MJoSHT
Malaysian Journal of Science, Health & Technology
[mjosht.usim.edu.my]

USIM

Article

Human Dimensions of Cybersecurity Operations: Survey Insights from SOC Professionals in Malaysia

Mohd Haffezal Md Yahaya[1] and Najwa Hayaati Mohd Alwi[1,2]

[1]*Faculty of Science and Technology, Universiti Sains Islam Malaysia, Nilai 71800, Negeri Sembilan, Malaysia.*

[2]*CyberSecurity and Systems Research Unit, Faculty of Science and Technology, Universiti Sains Islam Malaysia, Nilai 71800, Negeri Sembilan, Malaysia.*

Correspondence should be addressed to:
Najwa Hayaati Mohd Alwi; najwa@usim.edu.my

Article Info
Article history:
Received:15 July 2025
Accepted: 5 February 2026
Published:15 Mac 2026

Academic Editor:
Nurzi Juana Mohd Zaizi

Malaysian Journal of Science, Health & Technology

MJoSHT2025, Volume 11, Special Issue on the 5th International Conference on Recent Advancements in Science and Technology (ICoRAST 2025): Responsible Artificial Intelligence – Advancing Science and Technology for Humanity
eISSN: 2601-0003

https://doi.org/10.33102/dznmde05

***Abstract*— Security Operations Centres (SOCs) form the operational core of cyber defence strategies across the world. They are tasked with ensuring continuous monitoring, triage, detection, and response to ever-evolving threats. However, conventional performance metrics used to evaluate SOC efficacy—such as Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), and false positive rates—primarily assess system throughput while overlooking the psychosocial realities of the human analysts who underpin these metrics. This paper presents the findings of a quantitative workforce study conducted among 175 Malaysian SOC professionals across internal, hybrid, and managed security service provider (MSSP) environments. Using a Likert-based adaptation of the NIOSH Worker Well-Being Questionnaire (WellBQ), the study investigates stress, burnout, alert fatigue, task autonomy, psychological safety, tooling efficacy, and career development perceptions. Findings reveal that 73.1% of respondents experience emotional tiredness at least "Sometimes," while 78.9% agree that more automation would improve their well-being. Notably, 68.0% reported having opportunities to grow and develop their careers within their SOC environments. These insights highlight the need for a paradigm shift in SOC performance measurement—one that integrates human-centric indicators alongside traditional technical KPIs. The paper concludes with empirically grounded recommendations for embedding well-being frameworks into operational security management to ensure sustainable, high-performing cybersecurity teams.**

***Keywords*— Security Operations Center (SOC); Human-Centric, Cybersecurity; Mean Time to Detect (MTTD); Mean Time to Respond (MTTR).**

I. INTRODUCTION

Security Operations Centres (SOCs) are essential components of an organization's cybersecurity infrastructure. As the threat landscape grows more complex, SOCs are increasingly relied upon to manage high volumes of alerts, coordinate incident responses, and provide real-time visibility into enterprise threats. Traditionally, SOC performance has been measured through operational metrics such as Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), and false positive rates. While these indicators are valuable for assessing system responsiveness and procedural effectiveness, they fail to capture the human dimension of cybersecurity work.

SOC analysts operate in cognitively demanding environments characterized by high alert volumes, irregular schedules, and intense decision-making pressures. These working conditions can lead to emotional exhaustion, decreased vigilance, and burnout, particularly when there is limited autonomy or unclear career growth. Despite these challenges, human-centric metrics are rarely incorporated into SOC assessments, creating a critical blind spot in performance management.

In Malaysia, where cybersecurity capabilities are maturing rapidly under the national Malaysia Cyber Security Strategy [1], understanding the psychosocial experiences of SOC analysts is crucial for both workforce retention and strategic resilience. Further, according to the Delinea Global Cybersecurity Workforce Report [2], a significant proportion of security leaders report recurring negative business impacts due to poor alignment with business stakeholders. The report emphasizes that only 47% of decision-makers feel cybersecurity goals are highly aligned with business outcomes, and gaps in goal setting and communication undermine both security posture and analyst well-being. This study seeks to fill this gap by exploring the well-being of Malaysian SOC professionals using a structured, evidence-based approach. It builds upon validated occupational health instruments to provide a first-of-its-kind empirical assessment of analyst experience in high-pressure security environments.

II. LITERATURE REVIEW

A. Traditional Metrics and Their Shortcomings

Security Operations Centre (SOC) performance is commonly assessed using indicators like Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), and alert closure rates. Figure 1 gives an overview of Incident Metrics. While effective at measuring response efficiency, these metrics overlook key human performance dimensions such as decision complexity, mental fatigue, and tool usability. Vielberth et al. [3] argue that traditional metrics fail to reflect the full scope of operational effectiveness and do not account for human-centric challenges. Chamkar et al. [4] further emphasize that SOC evaluations should integrate analyst well-being, autonomy, and engagement alongside technical performance.

