Mismatched SOCs: A Case Study of Cybersecurity Goal Incongruency within an Academic SOC

Wellington Tatenda Gwavava
The University of Tulsa
School of Cyber Studies
wellington-gwavava@utulsa.edu

Andrew Morin
The University of Tulsa
School of Cyber Studies
andrew-morin@utulsa.edu

***Abstract*—As the cost and frequency of cybersecurity incidents continue to rise, so too has the pressure on security operation centers (SOC) to perform efficiently. This has forced cybersecurity leadership, such as chief information security officers (CISOs), into an arduous balancing act of maintaining a cost-effective cybersecurity posture while simultaneously retaining an efficient cybersecurity workforce. To meet both of these goals, SOC leadership will often track key performance indicators (KPIs) related to the daily tasks performed by SOC analysts. While these quantitative metrics allow SOC leadership to monitor certain analyst performance patterns, the evaluation of analysts based on these imperfect measurements may lead to undesirable operant conditioning. As such, it is not immediately obvious how, or even if, these KPIs improve upon the larger goals envisioned by organizational leadership. In this paper, we perform a mixed-methods case study of an academic SOC to determine how well KPIs translate the organizational goals from cybersecurity leadership to SOC analysts. Specifically, we use qualitative surveys and interviews, as well as quantitative KPI measurements from analysts to determine the congruency of CISO and SOC analyst goals. We find that analysts who perform well across KPIs are not necessarily the best at furthering SOC goals, and vice versa. We find that within this specific SOC, analysts appear to be incentivized to deviate from organizational cybersecurity goals in pursuit of better KPI scores.**

I. Introduction

Security Operations Centers (SOCs) are critical to organizational cybersecurity, serving as the first line of defense against evolving cyber threats. By leveraging advanced tools and skilled analysts, SOCs monitor networks, detect anomalies, and respond to incidents in real-time. However, despite their central role, SOCs face persistent challenges such as high analyst burnout, alert fatigue, and struggles to demonstrate their organizational value effectively [1], [2]. A common solution to these problems is the liberal use of key performance indicators (KPIs) which track analyst metrics within the SOC. These quantitative KPIs, such as mean time to remediation (MTTR) and ticket closure rates, are relatively easy to track, although not always an accurate representation of performance. For example, an experienced and knowledgeable analyst may elect to handle the most complex - likely time-consuming - alerts, resulting in a low ticket closure rate. Despite the unreliable nature of these metrics for measuring analyst performance [3], [4], they remain an industry standard, often coupled with qualitative assessments to account for the quantitative shortcomings. While a competent and efficient SOC analyst may score poorly according to KPIs, it is also possible that an unskilled and ineffective analyst could maintain high KPI scores. Prioritizing easy tickets, hurriedly reviewing alerts, and providing quick but incomprehensive documentation could all lead to improved KPIs while sabotaging organizational cybersecurity goals. This begs the question: *Are these KPIs simply imperfect measures of SOC analyst performance, or does the pursuit of improved KPI metrics directly contradict organizational cybersecurity goals?*

The disconnect between KPI-driven evaluations and organizational objectives highlights a significant, yet under-explored, problem of goal congruence. Goal congruence, or the alignment of goals across organizational hierarchies, is essential for cohesive operations in high-stakes environments such as SOCs. Within this hierarchy, the Chief Information Security Officer (CISO) plays a pivotal role in defining the strategic priorities of the SOC, translating the organization's risk tolerance and cybersecurity goals into operational objectives. These priorities often encompass not only technical efficiency—such as rapid incident response and remediation—but also broader goals like fostering collaboration, improving knowledge retention, and aligning day-to-day analyst activities with long-term security strategies. Without such alignment, SOCs risk focusing on easily quantifiable metrics at the expense of strategic cybersecurity priorities, leading to suboptimal performance and weakened organizational defenses. This issue is particularly pronounced in academic SOCs, where the transient nature of student analysts adds further complexity.

While prior research has explored SOC performance metrics and analyst challenges [2]–[6], a study of how organizational leadership translates strategic objectives into actionable goals for SOC analysts is yet to be performed. This paper uses an academic SOC as a case study to explore the alignment — or lack thereof — between SOC leadership goals and KPI-driven analyst goals. Using a mixed-methods approach, we combine qualitative insights from leadership interviews

Workshop on Security Operation Center Operations and Construction (WOSOC) 2025
24 February 2025, San Diego, CA, USA
ISBN 979-8-9919276-0-4
https://dx.doi.org/10.14722/wosoc.2025.23013
www.ndss-symposium.org

with quantitative KPI data assessed from tools the SOC to assess goal congruence. A case study with mixed-methods research is particularly suited to this topic, as it allows the integration of numerical data with rich qualitative insights to capture the complexity of organizational phenomena [7]. Furthermore, case studies provide an in-depth examination of context-specific dynamics, making them ideal for exploring nuanced interactions between SOC leadership and analysts [8].

This study makes three key contributions. First, a case study of an academic SOC provides empirical evidence of cybersecurity goal incongruency resulting from the misalignment between KPI metrics and organizational goals. Second, we introduce a process for measuring goal congruence within SOCs using a combination of quantitative and qualitative data. Finally, the results offer insights for SOC managers and CISOs to improve analyst performance evaluations, fostering a balance between technical efficiency and strategic alignment.

