Before the Vicious Cycle Starts: Preventing Burnout Across SOC Roles Through Flow-Aligned Design

Kashyap Thimmaraju*, Duc Anh Hoang*, Souradip Nath†, Jaron Mink† and Gail-Joon Ahn†
*Technische Universität Berlin
Email: kashyap.thimmaraju@tu-berlin.de, duc-anh.hoang@campus.tu-berlin.de
†Arizona State University
Email: {snath8, jaron.mink, gahn}@asu.edu

***Abstract*—The sustainability of Security Operations Centers depends on their people, yet 71% of practitioners report burnout and 24% plan to exit cybersecurity entirely. Flow theory offers a lens for understanding this human factor challenge: when job demands misalign with practitioner capabilities—whether through excessive complexity or insufficient challenge—work becomes overwhelming or tedious rather than engaging. We argue that achieving this balance begins at hiring, the earliest intervention point in a practitioner's organizational journey. If job descriptions inaccurately portray role requirements, organizations risk recruiting underskilled practitioners who face chronic anxiety or overskilled ones who experience boredom. Both misalignments trigger burnout pathways, yet we lack empirical understanding of what skills and experience levels current SOC job descriptions actually specify, making it impossible to assess whether stated requirements set practitioners up for flow or frustration.**

We address this gap by analyzing SOC job descriptions to establish the baseline of what challenge-skill profiles organizations claim to require. We collected and analyzed 106 public SOC job postings from November to December 2024 across 35 organizations in 11 countries, covering a range of SOC roles: Analysts, Incident Responders, Threat Hunters, and SOC Managers. Using Inductive Content Analysis, we coded certifications, technical skills, soft skills, tasks, and experience requirements (see Table I for an overview). Our preliminary analysis revealed three key patterns: (1) Communication skills dominate requirements (50.9% of 106 postings), substantially exceeding technical specifications like SIEM tools (18.9% of 106) or programming (30.2% of 106) suggesting that organizations prioritize communication and collaboration over purely technical capabilities. (2) Certification expectations are varied: CISSP leads (22% of 106), but 43 distinct credentials appear with no universal standard, creating uncertainty for practitioners about which certifications merit investment. (3) Technical requirements show clear patterns: Python dominates programming (27% of 106), Splunk leads SIEM platforms (14% of 106), and ISO 27001 (13% of 106) and NIST (10% of 106) are the most cited standards, indicating an emerging consensus on core technical competencies that can guide both hiring decisions and training priorities.

This work represents the first stage of a research agenda to prevent burnout through sustained alignment of challenge-skill. The findings from this study establish an empirical baseline for what organizations claim to need, enabling validation studies that compare the stated requirements with actual practice.

TABLE I
PERCENTAGE OF JOB DESCRIPTIONS (N=106) MENTIONING A SUBSET OF SKILL CATEGORIES.

Skill Category	**Count**	**% of Postings**
Professional Skills	84	79.2%
Threat Intelligence	58	54.7%
Certifications	36	34.0%
Programming	32	30.2%
Security Standards	22	20.8%
SIEM Tools	20	18.9%

I. INTRODUCTION

Security Operations Centers (SOCs) are responsible for continuous monitoring, threat detection, incident response, and vulnerability management within organizations [1]. SOC practitioners work in environments where cognitive demands are high, decisions must be made rapidly under uncertainty, and the consequences of errors can be severe. In principle, such work should foster conditions for optimal human performance according to flow theory [2]–[4]: clear goals, immediate feedback, and meaningful challenges that develop practitioners' capabilities. Yet reality reveals a stark mismatch between this potential and actual outcomes.

Recent industry surveys document troubling patterns. Tines' 2023 Voice of the SOC report found that 71% of SOC analysts experience burnout, with 64% considering leaving their jobs within a year [5]. A 2023 Devo/Wakefield Research survey revealed that 83% of IT security professionals admit they or someone in their department has made errors due to burnout that led to security breaches, with 85% anticipating they will leave their role due to burnout and 24% planning to exit cybersecurity entirely [6]. For SOC leaders, 62% of CISOs globally reported experiencing burnout in 2023 [7]. The organizational consequences are severe: 23% of SOC leaders report losing up to 19% of their staff annually, with some

Workshop on Security Operation Center Operations and Construction (WOSOC) 2026
23 February 2026, San Diego, CA, USA
ISBN 978-1-970672-03-9
https://dx.doi.org/10.14722/wosoc.2026.23009
www.ndss-symposium.org

organizations losing 40% or more of their teams [8], and the average time to fill a SOC position is seven months, with 15% of organizations reporting it takes two years or longer [8].

This persistent attrition and burnout represents not merely a human resources challenge but a fundamental threat to organizational security. When practitioners burn out and leave, institutional knowledge departs with them, leaving organizations vulnerable during extended hiring periods [9], [10]. The human cost is equally concerning: exhaustion, cynicism, and a sense of inefficacy pervade the field [11]–[15]

Multiple theoretical frameworks converge on a common explanation: person-role misfit, particularly skill-challenge mismatch. Maslach's Areas of Worklife model identifies six domains that, when misaligned, trigger burnout: workload, control, reward, community, fairness, and values [16]. Nepal et al.'s recent mixed-methods study of 35 incident responders identified workload, changing priorities, lack of clear goals and feedback, and inadequate recognition as key burnout factors Sundaramurthy et al.'s "Vicious Cycle Theory" traces burnout in the SOC to its origins: analysts whose skills are underdeveloped are not empowered to develop those skills due to lack of managerial trust, creating a self-reinforcing cycle of underperformance and disengagement that ultimately leads to departure [17].

Flow theory, as articulated by Csíkszentmihályi, provides a complementary lens for understanding these dynamics [2], [18]. Flow—the state of optimal experience where individuals are fully immersed and performing optimally—requires a delicate balance between task challenge and individual skill. When challenges significantly exceed skills, anxiety results. When skills significantly exceed challenges, boredom sets in. Research on software developers has demonstrated that practitioners who are in the flow-state, experience both higher productivity and greater well-being [19], [20]. If practitioners are in roles or enter roles either underskilled or overskilled for the demands they face, the mismatch might prevent flow and establishes conditions for the burnout cycle Sundaramurthy et al. identified.