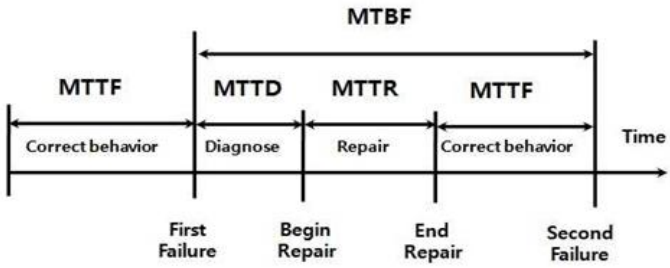

Figure 1 Overview of Incident Metrics

B. Burnout and Fatigue in Cybersecurity Work

Burnout in SOC roles is a recurring issue, primarily caused by repetitive alert triage, high-stakes incident response, and continuous shifts. Chandran et al. [5] demonstrated how emotional fatigue accumulates in SOC teams through alert volume, tool fatigue, and constrained task autonomy. Their human capital model highlights the feedback loop between stress and attrition, showing that burnout undermines both operational continuity and workforce retention.

C. Psychological Safety and Organizational Health

Psychological safety, the shared belief that individuals can voice concerns, admit mistakes, or express emotional strain without fear of retribution is foundational to effective team performance in high-pressure environments such as Security Operations Centres (SOCs). It enables proactive error reporting, fosters collaborative problem-solving, and strengthens emotional resilience. However, in many SOC environments, low psychological safety leads to suppressed communication and heightened stress, especially during critical incident response. Newman et al. [6] affirm that psychological safety is strongly linked to learning behaviour, engagement, and team effectiveness, yet it is frequently overlooked in technical and maturity frameworks that prioritize operational metrics over human-centered factors.

Despite its well-documented benefits, psychological safety remains underemphasized in the design and evaluation of SOCs. This study found that only 37% of survey respondents felt safe discussing burnout or emotional fatigue in the workplace. The absence of psychological safety not only impedes team learning and early error detection but also contributes to chronic stress and emotional disengagement, undermining the very performance these environments are built to support.

D. The Career Stagnation Challenge

The 2025 SANS SOC Survey [7] confirms that career progression has become the leading factor for employee retention, surpassing money and meaningful work, as illustrated in the latest findings (see Figure 2). This update highlights that while SOC analysts continue to cite a lack of clear advancement pathways and role clarity as key challenges, even modest improvements in progression opportunities have a decisive impact on whether skilled staff choose to stay. Without visible career ladders and active mentorship, organizations risk heightened turnover as analysts look for growth in roles beyond the SOC.

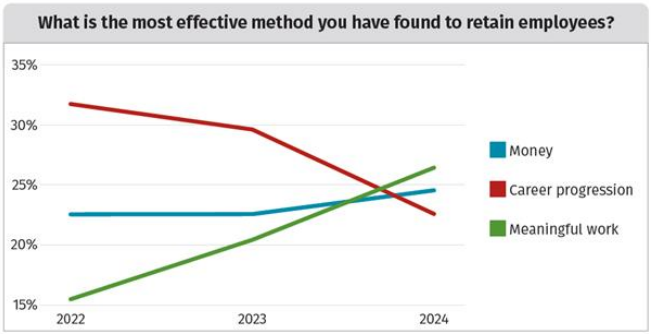

Figure 2. The 2024 SANS SOC Survey on what has been compelling people to stay

E. Human-Centric SOC Frameworks

Mainstream technical frameworks such as MITRE ATT&CK [8] and NIST CSF [9] focus on procedural and control maturity, but do not address analyst fatigue, psychological safety, or career incentives. Vielberth et al. [3] pointing out that there is no holistic SOC standard or framework, making it hard to audit a cohesive and complex SOC. Chamkar et al. [4] emphasises the need to design a universal set of metrics, that consider all the factors in SOCs which aligned with this study highlighting human-centric metrics as critical factor of SOCs. Kokulu et al. [10] conducted a qualitative study, interviewing SOC analysts and managers across sectors to identify issues limiting SOC performance. Their findings show "low visibility into the network infrastructure" as the most frequently cited problem, as well as mismatches between manager and analyst priorities, especially regarding automation, response speed, and metric effectiveness. The study emphasizes the need for research into communication, asset discovery, and refinement of security metrics, supporting calls within the industry for a shift toward human-centric and context-aware SOC frameworks.

III. Methodology

A. Survey Design and Adaptation

This study employed a structured questionnaire based on the NIOSH Worker Well-Being Questionnaire [11]. Figure 3 displays NIOSH WellBQ domains that were used as a reference.

Figure 3. NIOSH WellBQ domains

The adapted NIOSH Worker Well-Being Questionnaire (WellBQ) used in the survey differs from the original instrument primarily in its contextualization and focus on Security Operations Center (SOC)-specific experiences across eight key domains: Burnout Risk, Cognitive Load & Alert Fatigue, Job Satisfaction & Meanings, Career Development, Organizational Support, Technology Impacts, Workplace & Safety, and Poor Mental Health. While the NIOSH WellBQ is a comprehensive, multi-domain tool designed to assess worker well-being across generic occupational sectors—with domains such as work evaluation, workplace culture, safety climate, health status, and life outside work—the adapted version reorganizes and customizes these content areas specifically to reflect SOC operational realities.

