The Rationality of Automation Bias in Security Operation Centers

Traditional Peer Review Submissions

Jack Tilbury and Stephen Flowerday
The University of Tulsa, Department of Cyber Studies
jlt2680@utulsa.edu and stephen-flowerday@utulsa.edu

Abstract

Security Operation Centers (SOCs) are comprised of people, processes, and technology with the sole purpose of protecting the organization from cyber-attacks. This is achieved through the monitoring and mitigation of security threats, allowing for a solid security posture. These teams consist of SOC analysts, ranging from Tier 1 to Tier 3. To cope with the significant number of security alerts that SOC analysts must deal with, the integration of automation and automated decision aids (ADAs) is increasing. Research has demonstrated that automation poses a risk to the cognitive skillset of human operators as humans tend to become over-reliant on automated systems despite the presence of contradictory information. This cognitive bias is known as automation bias. The result of this literature review is the development of four Critical Success Factors (CSFs) for the adoption of automation within SOCs in an attempt to mitigate automation bias: (1) Task-based Automation; (2) Process-based Automation; (3) Automation Performance Appraisal; and (4) SOC Analyst Training of Automated Systems. In applying these CSFs, a beneficial balance between the SOC analyst and the use of automation is achieved. As a result, this study promotes the preservation of human-in-the-loop, whereby experienced and cognitively aware SOC analysts remain at the helm.

Keywords: Security Operation Center, SOC, SOC Analyst, Automation Bias, Automated Decision Aids, Critical Success Factors

Introduction

The Security Operation Center (SOC) represents an organization's primary unit in safeguarding against cyber-attacks. The SOC environment is characterized by time pressure and high-stress scenarios, as teams of SOC analysts systematically engage in damage limitation and restoration of systems (Akinrolabu et al., 2018; Hámornik & Krasznay, 2018; Naseer et al., 2021). Moreover, it is argued that how SOCs currently function contributes towards the creation of grueling conditions that SOC analysts need to effectively operate under. In a bid towards the establishment of a more conducive work setting, the increased adoption and usage of automation have been proposed to reduce the demands placed on SOC analysts. However, increased automation negatively impacts the cognitive skills of SOC analysts. This occurs in the form of automation bias. Therefore, when considering the needs of SOC analysts, automation must be adopted in a complementary, rather than a substitutive, manner. This study proposes the following problem statement:

> *The increased adoption of automation in SOCs has adverse effects on SOC analysts. This occurs through automation bias whereby SOC analysts become over-reliant on automated decisions, despite the presence of contradictory information. Higher levels of automation (LOA) lead to human-out-of-the-loop, resulting in the loss of situation awareness, cognitive skill degradation, and task complacency.*

Next, an all-inclusive look into the environment of a SOC will be discussed – how they are structured, where automation can be applied, the challenges they face, and the nature in which they operate. The theoretical foundation of this paper, automation bias, will then be discussed. This is followed by examples of high-

profile attacks whereby the potential for automation bias could have occurred. The critical success factors for the use of automation in a SOC in an attempt to mitigate automation bias are then presented. The contribution of this literature review culminates with the proposal of the Influence, Impact, and Alleviation of Automation Bias Model. Finally, the study's limitations and areas of future work are addressed.

SOCs: Structure, Challenges, and Environment

Despite the prevalence of the term 'SOC', Computer Emergency Response Team (CERT), Computer Incident Response Team (CIRT), and Managed Detection and Response (MDR) services are commonly used terms (Miloslavskaya, 2016). Certain research has differentiated between these teams, stating that the role of SOC analysts is to detect and escalate threats to a Computer Security Incident Response Team (CSIR) (Agyepong et al., 2020). This study postulates that as the lines between detection and response activities become blurred, SOCs should take on full responsibility for each stage of the incident response lifecycle – detection and analysis, containment, eradication, recovery, and post-incident activity (Cichonski et al., 2012). This paper utilizes the term 'SOC'. The structure of SOC analysts is listed in **Table 1** in terms of their respective levels and corresponding duties.

Table 1: Tiered Structure of SOC Analysts - Roles and Responsibilities

SOC Analyst	Roles and Responsibilities
Tier 1 Analyst – Alert triage	- Implementation and fine-tuning of network sensors. - Analyze network traffic alerts in the process of triage. - Escalate critical threats.
Tier 2 Analyst – Incident response	- Classification and analysis of critical threats. - Incident response strategies.
Tier 3 Analyst – Threat hunting	- Sophisticated attack analysis and mitigation. - Identify and remediate vulnerabilities not yet exploited.

