategies in the field of cybersecurity and similarly complex fields of work. Moreover, this knowledge could be used to create training and educational programs to improve work performance. Overall, publishing lessons and findings from CTAs is essential in addressing the urgent need for advancements in the cognitive aspects of cybersecurity.

Our work builds from past CTAs, and we focused specifically on the work by Gutzwiller et al. [16], who coined the term cyber-cognitive situation awareness, referring to the human cognition that supports performance of cybersecurity professionals. They conducted semi-structured interviews, a knowledge audit, and a concept mapping exercise with seven cyber analysts in the U.S. Navy. One of their most relevant insights was the development of a cyber-cognitive SA model suggested by the results of the CTA. The model included three elements: the network, the world, and the team. Knowledge of the network included the hardware and software assets on the network and how they behaved. Knowledge of the world included the larger security community and awareness of emerging threats. Finally, knowledge of the team included the procedures, resources, and constraints associated with team members. Because the participants were in the military, we were interested how this three-component model was applicable to an industry context.

The goals of the present paper are to demonstrate utility of a low-cost case study to support a CTA and provide lessons learned for future research on human cognition in cybersecurity. Specifically, we present the results obtained from a single cybersecurity subject matter expert (SME), defined as a professional recognized by management in the organization as having the highest level of proficiency, and demonstrate how these findings contribute to the broader process of developing mixed method research. By employing CTA techniques, we can delve into the cognitive processes and mental frameworks utilized by the SME, shedding light on their understanding of complex situations encountered in the cybersecurity domain. This approach allows us to capture perspectives that can inform the development of more comprehensive mixed method research designs, combining qualitative and quantitative approaches. By demonstrating how CTA can elicit mental models and be integrated into a larger research framework, this paper supports our understanding of cognition in incident response and informs research methodology.

2 Method

In late 2019, an interview was conducted with a single individual from a large networking technology company employing between 50,000 and 100,000 individuals. Recruitment was done by approaching the management of the organization's security operations center (SOC); we asked for a single individual who was among the most proficient individuals on the team. Management referred us to one participant who completed a demographics survey and participated in an interview lasting approximately three hours.

The purposes of the interview were to: (1) better understand expertise and mental models in incident response and (2) gain feedback on our development of a simulated scenario. The interview took place after a period of information gathering in which we formulated four broad research questions. To gain an understanding of expertise within a young industry, we were interested in exploring the indicators of expertise, assessing whether events or incidents were useful metrics for workload evaluation, examining the process of sensemaking, and gaining feedback on the three-component model proposed by Gutzwiller and colleagues, which includes network, world, and team components [16].

Four notetakers were present, including the first author and three research assistants. Interview content was verified among the notetakers to ensure consistency. In the interest of confidentiality, audio recording was not used, and instead, interview content was confirmed through the collaboration of the notetakers. Because of this, the interview content is presented in a paraphrased manner.

To gain feedback on our development of a simulated scenario, we presented our ideas for simulating cybersecurity events in a way that could be used for mixed-methods research. Our SME walked us through the use of Splunk, a log analysis tool, and published past versions of Splunk's Boss of the SOC (https://github.com/splunk/botsv1) cybersecurity competition.

3 Results

3.1 Interview Insights

Our SME held the title of information security investigator and had been in the role for eight years. The SME reported 16 years of experience in cybersecurity. This participant held a computer science bachelor's degree. Based upon the themes that emerged from the case study, we present seven critical skills of proficient incident responders. Following this, we offer insights related to Gutzwiller and colleagues CTA [16] and the use of Splunk as a simulation testbed to observe incident response.

3.1.1. Focus on the details.

On the topic of proficiency, our SME said that the team tends "to not shy away from technical details of things" and takes the time to understand how everything works. Our SME spoke of learning underlying complexities of the system itself, as it helps inform investigative process. When it comes to hiring, our SME emphasized the significance of understanding the fundamental workings of the system, rather than solely focusing on the tools used to rectify issues.