The survey instrument adapted 19 items from the NIOSH WellBQ while introducing 3 new constructs that do not present in the original instrument. The SOC instruments contain 9 sections (A - I) where sections A and B capture demographic and SOCs organizational profile contexts, including role specialization (SOC Analyst, Threat Hunter, DFIR), shift patterns, and alert volume characteristics.

Sections C-I systematically adapt NIOSH WellBQ items measuring burnout risk, cognitive load, job satisfaction, mental health, organizational support, and workplace environment. 3 new constructs which is development (E7-E9), technology impacts (H1-H2), and enhanced psychological safety measures (G6, G8). The new constructs that have been created still maintaining the integrity of the original NIOSH while tailored to capture SOC specific stressors such as alert fatigue, 24/7 operational demands, and cognitive loads from the threat analysis works. The survey responses will enable operationalization of the new proposed eight SOC well-being metrics:

i. Burnout Risk
ii. Cognitive Load & Alert Fatigue
iii. Job Satisfaction & Meanings
iv. Career Development
v. Organizational Support
vi. Technology Impacts
vii. Workplace & Safety
viii. Poor Mental Health

B. Sample Population

As there are no official registry or publicly available data regarding the total population of SOC professionals in Malaysia, the precise size of the population remains indeterminate. Consequently, the study relied on a purposive sample of practitioners who voluntarily participated in the survey. In total, 175 SOC professionals across Malaysia completed the instrument. Table I presents the demographic characteristics of the respondents, while Figure 4 illustrates the distribution of participants' roles. The sample encompassed both operational and managerial positions and reflected a diversity of professional experience, organizational contexts, and industry sectors. While the absence of a defined population precludes claims of full representativeness, the heterogeneity of respondents offers meaningful insights, though findings should be interpreted with caution given the voluntary nature of participation and potential self-selection bias.

TABLE I. SURVEY POPULATION

Category	Subcategory	Percentage
Role	SOC Analyst	51.4%
	CTI Analyst	8.6%
	DFIR	7.4%
	Red Team	6.9%
	SOC Engineer	6.3%
	Threat Hunter	2.3%
	Others	17.1%
Experience	Less than 1 year	22.3%
	1–3 years	37.1%
	3–5 years	13.7%
	More than 5 years	26.9%
Soc Model	Internal	41.1%
	MSSP	38.9%
	Hybrid	20.0%
Shift Type	Rotating	57.7%
	Day	24.6%
	Night	1.7%
	Flexible	16.0%

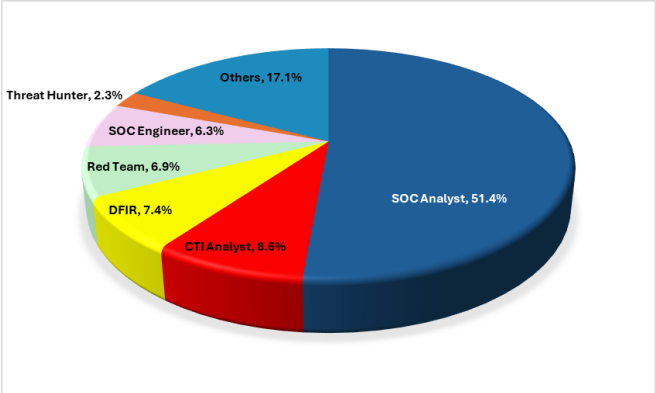

Figure 4. Survey participant roles

C. Data Analysis

Likert responses were analysed using percentage distributions. This approach was chosen to highlight the frequency and recurrence of specific experiences, enabling identification of high-risk areas such as persistent emotional fatigue, tooling dissatisfaction, or lack of role clarity.

D. Data Collection Timeline

The survey administration period lasted six weeks from June to July 2025 which allowed enough time for participants recruitment, allowing participants to complete their survey, and enough time to collect the responses. The research employed different recruitment approaches which included professional network announcements and organizational outreach to increase participant numbers while ensuring all participants joined voluntarily.

IV. RESULT

This section presents the statistic distributions of SOC workforce experiences across key psychosocial dimensions, derived from Likert-scale responses. Table II displays statistics over eight well-being metrics.

TABLE II. WELL-BEING METRICS RESULTS (N=175)

Metric	Mean	SD	Med	Range	Cronbach's α
Burnout Risk	52.8	13.7	52.0	20-100	0.74
Cognitive Load & Alert Fatigue	53.7	15.2	53.3	20-100	0.74
Job Satisfaction & Meanings	75.7	14.7	76.7	20-100	0.89
Career Developments	73.1	18.1	73.3	20-100	0.80
Organizational Supports	73.8	15.0	75.6	31.1–100	0.90
Technology Impacts	76.5	16.8	80.0	20-100	0.77
Workplace & Safety	78.1	16.4	80.0	20-100	0.65
Poor Mental Health	47.8	16.8	45.6	20–92.0	0.87

E. Burnout Risk

The study reveals that the average Burnout Risk score among the participants was 52.8 on a 0-100 scale, with a standard deviation of 13.7. This result was derived from five key indicators which is time pressure, fatigue, life interference, anxiety, and anger. This indicator suggests a moderate level of burnout risk within the group. Cronbach's alpha has been measured and captures a score of 0.74 for the internal consistency of the scale which indicating a reliable data.