SOC Challenges

SOC analysts must comb through a considerable number of alerts to identify high-severity threats (Miloslavskaya, 2016). This is referred to as alert fatigue (Agyepong et al., 2020; Kokulu et al., 2019; Vielberth et al., 2020). This is further hindered by the number of false positives, which is partly attributed to the numerous devices connecting to an organization's network – amplified by remote working (Kokulu et al., 2019). This increases the complexity of the existent challenge that analysts face – having the cognitive ability to discern which alerts need immediate attention versus those deemed not critical. This leads to a work environment that involves mundane and repetitive processes. Another challenge is coping with sophisticated attacks arising as the threat landscape evolves (Agyepong et al., 2020; Akinrolabu et al., 2018). SOCs, especially those protecting highly sensitive data, operate on a full-time basis, resulting in a laborious work setting. As such, research is replete with studies of SOC analyst burnout and high rates of attrition (Agyepong et al., 2020; Kokulu et al., 2019; Vielberth et al., 2020). It is for these reasons that enhanced levels of automation are requested, promoting lighter workloads for SOC analysts and increased efficiency of SOCs (Chamkar et al., 2022). However, a lesser focus is paid to the cognitive impact this has on SOC analysts.

SOC Environment

Time criticality and complex problem-solving are two of the main attributes that best describe the context of a SOC. As soon as threats are identified, SOC analysts are under pressure to quarantine the threat's effects and implement remediating solutions (Cummings, 2004; Dykstra et al., 2022; Hámornik & Krasznay, 2018). This is made more difficult due to the evolving threat landscape, where attackers are becoming more intelligent, their attack vectors are harder to pinpoint, and isolating the source is more onerous (Ofte & Katsikas, 2023). Furthermore, the decisions that SOCs make have a significant cost of error associated with them (Ofte & Katsikas, 2023). This illustrates the mentally taxing and demanding side of working in a SOC (Akinrolabu et al. 2018; Schraagen & van de Ven, 2008). Moreover, SOC analysts operate in an environment with a high workload, where multi-tasking is common practice. Many of these tasks are manual and

repetitive – representing prime characteristics for which automation is considered appropriate (Parasuraman & Manzey, 2010).

Similarities to the environment of a SOC can be found in Air Traffic Control (ATC) rooms; Pilot Cockpits; and Military Command and Control Centers (C&C) (De-Arteaga et al., 2020; Mosier et al., 1998). Research in these fields has investigated the adoption of automation and its effects on the human operator. The overarching finding is that performance and efficiency are improved when automated decision aids produce reliable and accurate decisions. However, when the decisions produced by the automated decision aids were incorrect, the impact was detrimental. In these instances, participants not utilizing automation performed better than those operating with incorrect automated decision aids (Metzger & Parasuraman, 2005).

Automation Bias

Automation bias refers to the propensity of individuals to become over-reliant on automated systems and the results/decisions that they generate. This bias persists even when (a) the automated systems produce inaccurate results and/or (b) the individual is in the presence of contradictory, yet correct, information. This contradictory information was generated without the use of automation (De-Arteaga et al., 2020; Skitka et al., 1999). Automation Bias means that humans develop the tendency to unwaveringly trust automation. This leads to situations where human decision-makers do not search for any contradictory, or confirmatory information, which can result in overlooking important details. Within automation bias there exist two classes of errors: *errors of omission* and *errors of commission*. Parasuraman and Manzay (2010) define errors of omission as a situation whereby a human operator fails to detect a critical issue as the automated system fails to provide an alert. These errors are regarded as scenarios where the necessary and required steps/actions are not taken, exhibiting complacent behavior. Thus, errors of omission exemplify how ADAs result in a loss of situation awareness as human operators rely so heavily on being alerted of issues rather than actively seeking them. Here, individuals leverage automation as heuristic replacements (De-Arteaga et al., 2020; Parasuraman et al., 2000; Parasuraman & Manzey, 2010). Contrary to that, errors of commission occur when human operators blindly follow the recommendations of automated systems even though it is incorrect. Based on these definitions, the introduction of automation introduces effects that are perhaps not anticipated. This is echoed by human-in-the-loop research advocates:

> "*Research has shown that automation does not simply supplant human activity but rather changes it, often in ways unintended and unanticipated by the designers of automation; moreover, instances of misuse and disuse of automation are common*" (Parasuraman and Manzey, 2010, p. 01).