The remainder of this paper is organized as follows. Section II reviews related work on SOC performance metrics and goal alignment theories. Section III details the methodology, including data collection and analysis processes. Section IV present findings from a case study of an academic SOC. Finally, Section V discusses implications for research and practice, and Section VI concludes.

II. Related Work

A Security Operations Center (SOC) acts as an organizational command center dedicated to maintaining cybersecurity [3]. SOCs consist of several elements—personnel with varying skills, structured operational processes, and sophisticated technology—each crucial to SOC performance from both technical and economic standpoints. Studies often employ the People, Processes, and Technologies (PPT) framework to categorize these components and assess SOC effectiveness [9]. This framework highlights the importance of integrating skilled analysts, robust processes, and sophisticated tools to achieve cybersecurity goals. However, research on SOC performance metrics focuses disproportionately on technological and process-oriented metrics, leaving the human aspect, particularly goal alignment, underexplored [4]. This underscores the need for a more holistic understanding of SOC performance that considers technical efficiency and the alignment of human efforts with organizational cybersecurity goals.

In addition to the PPT framework, General Systems Theory (GST) provides a theoretical lens for understanding SOCs as dynamic, interdependent systems. GST posits that organizations function as interconnected networks of people, processes, and technologies, where changes in one component can significantly impact the others [10]. Applying GST to SOCs reveals the critical role of alignment between leadership priorities and analyst activities in ensuring cohesive cybersecurity operations. Leadership priorities must be clearly translated into actionable goals for SOC analysts. This alignment is particularly relevant in academic SOCs, where the transient nature of student analysts adds complexity to goal congruence.

Within a SOC, analysts play a critical role in identifying, analyzing, and responding to security incidents. Their performance is influenced by several factors, including workload, access to tools, skill level, and organizational support systems. The CISO sets the strategic direction for the SOC, prioritizing security objectives based on risk tolerance and organizational needs. Effective SOCs ensure that analyst activities align with CISO-defined priorities. The CISO uses various performance measurement metrics to assess analyst effectiveness, ideally reflecting CISO priorities. These metrics often include time to identify threats, accuracy of incident classification, and efficacy of response actions, all within the context of CISO-defined priorities [5]. This emphasizes the importance of goal congruence, where individual analyst objectives are in harmony with the broader organizational cybersecurity strategy.

Building upon the understanding we derive from GST reveals a hierarchical structure of stakeholders within a SOC, ranging from the organization level down to individual analysts. The concept of "goal congruency" is particularly relevant here. Goal congruency refers to the alignment of goals across different levels within an organization [11]. In a SOC, this means that the individual aspirations of SOC analysts should align with the objectives set by the SOC manager, which in turn align with the broader strategic vision of the CISO and the overarching goals of the organization. This alignment fosters a unified approach, enabling the entire SOC to work cohesively towards a common cybersecurity strategy.

The "value of congruence" lies in an organization communicating its values and the behaviors it expects from its employees. Research [12] shows that when employees feel that there is alignment (congruence) between their values and those of the organization, they are more likely to experience job satisfaction. [13] research has shown that there is a positive relationship between a positive "value of congruence" and positive performance at various layers of the company. This insight suggests that congruence within a SOC can enhance its overall performance, while misalignment may highlight underlying weaknesses. Consequently, fostering value congruence within a SOC can serve as both a performance enhancer and a diagnostic tool for identifying potential areas of improvement.

Goal congruence is essential in organizational management, particularly in aligning stakeholders' objectives to ensure cohesive efforts toward overarching goals. In cybersecurity, aligning the goals of CISOs and SOC analysts is critical for effective security management. [14] explores the relationship between members' agreement on organizational goals and their attitudes, demonstrating the importance of congruence for organizational success. In the cybersecurity space, this is important as from the PPT framework; people play a critical role in the overall performance of the SOC and it is essential that they work together to improve cybersecurity posture. In this context, [15] defines "Goal Congruence" as agreement by all members of a team on a common set of objectives, which is positively associated with team cohesion, performance, and outcomes. Notably, the research introduces an empirical framework for quantifying congruence based on

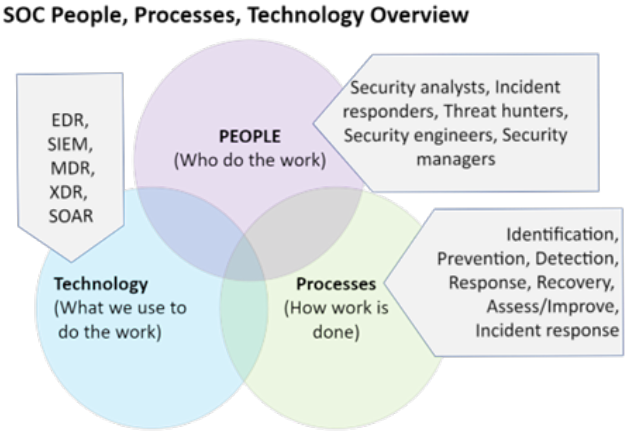

Fig. 1. People, Processes, and Technologies (PPT) framework adapted from Vielberth et al., which illustrates the interconnectedness of the three core components within a SOC.

goal similarity, providing a measurable perspective on its organizational impact. This approach underscores the significance of congruence in operations and can be related to SOCs.