Identifying the intervention point for preventing these cycles requires considering when different burnout factors emerge. Many factors manifest post-hiring as identified by Nepal et al. [12] in their study of incident responders who were past their "honeymoon" phase in their job: workload management, team dynamics, organizational support structures, and resource allocation practices develop over time within organizations. However, one critical factor can be addressed pre-hiring: the match between practitioner skills and role demands. If candidates enter SOC roles with skills appropriately calibrated to the challenges they will face, we establish the foundation for flow rather than frustration. This requires clarity about what skills different SOC roles actually demand. Yet organizations may neither accurately communicate these requirements nor fully understand them themselves.

Job descriptions (JDs) currently serve as the primary mechanism through which organizations communicate role requirements to potential candidates. In principle, accurate JDs fulfill multiple functions: they help organizations attract appropriately skilled candidates, enable candidates to self-select into roles matching their capabilities, and establish clear expectations that support the "clear goals" dimension of flow theory [3]. However, we hypothesize that current JDs may not accurately reflect the skills and experience truly needed for SOC roles. Some may list requirements that are overly generic, others may emphasize certifications over practical competencies, and still others may fail to capture the resilience, communication and collaboration demands that research suggests are central to SOC effectiveness [21], [22].

Our vision involves transforming the hiring pipeline to prevent burnout in SOCs. In particular, to validate and refine SOC job descriptions to support better challenge-skill alignment in hiring as a vicious cycle prevention strategy. This requires a two-stage research approach: first, systematically analyzing what JDs currently demand; second, validating these stated requirements against actual role demands as understood by practitioners and hiring managers. Such (in)validation would identify mismatches: where JDs either under-specify or misspecify requirements; and enable creation of more accurate JDs that support better hiring decisions. We hypothesize that accurate JDs, combined with flow-aligned hiring practices, can prevent the skill-challenge mismatch that triggers the Vicious Cycle [17] and ultimately contributes to burnout. We note this hypothesis requires empirical validation through systematic research comparing stated requirements with actual practice and tracking outcomes over time.

In this paper, we take the critical first step: systematically analyzing what SOC job descriptions currently demand. We collected 106 public SOC job postings from November–December 2024 across Europe, Asia, and North America, spanning four key roles: Analysts, Incident Responders, Threat Hunters, and SOC Managers. Using an Inductive Content Analysis approach [23], we coded certifications, technical skills, soft skills, tasks, and experience requirements. The coding process revealed challenges in source data *and* analyzed data quality and consistency that necessitate careful interpretation. Nevertheless, this preliminary systematization provides observations about current JD practices and establishes an empirical foundation for subsequent validation studies.

We make the following *contributions*:

- Using an interdisciplinary approach we present a flow-based theory that explains why burnout occurs based on the vicious cycle theory for SOC burnout and how to prevent it from occurring in the SOC.
- We present a dataset of 106 SOC job descriptions from 11 countries across three continents, offering a broad empirical view of how organizations currently communicate **SOC role requirements**.
- We developed and publicly share a **preliminary codebook** for systematically analyzing SOC job descriptions, capturing certifications, technical skills, soft skills, tasks, and experience requirements across roles.

https://git.tu-berlin.de/wosoc-2026/soc-jd-analysis

- We document key observations about current JD practices, including communication emphasis, vagueness challenges, certification and tool patterns, experience requirement inconsistencies, and gaps in resilience-related attributes, establishing the empirical foundation for validation research and JD refinement efforts.
- We articulate a research agenda for validating JD requirements against actual practice and testing whether accurate JDs combined with flow-aligned hiring can prevent the skill-challenge-trust mismatch that contributes to SOC burnout.

Ethical Considerations. All Job Descriptions were gathered from public sources and no people were involved in this research which exempted us from visiting the institutional review board. All the key concepts, ideas and data were created by us however, we leveraged AI-tools to improve the writing of this paper.

Paper Structure. The remainder of this paper is organized as follows. We provide background on the SOC organizational structure in Section II, and on theoretical frameworks for understanding burnout in Section III. In Section IV we discuss the challenge-skill balance and its implications for SOC hiring. Our analysis of SOC job descriptions, including the data collection and coding methodology are detailed in Section V. Our preliminary findings are presented in Section VI followed by a discussion in Section VII. We then highlight related work in Section VIII and then conclude in Section IX.

II. SOC Organizational Structure and Roles

An increasing number of organizations now operate a SOC team, where a specialized group is responsible for cybersecurity incidents. SOC teams are typically structured across four hierarchical tiers with distinct roles and their responsibilities, tasks, and skills [21], [24]. Understanding these distinct roles is essential for analyzing how job descriptions communicate requirements and whether those requirements support appropriate challenge-skill matching.

SOC Analysts are responsible for the initial evaluation and prioritization of incoming security alerts, activities, and anomalies. They serve as the first line of defense and escalate relevant incidents to the next higher tier [21]. **Incident Responders** conduct in-depth investigations of the security incidents escalated by the SOC analyst. For these conducted analyses and assessments they require a wide variety of threat intelligence tools [25]. Additionally, they are tasked to develop and implement strategies as well as protocols, playbooks, to mitigate and recover from security incidents. **Threat Hunters** proactively track down previously undetected threats and develop advanced techniques and security tools. Furthermore, they handle escalated security incidents and perform in-depth system research to identify possible vulnerabilities and gaps to prevent security incidents from occurring. **SOC Managers** are tasked to lead the SOC team oversee processes, ensure governance and compliance with policies, and give strategic directions.

III. Theoretical Frameworks for Understanding SOC Burnout

Three complementary theoretical frameworks inform our understanding of burnout and attrition in SOC environments, each highlighting the critical role of person-role fit and skill-challenge alignment.

Areas of Worklife. Leiter and Maslach [16] identify six domains that, when misaligned between person and work environment, contribute to burnout: workload, control, reward, community, fairness, and values. Among these, workload-capability mismatch is particularly relevant to hiring practices. Misalignment in workload occurs when job demands exceed the resources available to an individual [26]. When practitioners are hired into roles for which they lack sufficient skills, they face workload demands they cannot adequately manage, establishing conditions for chronic stress rather than sustainable engagement. Similarly, lack of control manifests when practitioners have insufficient authority or autonomy to perform their responsibilities effectively. When underskilled practitioners are not trusted with decision-making authority appropriate to their role, they experience reduced control, compounding the workload mismatch. Accurate job descriptions that clearly communicate required skill levels can help prevent these misalignments by enabling better person-role matching from the outset.