The problem statement of this paper highlighted the loss of situation awareness (SA) as a key impact of automation on SOC analysts. SA is measured at an individual level and can be defined as "the process of gathering information about a situation and converting this information into an awareness that can differentiate between the suitability of potential actions" (Ofte and Katsikas, 2023, p. 02). Cyber SA, in the context of SOCs, has been defined as the blend of technical and cognitive aspects that must be measured at the individual, team, and system levels (Ofte & Katsikas, 2023). Cyber SA recognizes the supportive role that systems adopted should play, but states that the SOC analyst must ultimately possess an awareness of their surroundings. Coupled together with the industry-related, contextual knowledge that SOC analysts ought to have, this should holistically equip them with the cognitive ability to make well-informed decisions. Therefore, the four impacts of automation on SOC analysts are:

1. **Loss of situational awareness**
2. **Cognitive skill degradation**
3. **Task complacency**
4. **Lack of vigilant information seeking**

It is also worth noting what the contributing factors of automation bias are:

1. **Path of least cognitive effort** – In the presence of ADAs, humans tend to instantly accept the computer-generated solution as correct (Cummings, 2004). Skitka et al. (1999) contend that humans exert the path of least cognitive effort, illustrating their reliance on automation.

2. **Diffusion of responsibility** – This concept has typically been explored in human-human interaction, where it is more commonly known as 'groupthink'. The diffusion of responsibility asserts that when in the presence of others, individuals assume that the group will solve the problem at hand before they do. Therefore, they do not cognitively engage to the levels that they would have if they were alone (Parasuraman & Manzey, 2010). This concept can be mapped onto human-machine interactions.
3. **Perception of superiority** – Humans may tend to regard automation as being able to outperform humans, and therefore, its decisions must be respected and adopted.
4. **Perception of authority** – Individuals may consider following the recommendations of ADAs from an obedience viewpoint and therefore, will follow through with their instructions.

Parasuraman et al. (2000) introduce automation complacency. This refers to the lack of sufficient monitoring of automated systems and investigates to what degree a human operator will verify and validate the results of automation, before accepting them to be true. Activities such as seeking confirmatory or disconfirmatory evidence of automated results would constitute sufficient monitoring and engagement with automated systems. If these activities are conducted by a SOC analyst, it could be stated that they are less likely to suffer from automation complacency. Based on the definition of automation complacency, errors of omission represent the clearest similarity between the two automation-induced concepts.

SOC Criticality

Both errors of omission and errors of commission experienced in SOCs have detrimental effects. This paper posits that the damage caused by cyber-attacks stretches beyond security breaches and data loss. Sophisticated cyber-attacks bear significant consequences for the masses. These include financial ramifications, reputational damage, and the compromise of sensitive data but can also consist of national states of emergency, disruption of public services, and interference with large communication network operators. The magnitude of these attacks illustrates the importance of SOCs in the pursuit of protecting their respective organization. High-impact cyber-attacks (**Table 2**) were most notably showcased through three significant events spanning the last decade: the Target data breach of 2013, the WannaCry ransomware attack of 2017, and the Colonial Pipeline attack of 2021.

Table 2*:* High-Impact Cyber Attacks – SOC Perspective

Cyber-Attack	***Description***
Target Data Breach	In a combination of spear-phishing and malware planted on point-of-sale devices, attackers were able to breach the defense of a large American retailer, Target. The result was that the confidential credit card information of customers was comprised. It is well-documented that the security team at Target was alerted of this malware but ignored it. Alerts that attackers were moving this data outside of Target's network were lodged but they too were ignored (Kassner, 2015). This breach offers the practical application and insight into automation bias and automation complacency. It could be assumed that given that the automated systems flagged the alerts, and it was received, SOC analysts perceived it to be a false positive. Reports of this breach state that whilst the malware was exposed, SOC analysts believed it to be unique in nature and deemed it non-critical. This is equated to an error of omission, whereby investigative action on an alert was not taken. It is also possible to postulate that an overreliance on increased automation systems led SOC analysts to demonstrate complacent practices, overlooking the significance of the malware alert. Furthermore, it is plausible that SOC analysts were no longer actively monitoring the signals, seeking confirmatory or disconfirmatory information on critical threats. Instead, SOC analysts appeared to have taken a more passive approach, relying on automation to take corrective action if and where needed. Another factor at play could