We can also see how the concept of goal congruence is pivotal in organizational management, particularly in aligning the objectives of different stakeholders within an organization to ensure that everyone is working towards the same overarching goals. This theory is especially relevant in the context of cybersecurity, where the alignment of goals between CISOs and SOC analysts is crucial for effective security management. Some areas in which this theory applies are supported by different research such as; *Inclusive Leadership and Turnover Intention* [16], which explores the role of inclusive leadership in enhancing follower-leader goal congruence, subsequently improving organizational commitment and reducing turnover intentions. This research underscores the importance of leadership styles that foster goal alignment among team members, which is directly applicable to the relationship between CISOs, who are beholden to organizational goals, and SOC analysts. [17] discusses *Formal Learning and Organizational Performance*; how formal learning processes within organizations can be optimized by aligning the goals of the organization with the learning objectives of the employees. This alignment, or goal congruence, is crucial for ensuring that training and development initiatives contribute effectively to organizational objectives, similar to training programs for SOC analysts that should align with the strategic security goals set by the CISO. *Addressing Agency Problem in Employee* [18] focuses on the role of goal congruence in resolving conflicts between management and employees during training programs. It highlights the importance of aligning employee training with organizational goals to enhance training effectiveness, which is relevant for SOC analysts' training being aligned with the CISO's strategic security objectives. *Factors Affecting the Sustainability of Public-Private Collaborations in Research* , [19] uses goal congruence theory to analyze how public and private sectors can align their goals in urban collaborations. This principle can be extrapolated to show how internal stakeholders within an organization, like a CISO and SOC analysts, can align their security-related goals for better organizational outcomes. [20] also explores the relationship between members' agreement on organizational goals and their attitudes, demonstrating the importance of congruence for organizational success. This is particularly important in SOCs, where the human factor is crucial for overall performance. These studies collectively emphasize the necessity of aligning leadership, training, and team objectives within SOCs to enhance cybersecurity outcomes and underscore the significance of congruence in SOC operations.

The alignment of goals between organizational leadership and SOC analysts ensures that all stakeholders are working towards the same security objectives. A potential gap between senior leadership goals and the analysts' daily activities can lead to sub-optimal performance and compromise the SOC's effectiveness. [21] introduces a constructive/destructive congruence model that describes several possible scenarios for goal congruence, ranging from the most favorable 'constructive goal congruence' to the least favorable 'destructive goal incongruence.' In the context of SOCs, constructive goal congruence means that SOC analysts, SOC managers, the CISO, and all other stakeholders are prioritizing the same goals. On the other hand, the research also describes 'destructive goal incongruence' as a failure to communicate goals across the organization, where employees do not accept the goals being communicated to them. Instead, employees have different self-interests and are reluctant to put them aside for the organization's goals. In a SOC, this might manifest as analysts prioritizing personal metrics, such as the number of tickets closed, over collaborative knowledge sharing or mentoring junior analysts, even though the latter contributes to the long-term health and effectiveness of the SOC.

This paper aims to explore the relationship between organizational cybersecurity goals as set by CISOs and SOC analyst goals promoted by KPIs. By conducting an in-depth case study

evaluating goal congruence within an academic SOC, this study provides insights into the effectiveness of current KPI-driven performance assessments. Additionally, we propose a methodology to assess and improve goal alignment, offering practical recommendations for SOC managers and CISOs to enhance team performance and cohesion. Our findings highlight the challenges of achieving goal congruence within a SOC environment and identify potential contributing factors to misalignment.

III. Methodology

This study employs a case study methodology as its primary framework to explore the alignment between SOC analyst performance and senior leadership priorities. Case studies are well-suited for investigating complex organizational phenomena, such as goal congruence, within a real-world context. The case study approach allows for an in-depth examination of how leadership objectives translate into operational practices and performance metrics, providing actionable insights specific to SOC environments. By focusing on a single academic SOC, this research captures nuanced dynamics that would be difficult to uncover through broader, generalized methods. Once identified, the characteristics of goal translation through an academic SOC can be expanded upon in future work related to contextual understanding of goals within complex organizations [8]. This study was reviewed and deemed exempt by an Institutional Review Board. This study utilizes a four-step mixed-methods approach to assess goal congruency comprehensively:

1) **Cybersecurity Goal Interviews**: Semi-structured interviews were conducted with key stakeholders, including the Chief Information Security Officer (CISO) and SOC manager, to gain insights into their perceptions of SOC analyst performance and organizational goals. The interviews were designed following established qualitative research protocols [22]–[24], ensuring validity and reliability. The interview responses were then used to isolate specific organizational cybersecurity goals.
2) **Qualitative Survey**: The goals identified from the preceding interviews were then used to construct a survey related to organizational cybersecurity goals. The survey used a five-point Likert scale to rate analysts on their performance related to the leadership-defined goals.
3) **Quantitative Data Collection**: Performance data were collected from the SOC's active tools, with a focus on widely recognized KPIs, such as mean time to remediation (MTTR), total tickets handled, and time spent on false positives. These KPIs are based on frameworks cited in research [6], [25]–[27].
4) **Comparative Analysis**: Survey scores and KPI metrics were then compared to identify alignment or discrepancies between subjective leadership evaluations and objective performance indicators. This dual perspective highlights potential gaps in the effectiveness of KPI-based assessments.

This approach enables the integration of subjective leadership perspectives with objective performance data, producing a multidimensional understanding of organizational dynamics. Thematic analysis was applied to the interview data to identify key goals and expectations expressed by SOC leadership. This process involved coding interview transcripts for recurring themes and aligning them with organizational objectives as defined by SOC leadership. The survey responses were analyzed for patterns, and KPI metrics were evaluated using ranking and scoring systems to quantify individual analyst performance. This hybrid approach ensures that both subjective and objective dimensions of analyst performance are accounted for, providing a nuanced understanding of organizational alignment.

