Issues in Information Systems
Volume 27, Issue 2, pp. 653-668, 2026

DOI: https://doi.org/10.48009/2_iis_2026_143

Cybersecurity analyst labor market trends: A descriptive analysis of online job postings in 2026

Alan Peslak, *Penn State University, arp14@psu.edu*
Jennifer L. Breese, *Penn State University, jzb545@psu.edu*
Brian Gardner, *Penn State University, bkg113@psu.edu*

Abstract

Persistent workforce shortages in cybersecurity have prompted considerable scholarly attention to the alignment between employer demand and pre-employment preparation. This study contributes empirical evidence to that conversation through a content analysis of 369 cybersecurity analyst job postings scraped from PostJobFree.com and analyzed in May 2026. Using a structured taxonomy spanning technical tools, certifications, compliance frameworks, security domains, soft skills, education, and compensation, we document the relative frequency of each requirement across the corpus. Results reveal a labor market characterized by (a) overwhelming preference for remote work arrangements (78.6%), (b) dominance of entry- and junior-level postings (66.1%), (c) modest tool-specific signaling but strong demand for cloud, SIEM, and threat-intelligence competencies, (d) a clear hierarchy of certifications led by CISSP (10.3%) and Security+ (7.0%), (e) heavy concentration of compliance language in defense-adjacent frameworks (DoD/DISA 20.1%, NIST 16.5%), and (f) a bachelor's degree expectation in 47.4% of postings against a near-universal field requirement in cybersecurity (99.7%). Salary data, available in only 12.5% of postings, yielded a mean of $104,673 and a median of $88,186. We discuss implications for curriculum design in undergraduate information technology and cybersecurity programs, while explicitly acknowledging the boundaries imposed by the corpus's brevity, single-source provenance, and limited geographic disclosure.

Keywords: cybersecurity workforce, job postings analysis, labor market signals, curriculum alignment, certifications, information technology education

Introduction

The cybersecurity workforce shortage is among the most frequently cited problems in contemporary information technology policy (Anderson, 2025). Industry surveys consistently report unfilled positions in the millions globally, and U.S. federal initiatives from the National Initiative for Cybersecurity Education (NICE) Framework to recent executive directives on workforce development have responded with calls to expand and modernize the pipeline of qualified analysts (Anieto, 2026; National Initiative for Cybersecurity Careers and Studies [NICCS], 2026).

Yet the question of what employers actually require of entry-level cybersecurity analysts, as opposed to what even more recent aspirational frameworks (Evans-Uzosike et al., 2025; McGuan et al., 2025; Rahman,

2025; Tessema, 2025) describe still remains under-examined in the peer-reviewed literature. However, it should be noted the speed of the labor market is not always in pace with literature.

Online job postings have emerged as a useful, yet imperfect, instrument for answering this question (Ozyurt & Ayaz, 2024). Postings reflect the language hiring managers and recruiters use at the moment of acquisition, offer near-real-time visibility into labor demand, and lend themselves to systematic textual analysis at scale. They are, however, a noisy signal: postings vary widely in length, completeness, and rhetorical strategy; aggregator sites duplicate listings; and the visible requirements may understate the tacit expectations applied at later stages of the hiring funnel.

This study contributes to the labor-market signaling literature by reporting a descriptive content analysis of 369 cybersecurity analyst postings drawn from PostJobFree.com and analyzed in May 2026. PostJobFree is an aggregator that pulls from a wide range of employers and recruiting agencies, giving the corpus broader coverage than a single company's career page (PostJobFree, n.d.). We document the prevalence of specific tools, certifications, compliance frameworks, security domains, and soft skills, alongside education, experience, salary, and geographic patterns. The intent is not to establish causal relationships but to map the surface of an active labor market in a form that curriculum designers, career advisors, and prospective analysts can interrogate.

Three research questions guide the analysis:

- **RQ1.** Which technical tools, certifications, and compliance frameworks appear most frequently in cybersecurity analyst postings?
- **RQ2.** How do security-domain emphases and soft-skill expectations distribute across the corpus?
- **RQ3.** What can the corpus reveal about education, experience, compensation, and geographic distribution at this point in the market?