	have been that the overall LOA in the SOC was too high, leading to the skills of SOC analysts declining over time. This attack highlights that technology, and automation alone, cannot prevent such events—adequate monitoring and observation from SOC analysts with a high degree of situational awareness is essential.
WannaCry	This malware attack was deployed on Windows machines that had failed to install the latest updates, leading to outdated software running on these machines. This attack impacted both individuals and organizations running this software. Victims were demanded to pay a ransom to have their machines restored. If the ransom was not paid, the permanent deletion of files would occur (Palmer, 2017). One organization that felt these effects harder than most was the hospitals on the NHS network in the United Kingdom. It is estimated that up to 70 000 devices in these hospitals were affected. These devices housed patient records, appointment schedules, and diagnostic equipment availability. The attack resulted in the large-scale cancellation of appointments and procedures leading to an overall disruption of the UK healthcare industry. Investigations into the attack revealed that security teams at the NHS were alerted to patch this known vulnerability two months before the attack. Given the nature of this alert, in that it stated that this attack would not target specific entities but rather anyone running the software, it is plausible to think that security analysts at the NHS did not regard it as highly. Whilst there may not exist concrete evidence of what degree automation played in this attack; it highlighted the dangers that exist when outdated and vulnerable systems are not updated. This is regarded as a by-product of overreliance on automation to maintain and update machinery.
Colonial Pipeline Attack	Leveraging leaked credentials allowed attackers to access the Colonial Pipeline systems through a Virtual Private Network (VPN) connection. What makes matters worse is the fact that multi-factor authentication (MFA) was not in place. Through this breach, attackers were able to plant malware that caused Colonial Pipeline to halt all its operations regarding its distribution of petroleum. This led to hikes in fuel prices, country-wide shortages, and a state of emergency being enacted (Osborne, 2021). Whilst it is evident that poor security practices (such as the lack of MFA) were present, it is argued that attentive monitoring of these systems was lacking. For example, it is the responsibility of SOCs to understand their organization's attack graphs and mitigate possible vulnerabilities - the legacy VPN system through which attackers gained remote access should have been terminated. Moreover, the levels of automation that already exist in the SOC could be of a high enough level that has caused a loss of situational awareness. Whilst the exact role that automation did/did not play in this scenario is unknown, there was a lack of human oversight and intervention. This suggests that there is still room for cognitive skill improvement in SOC analysts.

In the examples mentioned, it is evident that these attacks could have been avoided if more careful attention had been paid to by SOC analysts. Furthermore, the prevention measures needed do not represent highly sophisticated strategies. They appear to be more routine cyber hygiene practices, highlighting the potential complacency that exists due to increased automation. Inadequate monitoring and ignoring of alerts exposed Target, the failure to oversee routine software updates costs the NHS severely, and insufficient credential storage and authentication mechanisms employed at Colonial Pipeline led to their demise. All three cases reiterate the need for experienced and cognitively aware analysts who have expert skill sets and are knowledgeable of the environment and context in which they operate. Continuing to implement advanced

levels of automation may only exacerbate the issues currently faced. Instead, the attention towards the SOC analyst needs to be preserved, promoting increased situational awareness, active threat monitoring, and attention to understanding and implementing sophisticated prevention measures.

Critical Success Factors

The primary contribution of this paper is the proposal of four Critical Success Factors (CSFs) for the use of automation and automated decision aids in SOCs to assist in the mitigation of automation bias. These CSFs were derived from the reviewed literature and the emergent themes. CSFs are defined as the key activities, focus areas, and conditions that are imperative for success (Leidecker and Bruno, 1984). Not only must these CSFs be implemented but to reach their potential, they must be sustained. This paper identifies the following CSFs.

1. **Task-based Automation:** Determine the correct balance between automation and the preservation of SOC analyst skills on a singular task level.