F. Cognitive Load & Alert Fatigue

The Cognitive Load & Alert Fatigue assessed on areas such as lack of enthusiasm, lack of energy, and difficulty concentrating. The mean score for this metrics is 53.7 (SD = 15.2) with the Cronbach's alpha result of 0.74. Studies literature indicates that alert fatigue represents one of the significant work-related stressors affecting SOC analysts [4]. The wide distribution (20-100) shows that people experience fatigue at different levels which indicates that some analysts stay alert while others face extreme fatigue that could affect their ability to detect things and make decisions. This variation is fully acceptable considering the wide size of survey sample size received from different organizational contexts of SOC in Malaysian landscape.

G. Job Satisfaction & Meanings

Job Satisfaction & Meanings measured using six items from the survey which assessing the participant satisfaction, meaningfulness, purpose, inspiration, immersion, and enthusiasm for work. The metric was calculated with a mean score of 75.7 (SD = 14.7) and the Cronbach's alpha score of 0.89 which indicating an excellent internal consistency.

The high mean score indicates that the majority of Malaysian SOC professionals experience substantial job satisfaction and perceive their work as meaningful. This finding provides important context for interpreting against the moderate burnout risk scores in which analysts experience genuine engagement and purpose in security work despite occupational pressures. This distinction between meaningful work with moderate demands (present) and burnout resulting from meaningless work with excessive demands (not present) has important implications for organizational strategy. Rather than reducing workload dramatically, organizations may enhance well-being through recognition of meaningful contributions and clarification of purpose.

H. Career Developments

The Career Developments metric has been measured by using three items which assessing the growth opportunities, organizational support for development, and feedback quality, yielded a mean of 73.1 (SD = 18.1) with Cronbach's alpha of 0.80, indicating good internal consistency. Notably, Career Developments exhibited the highest standard deviation (18.1) among all metrics, indicating dramatic organizational differences in career support practices.

The finding shows moderate-to-high mean score which suggested that on average organizations are providing reasonable career development support. Based on the wide variation result, it is showing that some of the participants believed that their career progression is clear and being provided by the organization where others might struggle with career potential and opportunities. Through this metric, organizations can positively influence the Career Developments scores by coming up with strategic investments which can be focused on career development planning, skill development, and career advancement opportunities.

I. Organizational Supports

The Organizational Supports metric has been measured by using nine items assessing the feeling respected, feeling valued, recognition, trust, well-being prioritization, psychological safety, peer support, fair workload, and autonomy. The score calculated with a mean of 73.8 (SD = 15.0) with Cronbach's alpha score of 0.90 which indicating an excellent internal consistency. This nine-item metric demonstrates the strongest internal consistency among all measures, reflecting the coherence of items measuring organizational support dimensions.

Similar like career development analysis where the high mean score indicates that most respondents perceive substantial organizational support across multiple dimensions. However, the meaningful standard deviation (15.0) indicates variation in support experience across organizations.

Kokulu et al. [10] work interpreted that SOCs exhibit 'matched' issues (where analysts and managers largely agree) and 'mismatched' issues (where they significantly disagree). The areas of disagreement between manager and analysts are related to the speed of response, automation levels, evaluation metrics, and tool functionality. These were suggested that alignment between manager and analyst perspectives are important for SOC effectiveness.

J. Technology Impacts

The Technology Impacts metric has been measured by using two items assessing perceived workload reduction from tools and optimized alert triage, yielded a mean of 76.5 (SD = 16.8) with Cronbach's alpha of 0.77, indicating acceptable-to-good internal consistency.

The high mean score indicates that most organizations have successfully implemented technologies that analysts perceive as helpful for workload management and triage optimization. However, the wide range (20-100, SD = 16.8) demonstrates that a minority of organizations face significant tool-related challenges. Through this metric, organization with a low Technology Impacts scores should conduct comprehensive tool audits which further examining their usability, integration quality, automation coverage, and user training adequacy.

K. Workplace Safety

The Workplace Safety metric has been measured by using two items assessing both ergonomic workspace quality and physical safety at work. The score was calculated with a mean of 78.1 (SD = 16.4) with Cronbach's alpha score of 0.65 which indicating an acceptable internal consistency for exploratory research. Despite the modest internal consistency coefficient, the metric demonstrates construct validity through meaningful variation across 175 respondents (range: 20-100). The two items (ergonomic workspace and physical safety) assess distinct, but related safety dimensions reflect legitimate differences in how analysts experience workplace hazards.

The high mean score indicates that most respondents perceive adequate physical and ergonomic working conditions. The result data shows likely that SOC operations currently established in facilities which maintain basic safety standards for workplace environments.