Vicious Cycle Theory. Sundaramurthy et al. [17] developed the Vicious Cycle Theory through an ethnographic study of SOC analysts, identifying how burnout develops through a self-reinforcing pattern. The cycle begins when analysts whose skills are underdeveloped are not empowered to develop those skills due to lack of managerial trust. This creates underperformance, which further reduces trust and empowerment, eventually leading to departure. The theory identifies skill-challenge mismatch at entry as a critical trigger: if practitioners begin with skills inadequately calibrated to their role's demands or unable to grow their skills, they enter the cycle immediately. Conversely, appropriate skill-role matching at entry enables practitioners to build trust, develop capabilities, and avoid the cycle entirely. This suggests that hiring decisions informed by accurate job descriptions could serve as an intervention point to prevent the Vicious Cycle before it starts.

Flow Theory. Csíkszentmihályi [2], [18] describes flow as the psychology of optimal experience where individuals report being "in the zone." Flow is an integral aspect of Positive Psychology and falls under the umbrella of Positive Engagement in the PERMA theory [27]. It is in the flow state where we feel and perform our best [4] and is considered to be the antipode (opposite) of burnout [12]. Being in the flow state can be characterized by nine dimensions: challenge-skill balance, merging of action and awareness, clear goals, immediate feedback, complete concentration, sense of control, loss of self-consciousness, time transformation, and autotelic ("joy of doing") experience. Among these, challenge-skill balance is foundational to entering the so-called flow channel illustrated in Figure 1. When task challenges slightly exceed

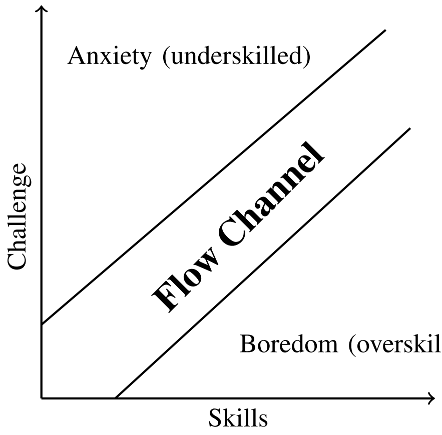

Fig. 1. The Flow Channel: Challenge-Skill Balance. When skills match challenges, individuals enter the flow state. Skills below challenge level lead to anxiety (underskilled), while skills exceeding challenges result in boredom (overskilled).

one's skill level, flow occurs; when challenges significantly exceed skills, anxiety results; when skills significantly exceed challenges, boredom sets in. Research on software developers has demonstrated that practitioners who achieve flow experience both higher productivity and greater well-being [19], [20].

IV. The Challenge-Skill Balance and Its Implications for SOC Hiring

The challenge-skill balance is particularly crucial for understanding work performance and well-being. While it is not always possible (or even unnecessary) to achieve flow in every task, persistent patterns of anxiety or boredom over extended periods can lead to burnout and attrition, potentially triggering the Vicious Cycle. When practitioners consistently operate in the anxiety zone, they may be unable to upskill effectively due to cognitive overload [28]–[30] and stress [31]. Alternatively, when practitioners persistently experience boredom, skill atrophy and disengagement may prevent them from taking on appropriately challenging work. In both cases, organizational factors such as inadequate training, lack of mentorship, or rigid role definitions may compound the challenge-skill mismatch.

This challenge-skill balance framework suggests important implications for SOC hiring. If practitioners enter roles with skills mismatched to the demands they face, they will struggle to achieve flow, instead experiencing either chronic anxiety (underskilled) or persistent boredom (overskilled), both very likely cases when analyzing SIEM alerts. Both states contribute to the burnout patterns documented in SOC environments. Establishing appropriate challenge-skill alignment from the outset requires clarity about knowing what JDs look like currently, what different SOC roles actually demand and whether organizations accurately communicate these requirements in their hiring materials. In the next section, we elaborate on our preliminary observations of 106 JDs from December 2024.

TABLE II
Preliminary Role Distribution in Dataset (n=107)

SOC Role	n
SOC Analyst	17
Incident Responder	38
Threat Hunter	39
SOC Manager	12

V. SOC Job Description Analysis

A. Data Collection

We collected 106 public SOC job postings between November and December 2024 from online job platforms (Indeed, StepStone, LinkedIn), company career pages and cybersecurity-specific recruiting companies. The dataset spans 35 organizations across Europe, Asia, and North America, including technology companies (Google, Microsoft, Meta), financial institutions (Citi), automotive manufacturers (Tesla, Mercedes-Benz), and specialized security firms (DCSO, Expel).

Job postings were included if they specified roles operating within or closely collaborating with SOCs. From initially screened advertisements, we selected most postings that articulated "basic" role requirements and responsibilities, this means we included some vague descriptions with insufficient detail. The final dataset tabulated in Table II roughly comprises of 17 SOC Analyst positions, 38 Incident Responder positions, 39 Threat Hunter positions, and 12 SOC Manager positions. We note here that we made subjective decisions about classifying a JD into one of the four roles we consider as part of the SOC. A complete list of organizations and posting counts appears in Table VIII Appendix A and also online.

https://git.tu-berlin.de/wosoc-2026/soc-jd-analysis

For each posting, we extracted role-relevant content including required qualifications, technical and soft skills, certifications, academic degrees, experience requirements, and responsibilities. Marketing content and benefit descriptions were excluded. We manually entered each posting into MAXQDA qualitative data analysis software, assigning each a unique identifier and standardizing the content into a consistent format for analysis.

B. Coding Methodology

Using Inductive Content Analysis [23] our coding process proceeded in four phases using MAXQDA.

Phase 1: Open Coding. Each job description was examined line-by-line to identify relevant keywords, allowing categories to emerge inductively from the data. While some categories appeared as explicit headings within postings (e.g., "Required Skills"), additional patterns surfaced through systematic analysis. This initial iteration produced six main categories: Certifications, Degree, Experience, Soft Skills, Technical Skills, and Tasks.

Phase 2: Category Refinement. Technical Skills were subdivided into nine domains (Data Management, Forensics, Identity and Access Management, Incident Response, Programming and Frameworks, Security Management and Governance, Security Monitoring and Attack Detection, Technologies and Infrastructure, Threat Intelligence and Hunting). Tasks were organized into eight categories (Analysis and Evaluation, Communication and Collaboration, Development and Innovation, Documentation and Management, Implementation and Operations, Incident Response and Risk Management, Learning, Planning and Strategy). Experience was divided into years of experience and role-specific experience requirements.

Phase 3: Automated Coding and Iteration. Identified keywords were coded using RegEx patterns in MAXQDA, enabling consistent application across the full dataset. The process was iterated multiple times, combining manual corrections with automated procedures to capture keyword variations and resolve ambiguities, achieving theoretical saturation.