The implication of this insight for researchers is that, in addition to technical knowledge, understanding of the relationships among concepts is important. Cybersecurity training and evaluation can benefit from the assessment of mental models. By expanding the definition of system to include the human and technology elements that impact outcomes, researchers can gain insight into how incident responders identify and understand the human behavior, by team members and adversaries, that impact the incident.

3.1.2. Response is making sense of what happened in the past.

Our SME emphasized that *response* is a vital part of the job, meaning that their focus is primarily on analyzing events that have already occurred. Our SME expressed this by stating, "We are not prevention. We are murder investigators." Their role does not involve witnessing the incident as it happens; instead, they are there to uncover and understand what happened in the past.

Researchers should learn more about the sensemaking process to identify its required skills. For example, learning the circumstances under which an incident responder should replace one account of the incident with another may inform training and improve decision making.

3.1.3. Learn to extrapolate.

The work of incident responders is challenging because the view, an understanding of what happened, is always incomplete. While metadata about network traffic is more commonly available than the actual contents of the network traffic, it fails to provide a complete picture of what happened. Consequently, incident responders must rely on inferring a broader set of information from an incomplete set. Drawing probabilistic conclusions about what happened from limited information requires an understanding of the base system.

While probabilistic reasoning is a foundational skill of incident responders, it is subject to heuristics and biases [18] that can be maladaptive. Training in incident response decision making should make learners aware of these biases and how to leverage heuristics more effectively. Without this, knowledge of biases in probabilistic reasoning could be leveraged by attackers.

3.1.4. Distinguish between event types.

Our SME reported that events and incidents were useful units of analysis. Events are information about what happened on a system or a network that helps inform the overall picture of the incident. Events are discrete things that happened and are recorded. "You put them together to find the incident." Our SME distinguished between two meanings of event; *traditional security events* include alerts from intrusion detection systems or firewalls. These are different from *informational events*, which function as statements of fact. The significance of an informational event is only apparent when combined with other informational events. According to our SME, informational events are like security footage. Whether knowing that an individual passed by a security camera is relevant to the incident depends on other informational events, like a biometric scan of that individual. The combination of informational events can result in traditional security events. This suggests that researchers should consider events as elements of SA, and the meaning and future states of these events may support higher levels of SA.

3.1.5. Leverage communication between team members where possible.

We wanted to learn more about whether "cradle-to-grave" described work at the SME's company as it had in [16]. A "cradle-to-grave" approach is one in which tasks started by one individual are primarily completed by the same individual. Emphasizing that they could speak only for their company, our SME described a desire for teamwork but barriers to its implementation. The company tries hard to not make it cradle to grave but they are not fully successful in that. The reason for this is that the cost of doing a handoff, where an investigation is transferred from one party to another, is high. Our SME said that it was challenging to document and to absorb information from the documentation. Three tiers are used in the company. The first tier consists mostly of contractors located outside the United States. Tier 1 mostly handles "very simple routine things. If they get something complicated, they escalate and hand-off. The second tier is when an investigator gets a case directly. The Tier 2 investigator works the

case completely and only hands it off in the event of a shift change. Sometimes, another person is brought into the investigation if they can provide needed expertise. They will consult with a new investigator, finishing with incident write up. Another exception is an emergency requiring "all hands-on deck." But, for the most part, incidents are handled cradle-to-grave in the company, which was described as "part of the job." It is the investigator's responsibility to figure it out. Following this, the SME suggested that once every two or three years an incident will require an investigator's work for months. That investigator "takes one for the team."

3.1.6. Be aware that cost and time constrain investigations.

We also wanted insights regarding some of the limitations of investigations. Our SME described, in general terms, opportunity cost as a limit to investigations. Investigations are costly and time-consuming, and "it's easy to rabbit hole on something that ultimately doesn't matter. You could spend the next year reverse engineering malware for no reason…To be a good effective investigator, one has to have gut instinct on whether doing the in-depth investigation will be fruitful and worth it…. One of the things that informs that, is. What are the systems involved? Is it an employee's laptop? Or is this the CFO laptop?" Here, our SME suggested that novice investigators may have the inclination to thoroughly investigate every aspect of an incident and gather as much information as possible to obtain a comprehensive understanding. However, it becomes necessary to strike a balance between the depth of understanding the incident and the urgency of the response.