The research framework adopted in this study addresses critical research gaps in the alignment of leadership goals with operational practices in SOCs. By systematically analyzing both subjective evaluations and objective metrics, the research provides a robust and nuanced understanding of organizational goal congruence. This framework advances theoretical understanding and offers practical insights for improving SOC performance evaluation systems. The findings not only address the immediate challenges in academic SOC environments but also provide a scalable framework for investigating goal alignment in other technical and operational contexts. Future research can expand on this methodology to explore diverse SOC settings, ensuring broader applicability and deeper insights into the interplay between leadership priorities and analyst performance.

A. Cybersecurity Goal Interviews

Before an evaluation of goal congruence can be performed, the goals perceived by SOC leadership must first be defined. To this end, we begin with a semi-structured interview of SOC leadership (CISO and SOC manager) to elicit these goals. The interview questions are designed to uncover detailed insights about the expectations, priorities, and performance metrics relevant to SOC operations and analyst performance beyond what the KPIs would track. To achieve this, we asked four open-ended questions which invite a qualitative response.

The first question asked is: *"What does the organization expect from the SOC?"* This question aims to understand the broader organizational goals and expectations for the SOC as understood by SOC leadership. Additionally, this question provides context for the CISO's priorities and the SOC manager's expectations.

Next, we ask: *"What are your strategic goals for the SOC?"* This question directly targets the leadership priorities, revealing the specific objectives they have set for the SOC and how they align with the organization's overall cybersecurity strategy. By asking this question second, we offer the SOC leadership an opportunity to offer goals that may not fit within those expected by the organization.

The third question we ask is: *"How do you measure the performance of the SOC?"* This question focuses on the KPIs used to evaluate the effectiveness of the SOC. Although

the SOC may not be explicitly tracking these metrics, we can use these responses to identify which KPIs they relate to. Responses to this question may also reveal important performance metrics not related to any of the commonly tracked KPIs.

Finally, we ask: *"What skills and competencies do you believe are crucial for lower-tier analysts?*" This question delves into what the SOC leadership expects of analyst performance. The responses reveal specific skills and competencies they deem essential for success, particularly at an early stage in the analyst's career. This information can be compared to the KPIs to identify any gaps in performance evaluation.

B. Qualitative Survey

Based on the responses to the interview questions, a thematic analysis is performed to identify common goals across SOC leadership. First, the interview data is transcribed and reviewed to gain a comprehensive understanding of the perspectives of the Chief Information Security Officer (CISO) and SOC manager. Thematic analysis is then employed to identify recurring themes and patterns in the data, and similar codes are grouped into broader themes related to SOC goals, such as technical proficiency, collaboration and mentorship, and learning and development. This process is informed by established qualitative research methods and best practices for conducting case studies and thematic analysis. [8], [28] Once the thematic analysis is complete, the identified goals are used to construct a survey for SOC leadership to complete. The survey uses a five-point Linkert scale to evaluate how well an analyst meets the previously identified cybersecurity goals. Compiling the survey responses allows for a ranking of SOC analysts based on their adherence to SOC leadership-identified goals. This ranking can then be used to determine how well an analyst's performance aligns with the organizational cybersecurity goals as understood by SOC leadership.

C. Quantitative Data Collection

Key Performance Indicators (KPIs) derived from research by [3], [5], [6], [26], [27] were used to evaluate SOC analyst performance quantitatively. These metrics provide a comprehensive understanding of SOC efficiency and effectiveness. Together, these studies offer a robust framework for evaluating SOC analyst performance, combining systematic methodologies with detailed technical metrics. We use these findings to select a subset of metrics obtainable from the tools used within the SOC we are evaluating. These metrics, described below, provide a quantitative view of how each analyst is performing in the SOC.

1) Mean Time to Remediation: Mean time to remediation (MTTR) is a metric that represents the total time from when a ticket is opened by the analyst until it is closed. It combines the mean time to detect, mean time to respond, and mean time to remediate. It is significant because MTTR is a critical indicator of the overall efficiency of the SOC in addressing and resolving incidents promptly. A lower MTTR suggests that the SOC analyst is effective in quickly identifying, responding to, and resolving security incidents, thereby minimizing potential damage and downtime.

2) Tickets Done by Analyst: Tickets done by analyst is a metric that shows the number of incidents each analyst handles, tracked from the total number of tickets the analyst has closed. It is significant because the number of tickets done by an analyst reflects their workload and productivity. It provides insight into the capacity and efficiency of individual analysts in managing and resolving security incidents. High productivity in this context indicates an analyst's ability to handle a significant volume of incidents effectively.

3) Tickets by Severity: Tickets by severity is a metric that indicates the severity of tickets handled by analysts. It assigns higher scores for tickets of high severity compared to medium and low severity. It is significant because tickets by severity provide a more contextual description of workload complexity compared to the total number of tickets alone. This metric reflects the complexity and criticality of the incidents managed by the analyst, offering a nuanced view of their performance in handling high-stakes situations.

4) Average Time Spent on False Positives: The average time spent on false positives is a metric derived from the false positive rate, which is the percentage of security alerts identified as false positives out of the total number of alerts. It is significant because the average time spent on false positives helps assess the accuracy of threat detection and the efficiency of analysts in identifying genuine threats. A lower average time indicates that analysts are proficient in quickly discerning false positives, allowing them to focus more on actual threats and improving the overall effectiveness of the SOC.