Background and Related Work

Job-posting analysis has a long lineage transforming job-posting into labor market intelligence, more recently, in education research and specifically in the current application of computing and cybersecurity (Aken et al., 2009; Romanko & O'Mahony, 2022; Ozyurt & Ayaz, 2024). Studies in fields such as data science, information systems, and software engineering have used postings to characterize skill bundles, contrasting academic curricula against industry demand, and tracing the diffusion of new tools and methodologies. In cybersecurity specifically, prior research has emphasized the gap between framework-level competency descriptions (e.g., NICE work roles) and the granular tooling and certification language found in postings (National Initiative for Cybersecurity Education NICE 2020 and 2026). Graham and Lu (2023) provided semantic network analysis of job advertisements to establish skills expectations in cybersecurity. Their study sought to answer two research questions: what are the most critical soft skills cybersecurity employers seek? And how are the soft skills related to the hard skills based on industry expectations?

Graham and Lu (2023) found three categories of soft skills emerged: Knowledge management and systems, big data analytical skills, and teamwork and diversity are all highly sought further the reinforce a critical role information systems is playing in cyber security. However, their conceptual model did not provide the statistical analysis in this current work. Khaouja et al. (2021) conducted a systematic review of the literature review current on skill identification from job ads their finding of relevance to this study determined the authors argued that if a skill is required by many job ads having the same job title, it is likely to be an important skill. Ramezan et al. (2026) suggest the integration of textual analysis of job advertisements with

qualitative data such as interviews, questionnaires, or surveys of current cybersecurity analysts and hiring managers could provide richer, context-aware insights into how cybersecurity analyst roles differ across industries and evolve over time.

Three threads in the existing literature motivate the present analysis. First, work on credential signaling has documented that certifications often function as gatekeeping devices distinct from the underlying competencies they nominally attest to; CISSP in particular has been the subject of recurring debate about its appropriateness as a screening filter for early-career roles. Second, studies of compliance regimes including NIST 800-53, RMF, and DoD/DISA STIGs have observed that public-sector and defense-contracting employers exert a disproportionate influence on the language of postings, particularly in the United States (National Institute of Standards and Technology [NIST], 2020). Third, research on remote work since the 2020-2022 period has tracked the persistence of distributed-work norms in technical occupations, raising questions about the geography of cybersecurity hiring. Against this backdrop, the present study makes no claim to causal inference. Rather, it offers a structured, replicable snapshot of one segment of the cybersecurity analyst posting environment in mid-2026, designed to be interpreted alongside the larger and more methodologically diverse literature.

Methods

Data Source and Collection

The corpus comprises 369 cleaned cybersecurity analyst job postings scraped from PostJobFree.com during May 2026. PostJobFree is a U.S.-based job aggregator that ingests listings from corporate career pages, staffing agencies, and other sources, making it a broad rather than employer-specific sampling frame (PostJobFree, n.d.). PostJobFree.com was used as the source of the job postings because their terms of service do not disallow web scraping. Other sources such as Indeed or ZipRecruiter explicitly prohibit web scraping per their terms of service. Postings were collected through automated scraping followed by deduplication and minimal text normalization. Listings with fewer than 50 words of substantive description were excluded as uninformative; the resulting minimum posting length in the analyzed corpus was 57 words.

Coding Taxonomy

A structured taxonomy was developed prior to analysis, drawing on the NICE Cybersecurity Workforce Framework, the European ESCO classification, and prior published job-posting studies. The taxonomy spans seven dimensions (European Skills, Competences, Qualifications and Occupations [ESCO], n.d.)