3.2 Reflections on the Three-Component Model

In addition, we were also interested in seeking feedback pertaining to a component model. Our SME's feedback on the three-component model of network, world, and team confirmed its relevance while suggesting that its applicability may vary. It is worth noting that we simply presented these terms as part of the interview process. Each component is described in detail by [16], but we did not provide complete definitions during the interview. In response to the terms, our SME said that the idea of network is "more than just the network." To paraphrase our participant: Networks have gotten faster, transmit more data, and have more intra-network communication that is unanalyzable and uncapturable. The world has pushed hard for point-to-point encryption. This makes traditional ways of doing analysis hard. Breaking encryption is a cost. It is breaking security in the name of security. It is a tradeoff you do not want to do. We have increasingly, as a field, been turning to every source of info that we can get, including host-based security. This requires more than knowledge of the network. Knowledge of the network is one small component of overall system.

Next, our SME suggested that knowledge of the team may not be as relevant as the broad conceptualization of the network described earlier. Finally, our SME was unsure of the meaning of knowledge of the world. When we explained that knowledge of the world indicated broad awareness of emerging cyberthreats, our participant responded that understanding attacker techniques is important. However, our participant drew a distinction between knowing world knowledge in the sense of building understanding of the world or knowing all possibilities. Rather, world awareness is built by studying adversarial techniques.

3.3 Simulation Development Results

Finally, we wanted to get feedback about simulating cyber events for knowledge elicitation research. Saying that the then-current Splunk and Boss of the SOC "sucks," but it's the "best we've got," our SME described the contest as more of a marketing tool rather than a training tool. We observed three general critiques; first, the Boss of the SOC dataset is idealized, whereas operational data and the queries that need to be performed on it are messier. That is, although Splunk is designed to help make sense out

of unstructured data from many sources, the data provided in the Boss of the SOC contest was an ideal case for Splunk to ingest and filter in the view of our SME. Second, the volume of data used by our SME in their enterprise was larger than what Splunk was able to process in 2019. Third, effective use of Splunk requires proficiency in Splunk itself and a well-developed understanding of its limitations. Our SME noted that they worked in an environment indexing three billion events per hour.

We editorially note that these critiques, like any software review, are unlikely to apply to later versions; Splunk has continued to evolve. As of this writing, Splunk offers a machine learning toolkit to further automate data decision making. Rather than reflecting the current state of Splunk, these critiques were useful in our investigation because they helped us to anticipate challenges in the use of the Boss of the SOC contest for research on human cognition. We describe those challenges and current progress on that work in the next section.

4 Discussion

The goal of this paper was to demonstrate how a single interview can support wider CTA efforts as part of mixed methods research to understand cognitive aspects of cybersecurity. We presented the results from a single SME and next describe how this information fits into the larger process of developing mixed-methods research for cybersecurity.

4.1 Cognition of Incident Responders

Even a brief interview with a single professional can help inform knowledge of the cognition of incident responders. First, resolving the incident is a high-level goal, and an incident may be a useful unit of analysis for understanding human performance. Investigating the incident and deciding on action emerged as subgoals. This process can be understood as sensemaking, which is learning "how the current state of affairs came about" [19]. Sensemaking is essentially the same process as situation assessment, the process of building SA. Because it occurs in a time-constrained environment with incomplete information, responders must have skills that allow them to extrapolate. This suggests examining the process and outcomes of sensemaking more closely. For example, individuals with knowledge of tools but lacking skill at sensemaking may adopt strategies of investigating everything to learn as much as possible about what happened. Based on our interview, we learned that event research is a time-consuming process, so investigators need to be strategic in their information gathering. They need to balance the depth of understanding of the incident with the urgency of a response, which interacts with the goals and characteristics of the organization.