Utilizing these metrics allows us to comprehensively evaluate the performance of SOC analysts. These metrics provide valuable insights into their efficiency, workload management, ability to handle complex incidents, and accuracy in threat detection.

D. Comparative Analysis

In the comparative analysis, the qualitative survey responses capturing leadership-defined goals are compared to the quantitative KPI scores to identify areas of alignment or misalignment. The survey responses are compiled, and the analysts are ranked based on their adherence to the goals identified by SOC leadership. This ranking is then compared to the analysts' performance on key performance indicators (KPIs) to determine the degree of goal congruence within the SOC. A misalignment of goals might be evident if analysts who score highly on the survey exhibit low performance on the KPIs, or vice versa.

IV. Case Study: Academic SOC

We perform a case study of this process to determine its effectiveness at quantifying goal congruency. This case study investigates a student-run SOC at a university. This SOC utilizes eleven part-time Tier 1 student analysts during academic semesters and two full-time Tier 2 analysts for continuous operation. Tier 1 analysts focus on initial threat

Student SOC Analyst Performance Survey
1. Work Ethic & Diligence: This analyst consistently dedicates the necessary time and effort to complete their assigned tasks.
2. Learning & Development: This analyst actively seeks opportunities to learn new skills and improve their existing abilities.
3. Proactive Problem Solving: This analyst demonstrates initiative in identifying and resolving problems, and effectively handles security incidents.
4. Technical Proficiency: This analyst effectively uses and understands the tools and systems employed within the SOC.
5. Knowledge & Curiosity: This analyst consistently seeks out new information and knowledge to broaden their understanding of cybersecurity.
6. Team Collaboration & Mentorship: This analyst willingly assists and mentors other team members, contributing to a positive and collaborative work environment.
7. Communication Skills: This analyst communicates their findings and recommendations clearly, concisely, and effectively, both verbally and in writing.
8. Accountability & Ownership: This analyst takes full responsibility for their actions, decisions, and the outcomes of their work.
9. Openness to Feedback & Ideas: This analyst is open to receiving feedback and actively contributes their own ideas and opinions to discussions

TABLE I
SURVEY QUESTIONS DERIVED FROM SOC LEADERSHIP'S EXPECTATIONS TAKEN FROM THE INTERVIEW

detection and escalation, while Tier 2 analysts handle in-depth investigation and response. One Tier 2 analyst serves as the SOC manager responsible for daily training, monitoring, and student supervision, and reports to the university CISO.

A. SOC Goals and Survey

To identify SOC leadership goals beyond KPIs, we perform in-depth interviews with the CISO and SOC manager using the questions described in Section III. Each interview lasted approximately one hour, and was recorded for future analysis. Thematic analysis of the recordings revealed nine key expectations of analyst performance centered around CISO strategic priorities, SOC manager operational expectations, and performance metrics used for SOC and analyst evaluation. Identified expectations can be seen in the survey in Table I.

Using these nine expectations, a survey was constructed which asks how an analyst conforms to each goal. The possible responses include "strongly disagree," "disagree," "neutral," "agree," and "strongly agree." Each response is assigned a value, from -2 to 2 respectively. The survey was provided to the SOC manager, who interacts directly with the analysts.

The survey results, seen in Table II, show how each analyst performs with respect to each of the nine identified SOC analyst performance goals. The table ranks the analysts in descending order of total score, where a higher total score implies better performance.

The highest-rated analyst, analyst H, was one point shy of a perfect ranking. The only goal they lacked a "strongly agree" rating for was technical proficiency, which was the lowest-scored goal across the entire survey. This is not surprising, as the SOC is operated by junior analysts in an academic setting. However, tied for third lowest overall is the second survey question which states that "this analyst actively seeks opportunities to learn new skills and improve their existing abilities."

The four lowest analysts received negative ratings for multiple goals. Aside from technical proficiency, the largest contributors to this negative score were: work ethic, collaboration and mentorship, communication skills, and openness to feedback. Interestingly, the SOC manager offered an "agree" response to both technical proficiency and work ethic for the lowest-ranked analyst overall. Meanwhile, their collaboration and mentorship, communication skills, and openness to feedback ratings were all negative. This highlights the importance of goals beyond individual performance perceived by SOC leadership. Specifically, a hard-working, technically proficient analyst may not be embracing SOC goals, despite being well-equipped to meet KPI targets.

B. KPI Performance

We begin by collecting KPI metrics for the eleven analysts. The SOC utilizes a suite of software tools to track performance, which we used to compile reports for each analyst. The reports provided the necessary KPIs described in Section III. The analysts were then assigned a rank based on how they performed relative to the other ten analysts. These results can be seen in Table III. Overall performance was calculated by summing the rank for each metric, with a lower total score indicating higher overall ranks.