Phase 4: Experience Categorization. Several job descriptions did not specify experience explicitly in years, or mentioned experience with specific categories from Phase 2, which made coding experience very challenging, we consider improving this aspect as future work. The approach taken in the public codebook has been to develop experience bands that map to qualitative descriptors of "experience": 1–2 years (early career, entry level, bachelor's degree), 3–5 years (mid-level, moderate, several, significant, proficient, master's degree, PhD), 6–10 years (extensive, seasoned, advanced), and 11+ years (senior level, expert level). Postings with no experience requirements were coded as "not required." Note that we did not analyze the experience category due to coding being unreliable.

C. Data Quality Observations.

This analysis faced several methodological constraints that affect interpretation. Job description quality varied substantially: some postings provided detailed competency frameworks with specific tools and technologies, while others used generic language such as "strong analytical skills" or "excellent communication abilities" without operational definitions. Experience requirements presented particular challenges—many postings used qualitative descriptors ("proficient", "senior-level", "extensive experience") that map ambiguously to actual capability levels, making systematic coding difficult. Coding was performed by a single researcher without inter-rater reliability testing, introducing potential interpretation variance and ambiguities. Most critically, stated requirements may not reflect actual hiring practices: recruiters may use job descriptions as aspirational specifications while accepting candidates meeting only subsets of requirements, or conversely, may prioritize unlisted characteristics during selection. These limitations highlight that *our analysis captures what organizations claim to require rather than what they actually require or what skills predict success in these roles.* The complete codebook and frequency distributions are available online.

VI. Our Preliminary Findings

The dataset reflects operational SOC workforce needs, with the majority of roles in hands-on security operations rather than management positions. Table I summarizes the overall coverage of different skill categories across the dataset. Due to coding quality, we do not present analyses for experience and technical skills but instead highlight some keywords.

TABLE III
Top 10 Professional Skills in SOC Job Descriptions (N=106). Emphasis column shows percentage of the 84 postings that mentioned professional skills.

Skill	Count	Cov. (%)	Emph. (%)
Communication	54	50.9	64.3
Writing skills	29	27.4	34.5
Teamwork Abilities	26	24.5	31.0
Problem solving skills	24	22.6	28.6
Analytical skills & mindset	24	22.6	28.6
Structured & Reliable Work Style	20	18.9	23.8
Motivated	15	14.2	17.9
On Call Availability	12	11.3	14.3
Attention to Detail	12	11.3	14.3
Adaptable	9	8.5	10.7

TABLE IV
Top 10 Professional Certifications in SOC Job Descriptions (N=106). Emphasis column shows percentage of the 36 postings that mentioned certifications.

Skill	Count	Cov. (%)	Emph. (%)
CISSP - Certified Information Systems Security Professional	24	22.6	66.7
CISM - Certified Information Security Manager	13	12.3	36.1
CEH - Certified Ethical Hacker	11	10.4	30.6
GCIH	10	9.4	27.8
Security+	10	9.4	27.8
SANS	9	8.5	25.0
GIAC	9	8.5	25.0
OSCP - Offensive Security Certified Professional	9	8.5	25.0
CCNA	7	6.6	19.4
GCIA	7	6.6	19.4

TABLE V
Top 10 Programming Languages in SOC Job Descriptions (N=106). Emphasis column shows percentage of the 32 postings that mentioned programming languages.

Skill	Count	Cov. (%)	Emph. (%)
Python	29	27.4	90.6
Go	10	9.4	31.2
PowerShell	10	9.4	31.2
Java	9	8.5	28.1
C, C#, C++	7	6.6	21.9
BASH - Bourne Again Shell	7	6.6	21.9
Scala	4	3.8	12.5
PHP	4	3.8	12.5
JavaScript	3	2.8	9.4
Perl	3	2.8	9.4

(1) Communication skills dominate requirements. Communication skills appeared in 54 of 106 postings (50.9%),

TABLE VI
SIEM PLATFORMS IN SOC JOB DESCRIPTIONS (N=106). EMPHASIS COLUMN SHOWS PERCENTAGE OF THE 20 POSTINGS THAT MENTIONED SIEM PLATFORMS.

Skill	Count	Cov. (%)	Emph. (%)
Splunk	15	14.2	75.0
Microsoft Sentinel	5	4.7	25.0
Elasticsearch	4	3.8	20.0
Microsoft Defender	4	3.8	20.0
ArcSight	3	2.8	15.0
QRadar	3	2.8	15.0
Kibana	1	0.9	5.0
Google Chronicle	1	0.9	5.0

TABLE VII
TOP 10 SECURITY STANDARDS AND FRAMEWORKS IN SOC JOB DESCRIPTIONS (N=106). EMPHASIS COLUMN SHOWS PERCENTAGE OF THE 22 POSTINGS THAT MENTIONED SECURITY STANDARDS.

Skill	Count	Cov. (%)	Emph. (%)
ISO 27001	14	13.2	63.6
NIST - National Institute of Standards and Technology	11	10.4	50.0
GDPR	6	5.7	27.3
OWASP	4	3.8	18.2
SOC 2	3	2.8	13.6
FedRAMP	3	2.8	13.6
CIS	2	1.9	9.1
STIG	2	1.9	9.1
IEC62443	2	1.9	9.1
NIS2	1	0.9	4.5

with writing explicitly emphasized in 29 postings (27.4%), as shown in Table III. Combined, more than 60% of job descriptions emphasize communication capabilities. This substantially exceeds technical specifications: SIEM tools appeared in only 18.9% of postings (Table VI), while programming requirements appeared in 30.2% of postings. Among soft skills (Table III), teamwork abilities (24.5%), problem-solving (22.6%), and analytical thinking (22.6%) constitute the cognitive and collaborative competencies organizations seek, but communication remains the single most consistently mentioned requirement across all position types.

(2) Certification expectations are varied with no dominant standard. While 34.0% of postings (36 of 106) mentioned at least one certification, as shown in Table IV, CISSP led among those requiring credentials (appearing in 66.7% of certification-mentioning postings, or 22.6% of all postings overall). CISM (12.3% of all postings) and CEH (10.4%) followed at substantially lower rates. The presence of 43 distinct certifications across the dataset suggests organizations recognize multiple paths to demonstrating competency. This diversity may reflect the varied technical domains within SOC work (monitoring, incident response, threat hunting, forensics) and the absence of a single universally recognized SOC credential. Notably, however, two-thirds of all postings (66.0%) made no mention of certifications, suggesting credentials may be preferred rather than strictly required.