This interview informed our ongoing research into identification of situation awareness elements. First, both traditional security events and informational events could contain goal-relevant information necessary for SA. However, filtering of many events to find the few relevant ones is a resource-intensive task. At the time of our interview, this was provided by first-tier contractors who escalated events as needed. In the time since this interview, rapid machine learning improvements hint that more of the filtering functions are automatable, and a transformative level of automation is on the horizon. Thus, this interview has aged as technology has rapidly evolved. This suggests new research questions in human-automation interaction as cybersecurity tools handle tasks that human team members performed in 2019. Because informational events function as statements of fact and may be relevant to an investigation, they may support level 1 (perception) SA elements. Traditional security events, especially as tools become better at providing relevant alerts, can augment level 1, when filtering for relevance, or level 2 (comprehension) SA, when alerts provide an integration of informational security events. For example, that an IP address visited the company's web site is an informational event and may or may not be relevant to the investigation. An intrusion detection system providing an alert that a known malicious script accessed the web site is a traditional security event, and again, may be level 1

information if relevant to the goal of investigating the incident. Combining that alert with the knowledge that the website was unpatched and, thus, vulnerable to the malicious script, contributes to level 2 SA. In the near-term, automation may already support higher levels of SA. Even so, understanding of the information in the situation and how it relates to the bigger picture in the company is a theme of the interview and not immediately automatable. Therefore, understanding human cognition by identifying and measuring SA will continue to be helpful.

4.2 Support of Mixed-Methods Research

This interview was conducted to help develop mixed-methods research in which qualitative investigation is used to bootstrap quantitative research. Specifically, CTA can be used to generate insights that lead to testable hypotheses and to suggest measurement strategies and interventions.

Our SME interview informed our evaluation of existing simulations to support a further qualitative and quantitative research. We needed to develop a testbed in which we could observe individuals at various skill levels perform a common cybersecurity task. Splunk was a candidate tool, and our interview uncovered several challenges in attempting to develop a simulated scenario. First, platform agnosticism was an important consideration. That is, we aimed to measure cognition in response to the scenario, not proficiency with the tool used in the scenario. The competition required prior knowledge of the platform. In a performance task, a participant would need to be given the competition scenario and asked to perform a task using Splunk. A lack of familiarity would either make completion of the task impossible, or the researcher would need to train all participants to a criterion as an attempt to control for the level of Splunk knowledge. There is a need for a platform that includes operational data at a scale that is appropriate for cybersecurity professionals with diverse expertise. However, asking an enterprise professional to comb through a tiny dataset is as unrealistic as having an entry-level cybersecurity professional make sense out of an enterprise dataset.

Our interview method allowed us to ask probing questions about the operational complexity of the work, particularly in relation to a company's operations, which contributes ecological context. Cyber network defenders may find it essential to develop a deep understanding of the business context in which they operate to address threats. The business environment, technical infrastructure, and operational standards of practice may vary across different companies and organizations, potentially limiting the generalizability of the results to other settings. This creates a need to either: (1) train individuals on the intricacies of the business before the exercise, or (2) devise measurement techniques that are not inherently reliant on such context. By finding innovative approaches to either impart the essential contextual knowledge or devise context-independent scenarios, we can enhance the overall ecological validity of inferences made using the testbed.

We addressed these issues by combining the Boss of the SOC scenario content with elicitation by critiquing (EBC) [20]. In EBC, the participant does not perform the task directly. Rather, a novice's performance of the task is prerecorded and played for the participant. The participant then critiques the novice's performance. In our ongoing research, we are investigating the content of the critiques for differences across levels of experience. As non-cybersecurity professionals, we were able to implement this scenario because it did not require us to develop a scenario from scratch. This approach also minimizes the need for comparison to one expert representation. We are using the same scenario to pilot quantitative measurement of SA.