Automation should not be implemented in a 'one size fits all' approach. The nature of the task needs to be critically evaluated and defined before determining the degree to which automation should be applied. From this, the correct LOA will be identified. The LOA framework consists of ten levels with Level 1 requiring the human to make all decisions and carry out all actions and Level 10 allowing the computer to act autonomously, disregarding the human (Endsley & Kaber, 1999). Leveraging the LOA framework will assist in understanding the implications on both the SOC analyst and the automated systems at a singular task level. This CSF requires that 3 critical sub-components be assessed before applying automation: Level of complexity, Level of criticality, and Cost of error.

- ***Level of Complexity*:** Routine, well-defined tasks can take on higher levels of automation given that their processes are clear. Complex and ambiguous tasks must adopt lower levels of automation given that they will require more oversight from the SOC analyst. This is because sophisticated attacks may be ambiguous in nature, requiring more involvement and oversight from SOC analysts.
- ***Level of Criticality*:** Tasks with associated threats that are deemed highly critical to business operations, i.e., those whose consequences are severe, must consist of lower levels of automation. Contrary to that, low-level threats that are clearly understood for what they are, and the limited damage they could cause, can adopt higher levels of automation. Less critical attacks may benefit from higher LOA whereby automation can go as far as implementing documented remediation strategies with the SOC analyst's consent.
- ***Cost of Error:*** Alerts with a high cost of error, i.e., if remediation or mitigation strategies are implemented incorrectly, must always have SOC analysts at the forefront. Alternatively, those with a low cost of error have more room for automation to be applied at a higher level.

It is imperative to understand that the combination of these three sub-components consists of various approaches. For example, a high level of complexity does not automatically equate to a high level of criticality. In the same manner, a high level of criticality does not automatically equate to a high cost of error. Whilst this is possible, it is event and threat specific. For example, it is possible that tasks with a high level of complexity are related to threats with a low level of criticality. However, these same tasks may have a high cost of error if they are not performed correctly.

2. **Process-based Automation:** Identify the process for which automation is to be applied as this provides a clear understanding of the cognitive impact on a SOC analyst.

Parasuraman and Sheridan (2000) state that automation is applied at different phases of a process, namely: information acquisition, information analysis, decision & action selection, and action implementation. Based on its definition, it is evident that automation bias is more prevalent in the latter two stages, decision & action selection and action implementation – where ADAs are focused. It is for this reason that automation in these two stages must not exceed LOA 6: automation executes a suggestion if the SOC analyst approves of it; or allows the SOC analyst a restricted time to veto the decision before automatically

executing. SOC analysts must be the only entities to ensure that the correct remediation strategies are carried out promptly. ADAs must be employed in a supportive manner, rather than infringing upon the decision-making of SOC analysts. As humans remain to be the key decision makers within SOCs, ADAs can assist the analyst in recommending multiple appropriate mitigation strategies, together with their strengths and weaknesses, to SOC analysts. It is positioned that LOA 7 and above, where automation starts behaving autonomously with limited human oversight, provide ripe conditions for automation bias and SOC analyst's skill degradation. Alternatively, when considering the first two phases, automation could significantly enhance this process, presenting the SOC analyst with a filtered view of important alerts. It is here where automation must be implemented to assist SOC analysts with the voluminous notification backlog and present the most severe alerts. In this case, automation is assisting with manual and repetitive tasks on behalf of the SOC analyst. This allows the SOC analyst to allocate time toward high-priority security incidents (Akinrolabu et al., 2018; Cummings, 2017). For example, log collection, correlation, and analysis activities can filter out non-critical alerts and analyze the remaining ones. Not only does this take care of mundane and repetitive tasks but it conducts initial analysis on those deemed important. Automated systems will still need to make decisions in this stage of the process in terms of what to deem critical and filter, versus what is not.

3. **Automation Performance Appraisal:** Conducting performance appraisal of ADA systems and validating their decisions will make SOC analysts more cognizant of the reliability and accuracy of automation.

This paper has referred to the interaction of the SOC analyst and automation (human-machine) and how to ensure that neither infringe upon the other. Therefore, automation and ADAs are thought of as 'team members' to SOC analysts and as a result, must be rated on their performance in the same manner the employees are. Frequent validation measurements of both the automation systems and the SOC analyst's performance are needed to ensure that both are producing the desired results. The performance must be measured holistically as it will yield insights into the efficiency of the SOC, reliability of automation, and knowledge/skillset growth areas of the SOC analyst. If it is found that: the results of automation are never challenged; decisions produced by ADAs are always implemented; and the performance ratings of SOC analysts are declining, then this is an indication that automation bias and complacency are occurring.