Table III identifies analyst H as the highest-ranked analyst, with the lowest total score of 16. However, this analyst was not first or second ranked in any single KPI, representing a balanced performance across all metrics. Analysts A and F are tied at second with identical scores of 17, and showing a similar balanced spread of performance across all KPIs. Analyst D is ranked fourth overall, despite ranking first in two KPIs. Analyst D leads the SOC in total tickets closed, as well as total severe tickets handled. Despite this, they rank lower based on relatively high MTTR and time spent on false positive alerts. Severe alerts, characterized by alerts that involve senior leadership, often require a more in-depth investigation given the elevated potential consequences. This highlights an important trade-off: the time required to lead the

Analyst	Work Ethic	Learning	Problem Solving	Technical Proficiency	Knowledge & Curiosity	Collaboration	Communication Skills	Accountability	Openness to Feedback	Total Score
H	2	2	2	1	2	2	2	2	2	**17**
B	2	2	2	1	2	2	1	2	2	**16**
C	2	1	2	1	1	2	2	2	2	**15**
J	1	1	2	1	1	2	1	2	2	**13**
A	1	2	2	1	2	1	0	1	2	**12**
D	2	0	1	0	-2	1	2	2	2	**8**
I	1	1	1	1	2	0	-1	1	1	**7**
K	-1	0	0	-1	0	0	1	0	0	**-1**
F	-1	0	0	-1	0	0	1	0	0	**-1**
E	1	-1	0	-2	0	-1	-1	1	1	**-2**
G	1	0	0	1	0	-1	-1	0	-2	**-2**
Total	**11**	**8**	**12**	**3**	**8**	**8**	**7**	**13**	**12**	

TABLE II

SURVEY RESULTS FROM THE SOC LEADERSHIP. COLUMNS TWO THROUGH TEN SHOW SCORE OF EACH EXPECTATION SCORED FROM -2 TO 2. THE LAST COLUMN REPRESENTS OVERALL SCORE FOR EACH ANALYST. THE LAST ROW SHOWS TOTAL SCORES EACH EXPECTATION CATEGORY

SOC in severe alerts handled may require a higher MTTR, potentially offsetting their overall ranking.

Analyst K, one rank below Analyst D, leads the SOC in MTTR and time spent on false positives, yet ranks lower than average on total tickets handled as well as severe tickets handled. A potential cause of this is that Analyst K specifically chooses less severe, and therefore less time-consuming tickets. This illustrates the opposite trade-off: being selective of which tickets are taken allows for a higher MTTR ranking, while suffering a lower overall ticket count.

C. Goal Congruency Analysis

We now compare the ranking of each analyst between their KPI ratings and their survey ratings. These comparisons can be seen in Table IV. The table shows that when comparing the metrics of performance of an analyst to the survey results provided by the SOC Manager, there is a notable difference in rankings.

Analyst H was the best-performing analyst by both metrics. However, they are the only analyst which remained the same ranking in both metrics. Analyst B has the largest difference between metrics, going from a KPI rank of 10, to a survey rank of 2. Despite handling the fewest tickets overall, and scoring lowest in time to handle tickets overall, Analyst B scored positively in every survey goal rating. Communication skills and technical proficiency are the only two survey-denoted areas of improvement. This highlights that while the analyst meets all of the SOC manager's expectations, their KPI performance represents a struggling analyst. The high ratings in openness to feedback, accountability, knowledge and curiosity, and work ethic all paint the picture of an analyst striving to improve. Analysts J and C repeat this deviation between metrics. Both perform poorly in KPI rankings, yet rank in the top five analysts based on the survey ranking.

Analyst F has the highest negative change from KPI rank to survey rank, falling from second to ninth. Despite similar KPI performance to Analyst A, who has a negative deviation of only 3, Analyst F scored poorly in the survey on work ethic, technical proficiency and is neutral in every other area except for communication skills. This suggests that while Analyst F may be technically proficient (as reflected in the KPIs), their perceived lack of work ethic negatively impacts the SOC overall.

Analyst G has the second largest negative difference, dropping from a KPI rank of 6 to the lowest survey rank of 11. While scoring high on MTTR and time spent on false positives, the survey showed poor scores in openness to feedback, communication skills, and collaboration. This indicates that while Analyst G may be technically capable and dedicated, their lack of collaboration and communication skills significantly hinders their perceived performance.

These findings indicate clear incongruencies between the SOC leadership goals and KPI goals. The variation in these rankings suggests that commonly relied upon KPIs may not be accurately capturing analyst performance. While KPIs appear to accurately capture technical proficiency, they fail to identify analysts' appetite for learning, collaboration, and other SOC-level goals.

SOC analysts who are aware of how KPIs will represent their performance to organizational leadership may be incentivized to abandon SOC goals. While it is true that KPIs measure an analyst's ability to efficiently handle tickets, the overall health of the SOC is reliant upon a larger set of

Analyst	MTTR	Tickets	Severity	FP Time	Total Score
H	5	3	3	5	**16**
A	4	5	4	4	**17**
F	3	4	7	3	**17**
D	8	1	1	8	**18**
K	1	8	9	1	**19**
G	2	9	10	2	**23**
E	6	7	5	6	**24**
C	11	2	2	11	**26**
I	9	6	6	9	**30**
B	7	11	11	7	**36**
J	10	9	8	10	**37**

TABLE III
KPI EVALUATION OF EACH ANALYST. COLUMNS TWO THROUGH FIVE CORRESPOND TO MTTR, TOTAL TICKETS HANDLED, SEVERE TICKETS HANDLED, AND TIME SPENT ON FALSE POSITIVES. THE LAST COLUMN REPRESENTS THE ROW SUM OF INDIVIDUAL KPI RANKS.