(3) Technical requirements show technology-specific patterns. Due to coding quality, we restricted our analysis to programming languages, SIEM tools, standards and certifications. When organizations specified technical requirements, clear patterns emerged. Python dominated programming requirements (27.4% of all postings, appearing in 90.6% of the 32 programming-mentioning postings), as shown in Table V. PowerShell (9.4% of all postings), Go (9.4%), and Java (8.5%) trailed substantially. SIEM platform specifications were relatively uncommon (18.9% of postings overall), but when mentioned, Splunk dominated (75.0% of SIEM-mentioning postings, or 14.2% of all postings), with Microsoft Sentinel (4.7% of all postings), Elasticsearch (3.8%), and Microsoft Defender (3.8%) mentioned occasionally (Table VI). Security standards knowledge appeared in 20.8% of postings, with ISO 27001 (13.2% of all postings) and NIST (10.4%) most frequently cited (Table VII). Among technical skill categories, incident response dominated (33.0% of all postings), followed by forensics (22.6%), reflecting the operational priorities of SOC work.

While this analysis establishes what organizations claim to need in job descriptions, it cannot answer the more fundamental question: do candidates meeting these stated requirements actually achieve challenge-skill balance on the job? A candidate with Python skills and CISSP certification might still experience anxiety if assigned tasks beyond their capability level, or boredom if relegated to routine monitoring work that underutilizes their expertise. Job descriptions specify credentials and competencies but not the challenges those credentials must address, nor the organizational context in which practitioners will apply their skills.

VII. DISCUSSION

A. Connecting Findings to the Flow Channel

Several findings support flow-enabling conditions. Communication emphasis (50.9% of 106 postings) aligns with research showing that feedback loops and clear goals—both essential flow dimensions—emerge from effective collaboration [32], [33]. However, excessive communication demands can fragment attention and disrupt flow states [19], [20], creating tension between coordination needs and deep focus. Python dominance (27.4% of 106) enables automation that can reduce cognitive load on routine tasks, freeing mental capacity for appropriately challenging analytical work—a prerequisite for entering flow. Other findings reveal barriers to flow assessment and achievement. Certification ambiguity (43 distinct credentials with no dominant standard) creates uncertainty that undermines candidates' ability to accurately gauge their skill levels relative to role demands. Resilience received rare mention (8.5% of 106 postings) despite research emphasis on its importance for SOC work [12], [21], [22]. We acknowledge that explicitly mentioning resilience in job descriptions may be challenging; however, it should be assessed during interviews to evaluate candidates' capacity to maintain flow under operational stress. Learning agility appeared infrequently (6.6% of 106) despite rapid threat evolution requiring continuous upskilling to prevent practitioners' skills from falling below evolving challenge levels, a trajectory toward the anxiety zone. Most critically, job descriptions specify credentials and tools but provide limited guidance about challenge complexity: the actual difficulty, ambiguity, and cognitive demands of daily tasks. While JDs serve as initial guides rather than complete specifications, this gap highlights the need for interview processes that systematically assess challenge-skill alignment. Our findings thus establish the baseline skill landscape from JDs, pointing toward the next research stage: examining how SOC interviews can capture the challenge dimensions necessary for accurate flow assessment and preventing the vicious cycle of underskilling, disempowerment, and burnout.

B. Connecting Findings to the Vicious Cycle Theory and Challenge-Skill Balance

To prevent a SOC practitioner from entering the "Low skills" state of the Vicious Cycle and leading to burnout, the challenge-skill balance plays a central role. Sundaramurthy et al.'s ethnographic research identified a destructive pattern: practitioners hired without sufficient skills become overwhelmed by operational demands, leading managers to withhold autonomy and trust, which further limits skill development opportunities and ultimately drives burnout and attrition [17]. Our job description findings reveal both opportunities and risks for breaking this cycle at the hiring stage. Previous research has identified that people in cybersecurity commonly find meaning and purpose in the work they do, which supports entering the flow channel and brings intrinsic motivation [31]. However, intrinsic motivation alone cannot sustain engagement when practitioners lack the skills to meet role demands or when skill growth stagnates. Our analysis shows that organizations specify extensive technical skill requirements—monitoring infrastructure (47.2% of 106 postings), threat intelligence (54.7% of 106), programming capabilities (27.4% of 106 for Python): providing a foundation for initial skill-challenge alignment. Yet the absence of explicit learning expectations (learning agility mentioned in only 6.6% of 106 postings) signals a potential gap in supporting continuous skill development necessary to prevent practitioners from falling behind evolving threat landscapes. When candidates and organizations accurately assess initial fit for SOC roles, practitioners enter roles neither severely underskilled (risking immediate anxiety and loss of manager trust) nor severely overskilled (risking immediate boredom). However, maintaining this balance over time requires what Leiter et al. terms "control", the autonomy to make decisions, apply judgment, and develop expertise through meaningful work [16]. Communication emphasis in 50.9% of 106 postings suggests collaborative environments where practitioners might exercise such autonomy, but job descriptions rarely make explicit the decision-making authority or growth opportunities that enable skill development, hopefully this is assessed during the interview. Hence, preventing the Vicious Cycle requires managers to trust employees with appropriate autonomy once initial skill-challenge alignment is established through hiring. As practitioners develop technical capabilities in areas like SIEM platforms, scripting, or threat analysis, teams and organizations should consider progressively complex tasks that maintain flow. Without this progression, even well-matched hires eventually become overskilled for their assigned responsibilities, leading to disengagement: a different path to burnout than the underskilled trajectory, but equally damaging to retention and performance.

C. Follow-Up Validation Studies Needed

Our job description analysis reveals what organizations claim to need, but validation against actual practice remains essential. Do candidates meeting these stated requirements achieve challenge-skill balance? Does communication emphasis in job descriptions translate to actual collaborative work? Do Python skills predict success, or do other factors dominate? These questions require practitioner and manager surveys, longitudinal tracking of hiring outcomes, and systematic assessment of challenge-skill alignment in operational contexts.

D. Recommendations and Future Work

We recommend, organizations to reduce credential ambiguity and clarify learning expectations in their JDs. Candidates should probe for challenge calibration and autonomy during interviews. Researchers should validate stated requirements against actual practice, longitudinal tracking of hiring cohorts, analysis of AI's impact on SOC skills, correlate job description accuracy with hiring outcomes and retention, and examine how AI integration affects role requirements.

VIII. Related Work

Research on SOC roles, structure and skills have been conducted by a handful of researchers in the past, however, none to the best of our knowledge leverage their research to prevent burnout. In the following we highlight how our findings correlate with related work.