4. **SOC Analyst Training of Automated Systems:** Training SOC analysts to understand and interpret decisions made by ADA systems will promote critical thinking, the development of their threat mitigation skills, and an increased awareness of automation bias and complacency.

The workload that SOCs face, coupled with the intelligence that ADAs can offer, means that automation can provide benefits to a team of SOC analysts. This study does not advocate for less automation to be employed but rather that caution must be applied when integrating it. Automation in a SOC is meant to act as a force multiplier, meaning that it must strengthen and augment the skills of the SOC analyst whilst creating an effective environment. If the SOC analyst is to experience this benefit, ADAs must not replace the core tasks of the SOC analyst. The SOC analyst must be able to leverage automation for the validation of results and insights into possible strategies based on a predefined set of criteria. For this to be achieved, the SOC analyst must be trained to understand how the automation functions as well as be aware of the risk of automation bias. A SOC analyst is not merely meant to implement an ADA decision but rather, the SOC analyst must foster the necessary skills to interpret the decisions made by ADAs. To realize this, ADAs must produce decision trees with contextual reasoning alongside each decision made. This will prevent both automation bias and complacency whilst encouraging the SOC analyst to engage in critical thinking. Critical thinking will develop the cognitive heuristics of knowing how to arrive at a particular decision without automation in the case that automation is either not available or has failed.

These CSFs ensure that humans are in the loop and at the center of automation implementation in SOCs. When implementing automation, humans must guide this process and define what automation must achieve without encroaching on the SOC analyst's skillset. A delicate balance between automation-led activities versus human-led activities must exist. Automation should gather, summarize, and present threat-related information to the SOC analyst, but it is the human that possesses the explicit knowledge and

expertise to make the final decision. Thus, it must be up to the SOC analyst to verify automated results and implement corrective action where appropriate. Previously, the influences of automation bias as well as the impact that can be felt on the SOC analyst were highlighted. These concepts, taken together with the CSFs that were developed based on the literature review conducted, are depicted in **Figure 1**.