Our use of EBC partially addresses the problem of Splunk familiarity. In an EBC scenario, the participant does not interact with Splunk directly. Instead, the participant is observing a novice investigate an incident using Splunk. This allowed participants who were not familiar with Splunk to follow along and focus on other aspects of the investigation that were relevant to their experience. That said, Splunk was still used in the scenario, and knowledge of Splunk was likely helpful in forming critiques.

4.3 Limitations

We have not provided a complete CTA but, rather, aimed to share ongoing work-in-progress. Although CTA is valuable even with small sample sizes or some limitations in access and depth of observation, our SME case study has both limitations. The field should continue to endeavor toward comprehensive, publishable CTAs to benefit the entire security community. When this is challenging or slow going, we argue that sharing tentative insights, as we have here, is valuable.

A second, and important, limitation of this work is the age of the interview and the major changes that have taken place in the past four years. While this may limit the applicability of the specific insights to present day, a lesson for us and other researchers in this domain is to strive for a faster cycle of data collection and dissemination. The technological and organizational environment evolves rapidly relative to human cognition, so the study of human-technology interaction is also rapidly evolving.

Because CTA is a qualitative technique, our findings are insights, and our conclusions are descriptive rather than prescriptive. They serve not to inform the present practice of cybersecurity but to guide researchers toward evidence-based models and measures of cybersecurity performance. This is a necessary step to impactful research in this domain. The limitations of a partial analysis should be considered when interpreting the results. In addition, the research presented in this paper is based on an interview with one SME and certainly does not capture the diversity and variability within the cybersecurity workforce. The results of this study are a small piece of the puzzle, and future research will enhance and advance the cumulation of knowledge in this important area. As noted previously, conducing a comprehensive CTA entails a significant cost and time investment. These limitations of the data collection process should be noted as they may impact the breadth and depth of the insights gained. Despite these limitations, the aim of this paper is to share knowledge and insights to expedite future research on the cognitive processes of cyber network defenders.

4.4 Conclusion

The cybersecurity threat landscape poses ongoing and costly challenges for organizations, with significant financial and operational impacts. The integration of human factors science, particularly in understanding the cognition of cybersecurity professionals, is critical to addressing the seemingly intractable nature of cybersecurity. The scale and scope of cybersecurity incidents pose significant challenges that necessitate a deeper understanding of the cognitive processes employed by cybersecurity professionals. CTA is a valuable tool to bridging this knowledge gap. We presented a discussion of specific challenges associated with applying CTA to incident response. We have also detailed an example of how CTA can support mixed-methods research by analyzing the results obtained by a single SME. By leveraging CTA and its integration with quantitative research methods, we can contribute to the effectiveness of cyber defense.

5 Acknowledgments

We sincerely thank our subject-matter expert for sharing their expertise. This work is based upon work supported by the National Science Foundation under Grant No. 1553018. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

References

[1] K. Bissell, J. Fox, R. M. LaSalle, and P. Dal Cin, “How aligning security and the business creates cyber resilience,” Accenture, 2021. [Online]. Available: https://www.accenture.com/content/dam/accenture/final/a-com-migration/custom/us-en/invest-cyber-resilience/pdf/Accenture-State-Of-Cybersecurity-2021.pdf#zoom=40

[2] IBM, “Cost of a data breach 2022: A million-dollar race to detect and respond,” IBM, 2022. [Online]. Available: https://www.ibm.com/reports/data-breach

[3] J. Fox, R. LaSalle, and P. Dal Cin, “The state of cybersecurity resilience 2021,” Accenture, 2021. [Online]. Available: https://www.accenture.com/us-en/insights/security/invest-cyber-resilience

[4] O. Niki, G. Saira, S. Arvind, and D. Mike, “Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that,” *Digit. Health*, vol. 8, p. 205520762211046, Jan. 2022, doi: 10.1177/20552076221104665.