Analyst	KPI Rank	Survey Rank	Difference
A	2	5	-3
B	10	2	8
C	8	3	5
D	4	6	-2
E	7	10	-3
F	2	9	-7
G	6	11	-5
H	1	1	0
I	9	7	2
J	11	4	7
K	5	8	-3

TABLE IV
COMPARISON OF SOC ANALYSTS' KPI RANKS AND SURVEY RANKS. THE LAST COLUMN HIGHLIGHTS THE DEVIATION BETWEEN KPI RANKS AND SURVEY-BASED RANKS, REFLECTING ALIGNMENT OR MISALIGNMENT

goals. This is amplified by the high turnover rate of SOC analysts. As SOCs suffer the attrition of experienced analysts, the collective knowledge base diminishes. In such a scenario, curious analysts which are eager to learn, collaborate, and positively respond to feedback are particularly beneficial.

V. CONCLUSION

As complex and damaging cybersecurity threats continue to proliferate, SOCs have emerged as an essential component of organizational cybersecurity. The cybersecurity analysts working within these SOCs are tasked with monitoring traffic, reviewing alerts, and remediating vulnerabilities when necessary. Unfortunately, SOCs are also persistently suffering from high analyst turnover rates and an inability to clearly communicate SOC performance to organizational leadership. To remedy these issues, SOCs have turned to KPIs to identify weak analysts and track performance metrics that can be presented to organizational leadership. While KPIs may accurately measure technical proficiency, such heavy reliance on them introduces a risk of goal incongruence, wherein the organizational goals are undermined by the implicit KPI-related SOC goals.

We perform a case study of an academic SOC to identify and measure any goal incongruency. Using data collected by the SOC, we calculate a set of performance metrics for each analyst based on KPIs. We then conduct semi-structured interviews with SOC leadership to identify what they perceive are the cybersecurity goals of the SOC, as communicated from organizational leadership. We use thematic analysis on the transcripts of these interviews to identify a set of nine SOC-level cybersecurity goals. Each analyst is then ranked by the SOC manager based on how well they are meeting these goals. A comparison is then made between the KPI performance and the survey performance to identify any goal incongruency.

We find that there is a clear lack of goal congruency between the KPI-defined goals and the survey goals. While KPIs accurately measure technical proficiency, they do not accurately capture how well an analyst supports the organizational cybersecurity goals. We find that the worst two performing analysts based on KPIs were rated second and fourth overall based on the SOC manager survey. Similarly, the third-best analyst based on KPIs was ranked third worst for the survey.

These findings highlight the importance of aligning cybersecurity goals across an organization. Although KPI metrics are important, they capture only a portion of what constitutes a productive SOC analyst. What's more, if an analyst is aware that their KPI performance plays a role in their evaluation, it provides further incentive for the analyst to prioritize these metrics over organizational cybersecurity goals. In such a case, as SOC analysts continue to perform in a manner that increases their KPI metrics, the overall health of the SOC may continue to degrade.

The alignment of cybersecurity goals across an organization is paramount. While it is known that KPIs are imperfect measures of analyst performance, this case study reveals how the reliance on them may stymie SOC performance through goal incongruency. As an exploratory case study, this research provides an initial step in understanding how KPI-driven evaluations impact SOC goal alignment. While our findings offer critical insights into analyst evaluation practices, further research is needed to assess these dynamics in professional SOCs. Future work includes investigating how KPIs are perceived by analysts, which metrics align with organizational goals, and how cybersecurity goals are communicated down the organizational hierarchy.

REFERENCES

[1] S. Chandran, A. G. Bardas, and J. Case, "A Human Capital Model for Mitigating Security Analyst Burnout," Jul. 2015.

[2] M. Vielberth, F. Bohm, I. Fichtinger, and G. Pernul, "Security Operations Center: A Systematic Study and Open Challenges," *IEEE Access*, vol. 8, pp. 227 756–227 779, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9296846/

[3] E. Agyepong, Y. Cherdantseva, P. Reinecke, and P. Burnap, "Challenges and performance metrics for security operations center analysts: a systematic review," *Journal of Cyber Security Technology*, vol. 4, no. 3, pp. 125–152, Jul. 2020. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/23742917.2019.1698178

[4] F. B. Kokulu, A. Soneji, T. Bao, Y. Shoshitaishvili, Z. Zhao, A. Doupé, and G.-J. Ahn, "Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '19. New York, NY, USA: Association for Computing Machinery, Nov. 2019, pp. 1955–1970. [Online]. Available: https://dl.acm.org/doi/10.1145/3319535.3354239

[5] E. Agyepong, Y. Cherdantseva, P. Reinecke, and P. Burnap, "A systematic method for measuring the performance of a cyber security operations centre analyst," *Computers & Security*, vol. 124, p. 102959, Jan. 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404822003510

[6] J. Forsberg and T. Frantti, "Technical performance metrics of a security operations center," *Computers & Security*, vol. 135, p. 103529, Dec. 2023. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S016740482300439X

[7] C. Teddlie and A. Tashakkori, "Mixed methods research," *The Sage handbook of qualitative research*, vol. 4, no. 1, pp. 285–300, 2011.

[8] R. K. Yin, "How to do better case studies," *The SAGE handbook of applied social research methods*, vol. 2, no. 254-282, 2009.