- Technical tools and platforms (e.g., SIEM products, cloud providers, scripting languages, EDR/XDR);
- Professional certifications (CISSP, Security+, CEH, CISM, OSCP, vendor and SANS credentials);
- Compliance frameworks (NIST, RMF, DoD/DISA, ISO 27001, HIPAA, PCI DSS, CMMC);
- Security domain focus (threat intelligence, incident response, GRC, vulnerability management, IAM, penetration testing, network security, cloud security, DFIR, AppSec);
- Soft skills and competencies (analytical, communication, leadership, documentation, problem-solving);
- Education, experience, and salary signals; and
- Geographic and work-arrangement signals (city/state mentions, remote/hybrid/on-site, security clearance language).

Analytic Procedure

Each posting was processed through case-insensitive keyword and regular-expression matching against the taxonomy, with curated alias lists to consolidate variant spellings (for example, "AWS" with "Amazon Web Services"; "IDS/IPS" with "intrusion detection" and "intrusion prevention"). Co-occurrences are reported as percentages of N = 369 postings. Because postings can mention multiple items in a single category, percentages within a category do not sum to 100. Salary statistics were computed on the subset of 46 postings (12.5%) that disclosed compensation, after parsing ranges to midpoints and excluding hourly figures that could not be reliably annualized. Geographic location was extracted by pattern-matching U.S. state names and abbreviations in the description text; only 46 postings (12.5%) yielded an identifiable location, in part because the majority were marketed as remote without a state anchor. All data are derived from publicly accessible job postings. No personally identifiable information about candidates was collected. The coded dataset and aggregation scripts are available from the author on request.

Results

Corpus Characteristics

Postings in the corpus vary dramatically in length. Mean word count is 238, but the distribution is heavily right-skewed: the median is just 75 words, the standard deviation is 320, the maximum reaches 1,942 words, and 72% of postings (266 of 369) contain fewer than 100 words. This pattern, summarized in Table 1, has interpretive consequences: most postings are essentially headline-level descriptions with limited specificity about required skills, while a smaller tail of long, well-specified postings does much of the work of populating the frequency counts reported below.

Table 1. Dataset Overview (N = 369)

Metric	Value
Total postings	369
Mean word count	238
Median word count	75
Standard deviation of word count	320
Minimum word count	57
Maximum word count	1,942
Postings under 100 words	266 (72.1%)
Postings 100–499 words	31 (8.4%)
Postings 500–999 words	59 (16.0%)
Postings 1,000+ words	13 (3.5%)

Three structural features are identified before turning to the substantive content of the postings. First, the work-arrangement signal is overwhelmingly remote. Of the 369 postings, 290 (78.6%) explicitly advertise remote work, compared with only 13 hybrid postings (3.5%) and 21 on-site postings (5.7%); the remaining 45 postings (12.2%) do not specify an arrangement. This pattern suggests that the visible market segment

represented in this corpus is strongly oriented toward distributed cybersecurity work. For prospective analysts, this may indicate that employers view many monitoring, analysis, compliance, vulnerability-management, and threat-intelligence responsibilities as work that can be performed effectively without a permanent physical presence. At the same time, this result should not be interpreted as evidence that nearly four out of five cybersecurity analyst jobs in the broader labor market are remote. The unusually high remote share may reflect the practices of the particular job-posting aggregator, the tendency of remote positions to be reposted across multiple locations, or the relative visibility of staffing-agency and contract positions in the sample.

Second, the corpus skews sharply toward entry- and junior-level roles. A total of 244 postings (66.1%) were coded at that seniority level, compared with 25 senior postings (6.8%) and only 2 manager/director postings (0.5%). An additional 91 postings (24.7%) did not provide an explicit seniority label. On its face, this distribution suggests a labor market in which employers are actively advertising junior analyst roles, particularly those associated with security operations, monitoring, compliance support, and threat analysis. However, the label "entry-level" should be interpreted cautiously. Elsewhere in the corpus, many postings still request a bachelor's degree, one or more certifications, and prior experience, with a two-year requirement appearing frequently. Thus, "entry" or "junior" may often mean early-career rather than no-experience. The gap between entry-level labels and experience expectations may be especially important for curriculum designers and career-services professionals, who should prepare students not only with foundational technical skills but also with portfolios, internships, projects, certifications, and other evidence of practical readiness.