A. SOC Roles and Structure

Understanding SOC organizational structure and role definitions provides essential context for analyzing job requirements. Vielberth et al. [21] offer a comprehensive view of SOCs, highlighting key roles, required skills, and operational challenges from research in 2020. Building on this foundation, Hofbauer and Mayer [25] provide a structured overview of key SOC roles and tools through a systematic literature review with expert interviews. In particular, the authors enumerated several technical, management, and consulting SOC roles that inform our understanding of the SOC landscape. Complementing these taxonomic efforts, Reisser et al. [22] employed an interview-based data collection methodology with eight practitioners, which contrasts with our more passive JD analysis. The authors observed that "ability to work in a team" was a frequently cited soft skill, which we also found in 30% of the 106 JDs in our dataset. In general, our observations on SOC-related skills overlapped with these prior characterizations of the field.

B. SOC Skills Assessment

While role definitions establish what SOC positions exist, understanding how to assess practitioner capabilities remains a distinct challenge. From a high level view, our analysis of JDs correlates with findings by other researchers, particularly regarding communication as a key soft skill and CISSP as the most commonly cited certification.

Radu et al. [34] designed and developed a set of tests to evaluate the skills of junior SOC analysts. We find that the approach of Radu et al. to tailor the test of skills in the hiring process to better reflect on-the-job situations aligns with our flow-based challenge-skills balance concept.

Extending beyond SOC-specific roles, Sumner et al. [35] presented a survey of the technical and professional skills needed for cybersecurity roles more broadly. As observed in our dataset and in Sumner et al., CISSP was the most-frequently mentioned certification. Similarly, both datasets confirm the presence of cybersecurity frameworks or standards, e.g., NIST and ISO. The concept of in-demand skills mentioned in the paper provides a useful way of prioritizing the availability of skills and what companies really want.

Ullah et al. [36] conducted a large-scale analysis of JDs and Stack Overflow threads and, similar to us, also observed CISSP to be the most cited certification. However, with respect to programming languages, we observed Python more frequently compared to Java. Communication and project management were mentioned as the most important soft skills by Ullah et al., whereas our analysis was not coded with project management. We note that their dataset overlaps a noticeable amount with SOC-related JDs, suggesting convergence in industry requirements across cybersecurity domains.

C. Burnout and Attrition in SOC

While prior work establishes what skills SOC roles require and how to assess them, understanding why practitioners leave these roles is equally critical. The intense workload [12], constant alert fatigue [37], [38], and high-pressure nature of SOC work [12], [17], [39] contribute to stress, burnout, and cognitive overload, ultimately affecting the security of the organizations they protect [11], [24], [40]–[50].

A majority of the research thus far has identified the presence of burnout [11]–[13], [17], [31]. However, research is sparse on preventions tailored to SOCs. In this paper, we leverage an existing theory for burnout in the SOC [17] and present a systematic approach to preventing burnout through flow-state theory, beginning with an empirical analysis of the job requirements that establish initial challenge-skill alignment.

IX. Conclusion

We set out to address a fundamental question: why does SOC work, which should enable optimal human performance through clear goals, immediate feedback, and meaningful challenges, instead produce burnout rates exceeding 70%? We hypothesized that person-role misfit, particularly skill-challenge mismatch, triggers the Vicious Cycle [17], leading practitioners from underskilling to disempowerment to lack of creativity to lack of growth resulting in burnout and attrition. If accurate job descriptions could support better challenge-skill alignment at hiring, we reasoned, organizations might prevent this cycle before it starts. However, testing this hypothesis required first understanding what SOC job descriptions currently communicate about role requirements.

Our preliminary analysis of 106 SOC job postings from November to December 2024 across 11 countries revealed three key patterns. First, communication skills dominate requirements, appearing in 50.9% of 106 postings and substantially exceeding technical specifications such as SIEM tools (18.9% of 106) or programming languages (30.2% of 106). Second, certification expectations are high but varied, with CISSP appearing most frequently (22.6% of 106 postings) among 43 distinct credentials, yet two-thirds of postings mention no certifications at all. Third, technical requirements show clear technology-specific patterns, with Python dominating programming needs (27.4% of 106), Splunk leading SIEM platforms (14.2% of 106), and ISO 27001 (13.2% of 106) and NIST (10.4% of 106) representing the most frequently cited security standards. These findings establish an empirical baseline for what organizations claim to need, though we acknowledge significant limitations: coding was performed by a single researcher without inter-rater reliability testing, experience and technical requirements proved particularly challenging to systematize due to vague qualitative descriptors, and stated requirements may diverge substantially from actual hiring practices.

The broader implications extend beyond hiring optimization to workforce sustainability and organizational security. If organizations can accurately communicate role requirements and assess challenge-skill fit during hiring, they establish conditions for practitioners to enter the flow channel rather than immediately experiencing anxiety or boredom. Over time, as skills develop, teams and organizations should progressively increase task complexity to maintain flow, preventing the skill stagnation that leads to disengagement or the overwhelming cognitive load that triggers the Vicious Cycle. This requires not just better job descriptions, but flow-aligned interview processes that assess challenge-skill readiness, adaptive role management systems that adjust responsibilities as practitioners develop, and potentially AI-assisted workflows that handle routine cognitive work while preserving appropriately challenging analytical tasks. Preventing SOC burnout thus demands systematic intervention across the employment lifecycle, starting with but extending far beyond hiring.

Acknowledgment

The authors thank the anonymous reviewers for their feedback. First author K. T. thanks Sybe Izaak Rispens for his feedback on an earlier version of this paper, Jean-Pierre Seifert for his support, and acknowledges financial support by the German Federal Ministry of Research, Technology and Space in the framework of the Q-Fiber project number 16KISQ124.

References

[1] C. Rodman, B. Kraus, and J. Novak, "SOC Service Areas: Identification, Prioritization, and Implementation," in *Proceedings 2024 Workshop on Security Operation Center Operations and Construction*. San Diego, CA, USA: Internet Society, 2024. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/wosoc2024-1-paper.pdf

[2] M. Csikszentmihalyi and J. LeFevre, "Optimal experience in work and leisure." *Journal of personality and social psychology*, vol. 56, no. 5, p. 815, 1989, publisher: American Psychological Association.

[3] S. Kotler, "Create a Work Environment That Fosters Flow," *Harvard Business Review*, May 2014. [Online]. Available: https://hbr.org/2014/05/create-a-work-environment-that-fosters-flow

[4] ——, "What Is Flow State? Definition, Benefits, and Tips," 2023. [Online]. Available: https://www.flowresearchcollective.com/blog/what-is-flow-state

[5] Tines, "Voice of the SOC 2023," https://www.tines.com/blog/voice-of-the-soc-2023/, 2023, accessed: 2024-12-11.