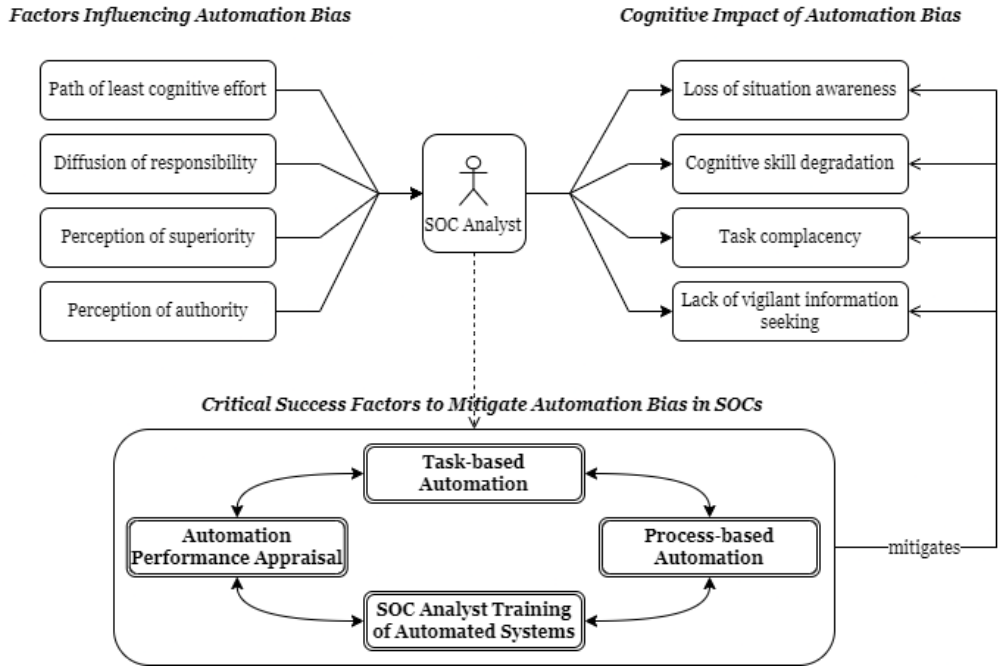

Figure 1: Influence, Impact, and Mitigation of Automation Bias Model

Limitations and Future Work

This study offers insights into the impact that automation has on SOC analysts, namely, automation bias. However, there are limitations to what has been discussed. Understanding the cognitive effects of automation bias on SOC analysts have not been tested in the SOC environment. This means that the insights provided in this paper are not supported by interviews with SOC analysts. Further, automation bias may not be the sole factor that impacts the cognitive ability of SOC analysts and thus, there may exist other factors that have not been discussed. Future work intends to validate the CSFs developed through the collection of empirical data that compares and contrasts the impact of automation on SOC analysts. This will allow for the Automation Bias Model to be updated either through the addition, removal, or merging of CSFs. Furthermore, measurement scales that measure automation bias and complacency have previously been developed and validated (Merritt et al., 2019; Singh et al., 1993). These tools measure attitudes towards monitoring automated systems, while the latter aims to measure confidence in these systems, reliability of the decisions made, trust in automation, and safety perceptions of ADAs. This will result in gaining an understanding of SOC analysts' intentions toward using automation. Contrary to this, the rapid development of automation tools, either resulting from the advancement of artificial intelligence or machine learning, must be seriously considered. It is beyond the scope as well as the expectation of SOC analysts to bear a full load of triaging incoming security alerts. However, identifying the balance point of how these two entities can enrich one another holds equal importance.

Conclusion

SOC analysts face a series of challenges which include dealing with an immense amount of security alerts and having to make important decisions in a time-sensitive manner. Automation assists in easing the workload and creating a more efficient environment. Further, automation should be employed in a SOC to assist in developing the cognitive skills of SOC analysts. The effects that this has on the cognitive ability of the SOC analyst need to be carefully considered. This is because, in the presence of automation, SOC

analysts become complacent, regardless of whether the automation is correct or not. Automation that generates undisputed results may provide short-term benefits in the form of enhanced efficiency and effectiveness. However, even in this instance, long-term adverse impacts on the cognitive competence of the SOC analyst arise. This is because, over time, automation results in the decline of a SOC analyst's skillset. In the opposite event that automation generates results that are inaccurate and unreliable, the negative impacts would not only be felt by the SOC analysts but would spill over into the organization (De-Arteaga et al., 2020). More efficient practices are needed in SOCs and one way to achieve this is using automation. However, the drive for efficiency must ensure that additional risk is not incurred to the organization and that a balance between automation and human activity is achieved. Before increased automation, SOC analysts were actively monitoring security alerts and patrolling the organization's security perimeters. However, automation leads SOC analysts to engage in more passive practices. This paper recommends that when adopting automation in a SOC environment, adherence to the identified critical success factors is maintained.

References

Agyepong, E., Cherdantseva, Y., Reinecke, P., & Burnap, P. (2020). Challenges and performance metrics for security operations center analysts: A systematic review. *Journal of Cyber Security Technology*, *4*(3), 125–152. https://doi.org/10.1080/23742917.2019.1698178

Akinrolabu, O., Agrafiotis, I., & Erola, A. (2018). The challenge of detecting sophisticated attacks: Insights from SOC Analysts. *Proceedings of the 13th International Conference on Availability, Reliability, and Security*, 1–9. https://doi.org/10.1145/3230833.3233280

Chamkar, S. A., Maleh, Y., & Gherabi, N. (2022). The Human Factor Capabilities in Security Operation Centers (SOC). *EDPACS*, *66*(1), 1–14. https://doi.org/10.1080/07366981.2021.1977026

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology* (NIST SP 800-61r2; p. NIST SP 800-61r2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

Cummings, M. L. (2004). *Automation Bias in Intelligent Time Critical Decision Support Systems*. American Institute for Aeronautics and Astronautics First Intelligent Systems Technical Conference, Reston, VA. https://web.archive.org/web/20051218092750id_/http://web.mit.edu:80/aeroastro/www/labs/halab/papers/CummingsAIAAbias.pdf

De-Arteaga, M., Fogliato, R., & Chouldechova, A. (2020). A Case for Humans-in-the-Loop: Decisions in the Presence of Erroneous Algorithmic Scores. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–12. https://doi.org/10.1145/3313831.3376638