[9] G. D. Bhatt, "Knowledge management in organizations: examining the interaction between technologies, techniques, and people," *Journal of Knowledge Management*, vol. 5, no. 1, pp. 68–75, Jan. 2001, publisher: MCB UP Ltd. [Online]. Available: https://doi.org/10.1108/13673270110384419

[10] W. Hofkirchner and M. Schafranek, "General System Theory," in *Philosophy of Complex Systems*, ser. Handbook of the Philosophy of Science, C. Hooker, Ed. Amsterdam: North-Holland, Jan. 2011, vol. 10, pp. 177–194. [Online]. Available: www.sciencedirect.com/science/article/pii/B9780444520760500067

[11] I. Kronberg and M. S. Gustafsson, "Goal Congruence - The Experience of a Performance Management System - A Case Study of AstraZeneca," 2012. [Online]. Available: https://api.semanticscholar.org/CorpusID:56132342

[12] B. Rich, J. Lepine, and E. Crawford, "Job Engagement: Antecedents and Effects on Job Performance," *Academy of Management Journal*, vol. 53, pp. 617–635, Jun. 2010.

[13] D. I. Jung and B. J. Avolio, "Opening the black box: an experimental investigation of the mediating effects of trust and value congruence on transformational and transactional leadership," *Journal of Organizational Behavior*, vol. 21, no. 8, pp. 949–964, 2000.

[14] J. B. Vancouver and N. W. Schmitt, "An Exploratory Examination of Person-Organization Fit: Organizational Goal Congruence," *Personnel Psychology*, vol. 44, no. 2, pp. 333–352, 1991. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1744-6570.1991.tb00962.x

[15] S. Beckman, A. Jian, A. Sabharwal, and K. Goucher-Lambert, "Examining Goal Congruence on Engineering Design and Innovation Student Teams," in *Volume 4: 18th International Conference on Design Education (DEC)*. Virtual, Online: American Society of Mechanical Engineers, Aug. 2021, p. V004T04A005. [Online]. Available: https://asmedigitalcollection.asme.org/IDETC-CIE/proceedings/IDETC-CIE2021/85406/V004T04A005/1128089

[16] R. Yasin, G. Jan, A. Huseynova, and M. Atif, "Inclusive leadership and turnover intention: the role of follower–leader goal congruence and organizational commitment," *Management Decision*, vol. 61, no. 3, pp. 589–609, Mar. 2023. [Online]. Available: https://www.emerald.com/insight/content/doi/10.1108/MD-07-2021-0925/full/html

[17] V. Madhavan, M. Venugopalan, B. Gupta, and G. S. Sisodia, "Addressing Agency Problem in Employee Training: The Role of Goal Congruence," *Sustainability*, vol. 15, no. 4, p. 3745, Jan. 2023, number: 4 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/2071-1050/15/4/3745

[18] V. Madhavan and M. Venugopalan, "Formal learning and organizational performance: the interplay of goal setting and flexible learning practices in attaining goal congruence," *Benchmarking: An International Journal*, vol. 31, no. 3, pp. 955–989, Jan. 2023, publisher: Emerald Publishing Limited. [Online]. Available: https://doi.org/10.1108/BIJ-10-2021-0623

[19] A. Diallo, "Factors Affecting the Sustainability of Public-Private Collaborations at the Municipal Level: The Case of Motorcycle Rallies," 2015. [Online]. Available: https://www.semanticscholar.org/paper/Factors-Affecting-the-Sustainability-of-at-the-The-Diallo/5984d12b89e443dafe5fb820202d2998ebbac3e3

[20] U. Menges and A. Kluge, "Contrasting and Synergizing CISOs' and Employees' Attitudes, Needs, and Resources for Security Using Personas," in *2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Jul. 2024, pp. 456–472, iSSN: 2768-0657. [Online]. Available: https://ieeexplore.ieee.org/document/10628768

[21] B. Schaffer, "The nature of goal congruence in organizations," *supervision*, vol. 68, p. 13, 2007.

[22] W. M. Lim, "What is qualitative research? an overview and guidelines," p. 14413582241264619, 2024, publisher: SAGE Publications Ltd. [Online]. Available: https://doi.org/10.1177/14413582241264619

[23] J. K. Lê and T. Schmid, "The practice of innovating research methods," vol. 25, no. 2, pp. 308–336, 2022, publisher: SAGE Publications Inc. [Online]. Available: https://doi.org/10.1177/1094428120935498

[24] D. W. Turner, "Qualitative interview design: A practical guide for novice investigators," *The Qualitative Report*, vol. 15, no. 3, pp. 754–760, 2010, num Pages: 7 Place: Fort Lauderdale, United States Publisher: The Qualitative Report. [Online]. Available: https://doi.org/10.46743/2160-3715/2010.1178

[25] E. Agyepong, Y. Cherdantseva, P. Reinecke, and P. Burnap, "Towards a Framework for Measuring the Performance of a Security Operations Center Analyst," in *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. Dublin, Ireland: IEEE, Jun. 2020, pp. 1–8. [Online]. Available: https://ieeexplore.ieee.org/document/9138872/

[26] S. Hathaway, "Going beyond traditional metrics: 3 key strategies to measuring your SOC performance," May 2021. [Online]. Available: https://blog.nviso.eu/2021/05/26/going-beyond-traditional-metrics-3-key-strategies-to-measuring-your-soc-performance/

[27] S. A. Chamkar, Y. Maleh, and N. Gherabi, "SOC Analyst Performance Metrics: Towards an optimal performance model," *EDPACS*, vol. 68, no. 3, pp. 16–29, Sep. 2023. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/07366981.2023.2259046

[28] G. Guest, K. M.MacQueen, and E. E.Namey, *Applied Thematic Analysis*. SAGE Publications, Inc., 2012. [Online]. Available: https://methods.sagepub.com/book/mono/applied-thematic-analysis/toc