[6] Devo Technology and Wakefield Research, "83% of IT security professionals say burnout causes data breaches," https://www.devo.com/company/newsroom/it-security-professionals-say-burnout-causes-data-breaches/, Sep. 2023, accessed: 2024-12-11.

[7] Proofpoint, "2024 voice of the CISO report," https://www.proofpoint.com/uk/newsroom/press-releases/proofpoints-2024-voice-ciso-report, Jul. 2024, accessed: 2024-12-11.

[8] SANS Institute, "It's time to break the SOC analyst burnout cycle," https://www.sans.org/blog/it-s-time-to-break-the-soc-analyst-burnout-cycle, 2023, accessed: 2024-12-11.

[9] Human Performance in Cybersecurity, "Protecting the Protectors: How Coaching Transforms Cybersecurity Professionals," Oct. 2025. [Online]. Available: https://www.youtube.com/watch?v=2AO8oTGUOn8

[10] ——, "Cybersecurity's Frontline: Identifying Burnout Catalysts in Incident Responders," Oct. 2025. [Online]. Available: https://www.youtube.com/watch?v=7GowyF1zzuU

[11] A. Reeves, M. Pattinson, and M. Butavicius, "Is Your CISO Burnt Out yet?: Examining Demographic Differences in Workplace Burnout Amongst Cyber Security Professionals," in *Human Aspects of Information Security and Assurance*. Cham: Springer Nature Switzerland, 2023, vol. 674, pp. 225–236. [Online]. Available: https://link.springer.com/10.1007/978-3-031-38530-8_18

[12] S. Nepal, J. Hernandez, R. Lewis, A. Chaudhry, B. Houck, E. Knudsen, R. Rojas, B. Tankus, H. Prafullchandra, and M. Czerwinski, "Burnout in cybersecurity incident responders: Exploring the factors that light the fire," *Proc. ACM Hum.-Comput. Interact.*, vol. 8, no. CSCW1, Apr. 2024.

[13] K. A. Dupont, "From Burnout to Resilience: Executive Coaching as a Strategic Intervention in Cybersecurity Workforces," 2025.

[14] S. Shelton, "The State of Stress in IT Security 2023," Green Shoe Consulting, Tech. Rep., 2023.

[15] Steve Shelton, "The State of Stress in Cybersecurity 2025," 2025.

[16] M. P. Leiter and C. Maslach, "Areas of worklife: A structured approach to organizational predictors of job burnout," *Research in Occupational Stress and Well-being*, vol. 3, pp. 91–134, 2004.

[17] S. C. Sundaramurthy, A. G. Bardas, J. Case, X. Ou, M. Wesch, J. McHugh, S. R. Rajagopalan, and L. F. Cranor, "A Human Capital Model for Mitigating Security Analyst Burnout," in *USENIX Symposium On Usable Privacy and Security (SOUPS 2015)*, 2015, pp. 347–359. [Online]. Available: https://www.usenix.org/conference/soups2015/proceedings

[18] M. Csikszentmihalyi, *Flow: The psychology of happiness*. Random House, 2013.

[19] A. Noda, A. N. Meyer, D. Ford, M.-A. Storey, N. Marquardt, and T. Zimmermann, "DevEx: What actually drives productivity," *Queue*, vol. 21, no. 2, pp. 35–58, 2023.

[20] N. Forsgren, M.-A. Storey, C. Maddila, T. Zimmermann, B. Houck, and J. Butler, "DevEx in action," pp. 35–51, 2024.

[21] M. Vielberth, F. Böhm, I. Fichtinger, and G. Pernul, "Security operations center: A systematic study and open challenges," *Ieee Access*, vol. 8, pp. 227 756–227 779, 2020.

[22] A. Reisser, M. Vielberth, S. Fohringer, and G. Pernul, "Security Operations Center Roles and Skills: A Comparison of Theory and Practice," in *Data and Applications Security and Privacy XXXVI*, S. Sural and H. Lu, Eds. Cham: Springer International Publishing, 2022, pp. 316–327.

[23] D. F. Vears and L. Gillam, "Inductive content analysis: A guide for beginning qualitative researchers," *Focus on Health Professional Education: A Multi-Professional Journal*, vol. 23, no. 1, pp. 111–127, Mar. 2022, publisher: ANZAHPE: Australian & New Zealand Association for Health Professional Educators. [Online]. Available: https://search.informit.org/doi/abs/10.3316/informit.455663644555599

[24] 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*. London United Kingdom: ACM, Nov. 2019, pp. 1955–1970. [Online]. Available: https://dl.acm.org/doi/10.1145/3319535.3354239

[25] J. Hofbauer and K. Mayer, "Blue team fundamentals: Roles and tools in a security operations center," in *Securware 2024, The Eighteenth International Conference On Emerging Security Information, Systems And Technologies*, 2024.

[26] A. B. Bakker and E. Demerouti, "The Job Demands-Resources model: state of the art," *Journal of Managerial Psychology*, vol. 22, no. 3, pp. 309–328, Apr. 2007. [Online]. Available: https://www.emerald.com/insight/content/doi/10.1108/02683940710733115/full/html

[27] M. Seligman, "PERMA and the building blocks of well-being," *The Journal of Positive Psychology*, vol. 13, no. 4, pp. 333–335, Jul. 2018, publisher: Routledge _eprint: https://doi.org/10.1080/17439760.2018.1437466. [Online]. Available: https://doi.org/10.1080/17439760.2018.1437466

[28] J. Sweller, "Cognitive load theory," in *Psychology of learning and motivation*. Elsevier, 2011, vol. 55, pp. 37–76. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780123876911000028

[29] L. Vaishnav and S. Goel, "The Impact of Cognitive Load on Responses to Security Alerts: Investigating Human Errors," *AMCIS 2025 Proceedings*, Aug. 2025. [Online]. Available: https://aisel.aisnet.org/amcis2025/sig_sec/sig_sec/51

[30] J. Dykstra and C. L. Paul, "Cyber Operations Stress Survey (COSS): Studying fatigue, frustration, and cognitive workload in cybersecurity operations," in *11th USENIX workshop on cyber security experimentation and test (CSET 18)*. Baltimore, MD: USENIX Association, Aug. 2018. [Online]. Available: https://www.usenix.org/system/files/conference/cset18/cset18-paper-dykstra-updated.pdf