Dykstra, J., Met, J., Backert, N., Mattie, R., & Hough, D. (2022). Action Bias and the Two Most Dangerous Words in Cybersecurity Incident Response: An Argument for More Measured Incident Response. *IEEE Security & Privacy*, *20*(3), 102–106. https://doi.org/10.1109/MSEC.2022.3159471

Endsley, M. R., & Kaber, D. B. (1999). Level of automation effects on performance, situation awareness, and workload in a dynamic control task. *Ergonomics*, *42*(3), 462–492. https://doi.org/10.1080/001401399185595

Hámornik, B. P., & Krasznay, C. (2018). A Team-Level Perspective of Human Factors in Cyber Security: Security Operations Centers. In D. Nicholson (Ed.), *Advances in Human Factors in Cybersecurity* (Vol. 593, pp. 224–236). Springer International Publishing. https://doi.org/10.1007/978-3-319-60585-2_21

Kassner, M (2015, February 2). Anatomy of the Target data breach: Missed opportunities and lessons learned. ZDNet/tech. https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

Kokulu, F. B., Soneji, A., Bao, T., Shoshitaishvili, Y., Zhao, Z., Doupé, A., & Ahn, G.-J. (2019). Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues.

Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 1955–1970. https://doi.org/10.1145/3319535.3354239

Merritt, S. M., Ako-Brew, A., Bryant, W. J., Staley, A., McKenna, M., Leone, A., & Shirase, L. (2019). Automation-Induced Complacency Potential: Development and Validation of a New Scale. *Frontiers in Psychology*, *10*, 225. https://doi.org/10.3389/fpsyg.2019.00225

Metzger, U., & Parasuraman, R. (2005). Automation in Future Air Traffic Management: Effects of Decision Aid Reliability on Controller Performance and Mental Workload. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *47*(1), 35–49. https://doi.org/10.1518/0018720053653802

Miloslavskaya, N. (2016). Security Operations Centers for Information Security Incident Management. *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, 131–136. https://doi.org/10.1109/FiCloud.2016.26

Mosier, K. L., Skitka, L. J., Heers, S., & Burdick, M. (1998). Automation Bias: Decision Making and Performance in High-Tech Cockpits. *The International Journal of Aviation Psychology*, *8*(1), 47–63. https://doi.org/10.1207/s15327108ijap0801_3

Naseer, H., Maynard, S. B., & Desouza, K. C. (2021). Demystifying analytical information processing capability: The case of cybersecurity incident response. *Decision Support Systems*, *143*, 113476. https://doi.org/10.1016/j.dss.2020.113476

Ofte, H. J., & Katsikas, S. (2023). Understanding situation awareness in SOCs, a systematic literature review. *Computers & Security*, *126*, 103069. https://doi.org/10.1016/j.cose.2022.103069

Osborne, C. (2021, May 13). *Colonial Pipeline ransomware attack: Everything you need to know*. ZDNet/tech. https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/

Palmer, D. (2017, October 27). *WannaCry ransomware: Hospitals were warned to patch systems to protect against cyber-attack - but didn't*. ZDNet/tech. https://www.zdnet.com/article/wannacry-ransomware-hospitals-were-warned-to-patch-system-to-protect-against-cyber-attack-but-didn't/

Parasuraman, R., & Manzey, D. H. (2010). Complacency and Bias in Human Use of Automation: An Attentional Integration. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *52*(3), 381–410. https://doi.org/10.1177/0018720810376055

Parasuraman, R., Sheridan, T. B., & Wickens, C. D. (2000). A model for types and levels of human interaction with automation. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, *30*(3), 286–297. https://doi.org/10.1109/3468.844354

Singh, I. L., Molloy, R., & Parasuraman, R. (1993). Individual Differences in Monitoring Failures of Automation. *The Journal of General Psychology*, *120*(3), 357–373. https://doi.org/10.1080/00221309.1993.9711153

Skitka, L. J., Mosier, K. L., & Burdick, M. (1999). Does automation bias decision-making? *International Journal of Human-Computer Studies*, *51*(5), 991–1006. https://doi.org/10.1006/ijhc.1999.0252

Vielberth, M., Bohm, F., Fichtinger, I., & Pernul, G. (2020). Security Operations Center: A Systematic Study and Open Challenges. *IEEE Access*, *8*, 227756–227779. https://doi.org/10.1109/ACCESS.2020.3045514