[5] E. Agyepong, Y. Cherdantseva, P. Reinecke, and Burnap, “Challenges and performance metrics for security operations center analysts: a systematic review,” *J. Cyber Secur. Technol.*, vol. 4, no. 3, pp. 125–152, 2020.

[6] J. Dykstra, *Essential cybersecurity science: build, test, and evaluate secure systems.* O’Reilly Media, Inc., 2015.

[7] G. Klein and C. Wright, “Macrocognition: From Theory to Toolbox,” *Front. Psychol.*, vol. 7, Jan. 2016, doi: 10.3389/fpsyg.2016.00054.

[8] M. R. Endsley, “Design and Evaluation for Situation Awareness Enhancement,” *Proc. Hum. Factors Soc. Annu. Meet.*, vol. 32, no. 2, pp. 97–101, Oct. 1988, doi: 10.1177/154193128803200221.

[9] M. R. Endsley, “A Survey of Situation Awareness Requirements in Air-to-Air Combat Fighters,” *Int. J. Aviat. Psychol.*, vol. 3, no. 2, pp. 157–168, Apr. 1993, doi: 10.1207/s15327108ijap0302_5.

[10] T. L. Seamster and R. E. Redding, *Applied cognitive task analysis in aviation*. Routledge, 2017.

[11] C. L. Paul and K. Whitley, “A Taxonomy of Cyber Awareness Questions for the User-Centered Design of Cyber Situation Awareness,” in *Human Aspects of Information Security, Privacy, and Trust*, L. Marinos and I. Askoxylakis, Eds., in Lecture Notes in Computer Science, vol. 8030. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 145–154. doi: 10.1007/978-3-642-39345-7_16.

[12] A. Scott, I. Cooke, K. Sliwinska, N. Wong, and D. Schuster, “Elicitation by Critiquing: Applications to Computer Network Defense,” *Proc. Hum. Factors Ergon. Soc. Annu. Meet.*, vol. 62, no. 1, pp. 1247–1251, Sep. 2018, doi: 10.1177/1541931218621286.

[13] G. P. Coldebella and B. M. White, “Foundational Questions Regarding the Federal Role in Cybersecurity,” *J. Natl. Secur. Policy*, vol. 4, p. 233, 2010.

[14] L. Buchanan, A. D’Amico, and D. Kirkpatrick, “Mixed method approach to identify analytic questions to be visualized for military cyber incident handlers,” in *2016 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Baltimore, MD, USA: IEEE, Oct. 2016, pp. 1–8. doi: 10.1109/VIZSEC.2016.7739578.

[15] N. J. Cooke, M. Champion, P. Rajivan, and S. Jariwala, “Cyber situation awareness and teamwork,” *ICST Trans. Secur. Saf.*, vol. 1, no. 2, p. e5, May 2013, doi: 10.4108/trans.sesa.01-06.2013.e5.

[16] R. S. Gutzwiller, S. M. Hunt, and D. S. Lange, “A task analysis toward characterizing cyber-cognitive situation awareness (CCSA) in cyber defense analysts,” in *2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, San Diego, CA, USA: IEEE, Mar. 2016, pp. 14–20. doi: 10.1109/COGSIMA.2016.7497780.

[17] S. Trent, R. R. Hoffman, D. Merritt, and S. Smith, “Modelling the Cognitive Work of Cyber Protection Teams,” 2023.

[18] A. Tversky, D. Kahneman., "Probabilistic reasoning." in *Readings in Philosophy and Cognitive Science*. MIT Press, 1993.

[19] B. Crandall, G. A. Klein, and Hoffman R. R., *Working minds: A Practicioners guide to cognitive task analysis*. MIT Press, 2006.

[20] J. E. Miller, E. S. Patterson, and D. D. Woods, “Elicitation by critiquing as a cognitive task analysis methodology,” *Cogn. Technol. Work*, vol. 8, no. 2, pp. 90–102, Jun. 2006, doi: 10.1007/s10111-005-0023-7.