L. Poor Mental Health

The participants responded to poor mental health items which produced an average score of 47.8 equivalent (SD = 16.8, Median = 45.6, Range = 20–92). The high standard deviation among 175 SOC respondents indicates substantial variability due to different analysts found either minimal mental health problems or major significant distress. The observed pattern shows that SOC workers from a particular group experience extended mental health issues which require dedicated mental health treatment programs. Using the same well-being measurement constructs, human resource team or equivalence can come up with risk mitigation planning such as consultation, mental health support, team building and other mental wellness strategy.

V. COMPARATIVE ANALYSIS ACROSS SOC CONTEXTS

This section provides deeper dive for subgroup analysis between Internal SOC vs MSSP (N=140) by utilising the 8 metrics and the survey demographic contexts. Table III presents the well-being metrics comparison between Internal SOC and MSSP respondents.

TABLE III. COMPARISON: INTERNAL SOC VS. MSSP (N=140)

Metric	Internal (n=72)	MSSP (n=68)
	Mean	Mean
Burnout Risk	54.7	54.2
Cognitive Load & Alert Fatigue	54.8	56.8
Job Satisfaction & Meanings	74.9	72.8
Career Developments	74.1	70.4
Organizational Supports	76.3	69.2
Technology Impacts	77.0	72.6
Workplace & Safety	77.4	75.0
Poor Mental Health	47.2	53.0

Analysis of well-being metrics across operational models reveals patterns reflecting organizational and structural differences between internal and MSSP contexts. While both contexts show comparable burnout risk (Internal: M = 54.7; MSSP: M = 54.2), other dimensions show meaningful differences.

Organizational Support demonstrates the most substantial difference, with internal SOC professionals reporting significantly higher support perception (M = 76.3) compared to MSSP personnel (M = 69.2). This moderate effect size suggests that internal organizational structures provide stronger perceived backing than MSSP service delivery models.

Career Development shows a significant advantage for internal SOC professionals (M = 74.1 vs. M = 70.4). This can be interpreted with a theory suggesting that internal advancement opportunities are more transparent in dedicated operations than in client-service delivery models.

Notably, Poor Mental Health reveals that MSSP personnel reporting significantly higher mental health status (M = 53.0) compared to internal SOC professionals (M = 47.2).

Job Satisfaction & Meaning of Internal SOC is showing higher satisfaction rate (M = 74.9 vs. M = 72.8).

Differences in Burnout Risk and Cognitive Load which the two most operationally proximal stressors are not statistically significant. This indication provide assumption that the fundamental demands of 24/7 monitoring and alert management are similar across organizational models. The truly differences emerge in how organizational context shapes response to and recovery from these demands. Figure 5 illustrates well-being metrics comparison between Internal SOC and MSSP in a radar charts view.

In addition to Internal SOC vs MSSP comparison, other descriptive analyses reveal notable trends. The study shows that analysts who have worked for less than twelve months are having lower Cognitive Load & Alert Fatigue scores which at M=53.8 compared to analysts who worked for five or more years with score of M=60.0. This indicating that senior employees experience higher mental workload and more responsibilities in their day-to-day work.

The SOC Managers showed higher Job Satisfaction levels than analysts indicating that leadership positions confer a heightened feeling of purpose (M = 80.0 vs M = 73.4).

The finance industry had diminished Organizational

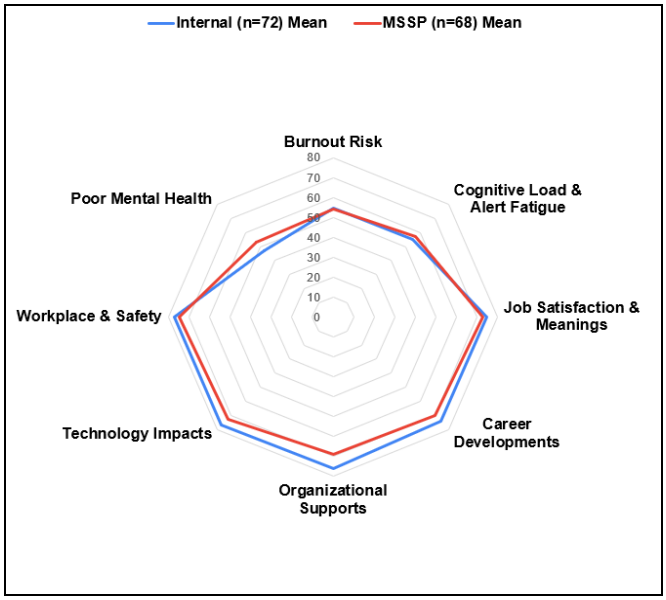

Figure 5. Internal SOC vs MSSP

Supports (M = 68.3) in contrast to energy sector (M = 84.2), possibly indicative of regulatory compliance cultures.

VI. SIMILAR INTERNATIONAL STUDY

A comparative analysis was conducted between this study against the global SANS 2025 SOC Survey [7], each offering distinct insights into the organizational and human dimensions of security operations.

The two surveys have different core objectives: The SANS SOC Survey 2025 [7] aims to benchmark SOC operational maturity, staffing, and technology adoption globally, providing industry-wide insights into tools, processes, and structural challenges in SOCs. By contrast, this study focuses specifically on the human-centric experience of analysts, using adapted occupational health measures to assess stress, burnout, psychological safety, and career progression in a national context.