[31] K. Thimmaraju, S. I. Rispens, and G.-J. Ahn, "Human Performance in Security Operations: A Survey on Burnout, Well-Being and Flow State Among Practitioners," in *Proceedings 2025 Workshop on Security Operation Center Operations and Construction*. San Diego, CA, USA: Internet Society, 2025. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/wosoc25-final2.pdf

[32] C. J. Walker, "Experiencing flow: Is doing it together better than doing it alone?" *The Journal of Positive Psychology*, vol. 5, no. 1, pp. 3–11, 2010. [Online]. Available: https://doi.org/10.1080/17439760903271116

[33] K. Heyne, D. Pavlas, and E. Salas, "An Investigation on the Effects of Flow State on Team Process and Outcomes," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 55, no. 1, pp. 475–479, Sep. 2011, publisher: SAGE Publications Inc. [Online]. Available: https://journals.sagepub.com/action/showAbstract

[34] A. Radu, L. Kersten, R. Wosyka, T. Mulders, E. Zambon, and L. Allodi, "A Test Tool to Evaluate the Skill Sets of Tier-1 Security Analysts in a SOC Environment: A Case Study from Recruitment to Operations," in *Proceedings 2025 Workshop on Security Operation Center Operations and Construction*. San Diego, CA, USA: Internet Society, 2025. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/wosoc25-final1.pdf

[35] M. Sumner, K. Pearlson, D. Mazzola, and C. Maurer, "What Technical and Professional Skills are Needed for Cybersecurity Roles?" 2023.

[36] F. Ullah, X. Ye, U. Fatima, Z. Akhtar, Y. Wu, and H. Ahmad, "What Skills Do Cyber Security Professionals Need?" Feb. 2025, arXiv:2502.13658 [cs]. [Online]. Available: http://arxiv.org/abs/2502.13658

[37] W. U. Hassan, S. Guo, D. Li, Z. Chen, K. Jee, Z. Li, and A. Bates, "NoDoze: Combatting Threat Alert Fatigue with Automated Provenance Triage," in *Proceedings 2019 Network and Distributed System Security Symposium*. San Diego, CA: Internet Society, 2019. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_03B-1-3_UlHassan_paper.pdf

[38] B. A. Alahmadi, L. Axon, and I. Martinovic, "99% False Positives: A Qualitative Study of SOC Analysts' Perspectives on Security Alarms."

[39] C. Nobles, “Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem,” *HOLISTICA – Journal of Business and Public Administration*, vol. 13, no. 1, pp. 49–72, Jul. 2022. [Online]. Available: https://sciendo.com/article/10.2478/hjbpa-2022-0003

[40] K. R. Jones, D. A. Brucker-Hahn, B. Fidler, and A. G. Bardas, “Work-From-Home and COVID-19: Trajectories of endpoint security management in a security operations center,” in *32nd USENIX security symposium (USENIX security 23)*. Anaheim, CA: USENIX Association, Aug. 2023, pp. 2293–2310. [Online]. Available: https://www.usenix.org/conference/usenixsecurity23/presentation/jones

[41] D. Technology, “83% of IT Security Professionals Say Burnout Causes Data Breaches.” [Online]. Available: https://www.prnewswire.com/news-releases/83-of-it-security-professionals-say-burnout-causes-data-breaches-301931646.html

[42] Nominet, “Life Inside The Perimeter: Understanding the modern CISO,” Tech. Rep., 2019. [Online]. Available: https://media.nominet.uk/wp-content/uploads/2019/02/12130924/Nominet-Cyber_CISO-report_FINAL-130219.pdf

[43] VentureBeat, “Mental health: 66% of cybersecurity analysts experienced burnout this year,” Dec. 2022. [Online]. Available: https://venturebeat.com/security/mental-health-cybersecurity-analysts/

[44] Tines, “Report: State of Mental Health in Cybersecurity,” 2022. [Online]. Available: https://www.tines.com/reports/state-of-mental-health-in-cybersecurity

[45] S. Media, “Mental Health in Cyber Security,” Oct. 2022. [Online]. Available: https://sekuro.io/blog/mental-health-in-cyber-security-whitepaper/

[46] Devo Technology and Wakefield Research, “2022 Devo SOC Performance Report™ SOC Leaders and Staff Are Still Not Aligned,” 2022. [Online]. Available: https://www.csoonline.com/article/573869/information-overload-burnout-talent-retention-impacting-soc-performance.html

[47] VMware, “VMware Report Warns of Deepfake Attacks and Cyber Extortion,” Aug. 2022. [Online]. Available: https://news.vmware.com/releases/vmware-report-warns-of-deepfake-attacks-and-cyber-extortion

[48] Mimecast, “The State of Ransomware Readiness 2022: Reducing the Personal and Business Cost,” 2022. [Online]. Available: https://www.mimecast.com/resources/ebooks/the-state-of-ransomware-readiness-2022/

[49] (ISC)2, “(ISC)2 Cybersecurity Workforce Study,” Tech. Rep., 2022. [Online]. Available: https://www.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study.pdf?rev=ae39d66a4616478792d38da57fb80564&hash=31B8381DC81AD70B9B6DA6FF84534B33

[50] Cynet, “Cynet Reveals 94% of CISOs Suffer from Work-Related Stress and It’s Putting Companies at Risk,” Feb. 2023. [Online]. Available: https://www.businesswire.com/news/home/20230222005112/en/Cynet-Reveals-94-of-CISOs-Suffer-from-Work-Related-Stress-and-It%E2%80%99s-Putting-Companies-at-Risk

Appendix

TABLE VIII
Organizations and Job Posting Counts in Dataset (n=106)

Organization	**n**	**Organization**	**n**
360 SOC Inc	1	Mercedes-Benz	2
Asembia	1	Meta	2
Atruvia AG	2	Microsoft	6
Baker Hughes	2	MHP (Porsche)	3
Citi	4	Motorola Solutions	2
Cloudflare	4	NTT Data	6
Computacenter	2	Otto GmbH	1
DAZN	2	Profiler GmbH	5
DCSO	4	r-tec IT Security	4
Eclaro	1	SilverSky	3
Encora	1	Tesla	4
EthicalHat	2	Trustmi	1
Expel	4	thyssenkrupp AG	3
Google	6	UK Carl Gustav Carus	3
GSK	1	Wiz	2
ION	2	Wipro	4
LB IT Niedersachsen	1	X (formerly Twitter)	5
		Unknown	11

UK = Universitätsklinikum; LB = Landesbetrieb