While SANS prioritizes technical, organizational, and maturity metrics to guide industry best practices, the Malaysian study spotlights psychosocial well-being and analyst sustainability—emphasizing a need to rethink SOC effectiveness beyond technical KPIs. This difference means SANS offers global operational comparisons, while the Malaysian survey provides unique, actionable insights for workforce resilience and human-centered improvement strategies.

The Malaysian SOC workforce experiences high rates of emotional fatigue and stress, closely mirroring global findings from the SANS 2025 SOC Survey [7], where understaffing, retention challenges, and alert fatigue are universal issues. Both surveys highlight that analysts see automation as crucial to reducing repetitive work and improving wellbeing, yet current tools and processes—manual reporting, tool sprawl—fall short of those expectations.

Distinctly, the Malaysian study places a unique emphasis on psychosocial factors like psychological safety and career development, with only 42% feeling safe discussing burnout and 68% perceiving career growth opportunities. In contrast, the SANS global survey adopts a broader view, focusing more on operational metrics and technical deficits, while noting only slowly improving leadership support and unclear career progression. This shows Malaysian SOCs are more attuned to human-centric challenges, whereas global trends emphasize foundational capability and slow organizational change.

VII. RECOMMENDATIONS

To address the critical findings of this study, several human-centric interventions are recommended.

A. Well-being metrics integration

Organizations should integrate well-being metrics into SOC performance dashboards. These may include burnout frequency, alert fatigue ratio, career clarity index, and psychological safety scores to supplement traditional KPIs. Table IV shows the Conceptual Workforce Well-Being Metrics. Each suggested metric proposed to be normalized to a percentage or index scale, allowing comparative evaluation across organizations or analyst profiles.

Figure 6 presents a radar chart illustrating the mean scores for each of the workforce well-being metrics suggested in this study. Higher scores indicate stronger positive perceptions (e.g., better psychological safety or more meaningful work), while lower scores may highlight areas needing attention. The visual profile reveals relative strengths in dimensions such as "Technology Impacts" and "Workplace & Safety", while metrics like "Career Developments" and "Organizational Supports" appear comparatively lower, indicating interventions are required for better supports and clear development plan in SOC environments.

Figure 7 illustrates a conceptual role-based differences in perceived workforce well-being using radar chart for Analysts, and Managers. Both roles show relatively consistent scores in core constructs like Burnout Risk, certain distinctions emerge. For example, Managers report higher Career Developments Confidence and higher Job Satisfaction & Meanings compared to Analysts. Additionally, Analysts tend to report higher Mental Health concern and lower scores on Organizational Supports, possibly reflecting their operational workload and lack of support from team members and manager. This segmentation enables more tailored interventions for each role based on well-being profile differences.

TABLE IV. CONCEPTUAL WORKFORCE WELL-BEING METRICS

Metric	Description
Burnout Risk Score	Measures stress frequency, exhaustion, and poor mental health
Cognitive Load & Alert Fatigue	Measures mental effort demand, decision fatigue, alert volume pressure, and sustained attention requirements during monitoring tasks
Job Satisfaction & Meanings	Measures intrinsic motivation, sense of purpose, emotional connection to work, and professional identity satisfaction
Career Development	Measures perception of growth opportunities, advancement pathways, organizational support for professional development
Organizational Supports	Captures recognition, trust in management, perceived fairness, peer support, psychological safety for discussing burnout, and decision-making autonomy
Technology Impacts	Measures whether tooling helps reduce workload, mental burden, and improves efficiency (automation relief perception)
Workplace & Safety	Assesses alert triage volume, workspace ergonomics, physical safety, work-life balance perception
Poor Mental Health	Direct measure of recent days experiencing poor mental or emotional health (0-30 days count) combined with symptom frequency (depression, anxiety, worry)

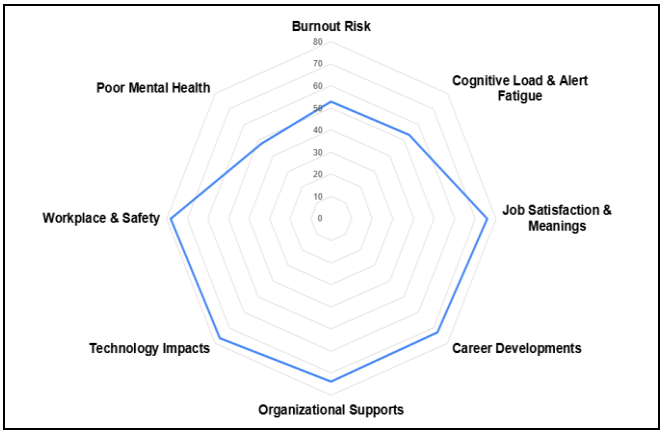

Figure 6. Conceptual workforce well-being spider radar

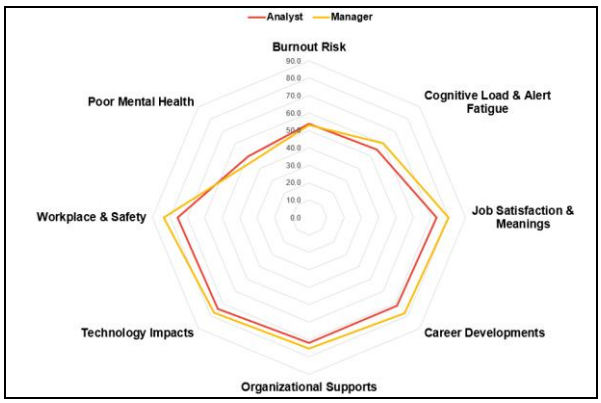

Figure 7 Conceptual workforce well-being radar by roles

B. *Strategically automation efforts*

Automation efforts must be strategically designed to reduce noise, not just improve speed. Implementations should include analyst-informed playbooks, feedback-based alert suppression tuning, and security orchestration, automation and response (SOAR) tools with override capabilities for contextual decision-making.

C. *Psychological safety*

Psychological safety must be fostered intentionally. Techniques include team debriefs following major incidents, regular wellness check-ins, and anonymous reporting mechanisms that encourage transparency without fear of retaliation.

D. *Career path clarity*

Organizations must clarify career development pathways. This may involve introducing tiered analyst levels (e.g., Tier 1 to Tier 3) as shown in Figure 8, offering internal mobility into roles like DFIR or CTI, and sponsoring certification tracks or mentorship schemes.

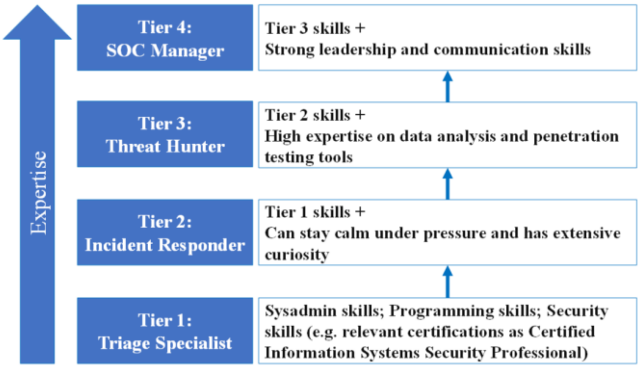

Figure 8. SOC tiers by Vielberth et al. [3]

E. *Physical working conditions and shift ergonomics*

Physical working conditions and shift ergonomics should be optimized. This includes quarterly ergonomic reviews, access to mental wellness support, and budgets for workspace enhancements to reduce fatigue from environmental factors.

VIII. CONCLUSION

This study has gone through from literature review where the current metrics deficiencies has been identified, to empirical demonstration by using 175 Malaysian SOC practitioners' well-being data via the survey which adapted the NIOSH WellBQ instruments, the eight well-being metrics Burnout Risk, Cognitive Load & Alert Fatigue, Job Satisfaction & Meanings, Career Developments, Organizational Supports, Technology Impacts, Workplace & Safety, and Poor Mental Health addressed human factors that has been systematically neglected in traditional technical performance frameworks. The research theoretically expands occupational well-being theory to cybersecurity operations dimension.

The metrics facilitates evidence-based management of workforce well-being that are capable to assists SOC leaders and HR professionals with actionable decision-making data.

The findings reveal widespread emotional fatigue, inconsistent perceptions of psychological safety, and a strong analyst demand for smarter tooling and clearer career progression. These insights point to the need for SOCs to evolve beyond traditional performance metrics and integrate human-centric indicators into operational management.

Doing so is critical not only for team resilience but also for the long-term sustainability and effectiveness of national cybersecurity capabilities.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of this paper.

ACKNOWLEDGEMENT

The authors extend their sincere gratitude to the respondents from the Security Operations Center (SOC) teams of all participating companies. Their invaluable contribution of proprietary data was fundamental to the successful completion of this research, providing the critical insights necessary for this journal paper.

REFERENCES

[1] National Cyber Security Agency (NACSA), "Malaysia Cyber Security Strategy 2020-2024," National Security Council, Prime Minister's Department, Putrajaya, Malaysia, Oct. 2020. [Online]. Available: https://asset.mkn.gov.my/web/wp-content/uploads/sites/3/2019/08/MalaysiaCyberSecurityStrategy2020-2024Compressed.pdf

[2] J. Carson, "Mismatched metrics reflect lack of cybersecurity and business alignment," *Delinea*, May 09, 2023. https://delinea.com/blog/aligning-cybersecurity-and-business-goals

[3] M. Vielberth, F. Bohm, I. Fichtinger, and G. Pernul, "Security Operations Center: A systematic study and open challenges," *IEEE*

Access, vol. 8, pp. 227756–227779, Jan. 2020, doi: 10.1109/access.2020.3045514.

[4] 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, doi: 10.1080/07366981.2023.2259046.

[5] S. Chandran et al., "A human capital model for mitigating security analyst burnout," 2015. [Online]. Available: https://www.usenix.org/system/files/conference/soups2015/soups15-paper-sundaramurthy.pdf

[6] A. Newman, R. Donohue, and N. Eva, "Psychological safety: A systematic review of the literature," Human Resource Management Review, vol. 27, no. 3, pp. 521–535, Jan. 2017, doi: 10.1016/j.hrmr.2017.01.001.

[7] "SANS 2025 SOC Survey," SANS Institute. https://www.sans.org/white-papers/sans-2025-soc-survey

[8] The MITRE Corporation. (2015). MITRE ATT&CK framework. https://attack.mitre.org

[9] N. I. of S. A. Technology, "The NIST Cybersecurity Framework (CSF) 2.0," Aug. 2023. doi: 10.6028/nist.cswp.29.

[10] F. B. Kokulu et al., "Matched and Mismatched SOCs: A Qualitative study on Security Operations Center issues," 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), p. 16, 2019, [Online]. Available: https://doi.org/10.1145/3319535.3354239

[11] S. Sauter et al., "NIOSH worker well-being questionnaire (WellBQ).," Feb. 2024. doi: 10.26616/nioshpub2021110revised032024.

[12] A. Loconsolo, "Securing digital identities: From the deployment to the analysis of a PKI ecosystem with virtual HSMs leveraging open-source tools," Ph.D. dissertation, Politecnico di Torino, Italy, 2024.

[13] M. Anastasova, R. Azarderakhsh, and M. M. Kermani, "Fully Hybrid TLSv1.3 in WolfSSL on Cortex-M4," in *Proc. Int. Conf. Appl. Cryptogr. Netw. Security*, 2024, pp. 376–395.

[14] D. Stebila, M. Campagna, and L. Chen, "Post-quantum key exchange for the Internet and the Open Quantum Safe project," Proc. IEEE, vol. 108, no. 10, pp. 1780–1802, Oct. 2020, doi: 10.1109/JPROC.2020.3008703.

[15] N. Bindel and S. McCarthy, "The need for being explicit: Failed attempts to construct implicit certificates from lattices," *Comput. J.*, vol. 66, no. 6, pp. 1320–1334, 2023.

[16] T. E. Carroll, L. M. Redington, A. M. Moran-Schmoker, and A. J. Murray, "Inventory of Public Key Cryptography in US Electric Vehicle Charging," Pacific Northwest National Laboratory (PNNL), 2023.

[17] K. Krishan, "Implementation of quantum-safe VPN," M.S. thesis, Faculty of Informatics, Masaryk Univ., Brno, Czech Republic, 2025.

[18] G. D'Onghia, D. G. Berbecaru, and A. Lioy, "Shaping a Quantum-Resistant Future: Strategies for Post-Quantum PKI," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, 2024, pp. 1–6.

[19] D. Berger, M. Lemoudden, and W. J. Buchanan, "Post-Quantum Migration of the Tor Application," *J. Cybersecurity Privacy*, vol. 5, no. 2, p. 13, 2025.

[20] W. Yang, X. Li, Z. Feng, and J. Hao, "TLSsem: A TLS security-enhanced mechanism against MITM attacks in public WiFis," in *Proc. 22nd Int. Conf. Eng. Complex Comput. Syst. (ICECCS)*, 2017, pp. 30–39.

[21] L. P. Fraile *et al.*, "Enabling Quantum-Resistant EDHOC: Design and Performance Evaluation," *IEEE Access*, 2025.

[22] Q. Khan *et al.*, "Toward Post-Quantum Digital Certificate for eSIM," in *Proc. Silicon Valley Cybersecurity Conf. (SVCC)*, 2024, pp. 1–3.

[23] S. Sunahara *et al.*, "A Framework for Institutional Privacy Considered Full DNS over HTTPS Architecture," *IEEE Access*, 2025.

[24] J. E. R. F. de Oliveira, "qSCMS: Post-quantum security credential management system for vehicular communications," Ph.D. dissertation, Univ. São Paulo, Brazil, 2019.

[25] T. Waseem, "Analysis of PQConnect," Master dissertation, Tampere University, Finland, 2025.

[26] H. Kwon, "Secure and Scalable Device Attestation Protocol with Aggregate Signature," *Symmetry*, vol. 17, no. 5, p. 698, 2025.

[27] S. Paul, P. Scheible, and F. Wiemer, "Towards post-quantum security for cyber-physical systems: Integrating PQC into industrial M2M communication," *J. Comput. Security*, vol. 30, no. 4, pp. 623–653, 2022.

[28] J. Samandari and C. Gritti, "Post-Quantum Authentication and Integrity in 3-Layer IoT Architectures," in *Proc. Int. Conf. Privacy, Security and Trust (PST)*, 2024, pp. 1–11.

[29] G. Kornaros, G. Berki, and M. Grammatikakis, "Quantum-secure communication for trusted edge computing with IoT devices," in *Proc. IFIP Int. Conf. ICT Syst. Security and Privacy Protection*, 2023, pp. 163–176.

[30] J. Stapleton and W. C. Epstein, *Security Without Obscurity: A Guide to PKI Operations*. Boca Raton, FL, USA: CRC Press, 2024.