Third, security-clearance language is relatively limited but still meaningful. Thirty-six postings (9.8%) mention some form of clearance, including Secret clearance in 18 postings (4.9%), Top Secret clearance in 9 postings (2.4%), and TS/SCI clearance in 7 postings (1.9%). In addition, 30 postings (8.1%) reference Department of Defense work more broadly. Although these percentages are much smaller than the remote-work or entry-level shares, they indicate that a visible segment of the analyst market is connected to federal, defense, intelligence, or defense-contracting environments. These roles may carry distinctive requirements beyond general cybersecurity knowledge, such as familiarity with NIST controls, the Risk Management Framework, DoD/DISA guidance, controlled-information handling, and eligibility for or possession of a security clearance. The presence of these postings may also help explain the strong representation of defense-oriented compliance language elsewhere in the results. Still, because the sample comes from one aggregator and contains relatively limited geographic information, the findings should be understood as evidence of a defense-adjacent segment within this corpus rather than as a precise estimate of the national cybersecurity labor market.

Table 2. Work Arrangement, Seniority, and Clearance Signals

Category	Indicator	Count	% of N
Work arrangement	Remote	290	78.6%
	Hybrid	13	3.5%
	On-site	21	5.7%
Seniority	Entry / Junior	244	66.1%
	Mid-Level	7	1.9%
	Senior	25	6.8%

Category	Indicator	Count	% of N
	Manager / Director	2	0.5%
	Unspecified	91	24.7%
Security clearance	Any clearance mentioned	36	9.8%
	Secret	18	4.9%
	Top Secret (TS)	9	2.4%
	TS/SCI	7	1.9%
	DoD-related	30	8.1%

Technical Tools and Platforms

Table 3 lists every technical tool or platform appearing in at least 1% of postings. The leading items reflect a recognizable cluster of contemporary analyst tooling: generic cloud language leads at 9.5%, followed by SIEM at 7.9%, threat-intelligence platforms at 7.3%, and AWS at 7.0%. Below that, the long tail flattens quickly: identity and access management (IAM) at 4.6%, EDR and IDS/IPS each at 3.8%, and Splunk at 3.5% are the only named products to reach the 3% threshold. Scripting languages: Python at 3.0% and PowerShell at 2.2% appear less prominently than is sometimes assumed in curriculum debates.

Two observations about this distribution require cautious consideration. First, absolute frequencies are modest: even the leading skill is named in fewer than one posting in ten, a consequence of the corpus's prevalence of short, generic descriptions. Second, the ordering is broadly consistent with a SOC-analyst archetype (cloud, SIEM, threat intel, EDR, IAM, scripting) rather than a specialist red-team or DFIR archetype.

Table 3. Technical Tools and Platforms (≥1% of Postings)

Tool / Platform	Count	% of Postings
Cloud (general)	35	9.5%
SIEM (general)	29	7.9%
Threat Intelligence	27	7.3%
AWS	26	7.0%
Firewall	20	5.4%
IAM	17	4.6%
EDR (general)	14	3.8%
IDS/IPS	14	3.8%
Splunk	13	3.5%
Python	11	3.0%
Azure	10	2.7%

Tool / Platform	Count	% of Postings
Malware Analysis	9	2.4%
Active Directory	9	2.4%
PowerShell	8	2.2%
Microsoft Sentinel	7	1.9%
GCP	7	1.9%
SQL	7	1.9%
CrowdStrike	6	1.6%
CI/CD	6	1.6%
Elastic/ELK	5	1.4%
XDR (general)	5	1.4%
MITRE ATT&CK	5	1.4%
Zero Trust	5	1.4%
QRadar	4	1.1%
VPN	4	1.1%

Certifications

Certifications are the single most concentrated category in the corpus. CISSP leads at 10.3% of postings, followed by CompTIA Security+ at 7.0%, CEH at 5.1%, and CISM at 4.9%; the broader "any CompTIA" category reaches 4.3%. Hands-on credentials such as OSCP appear in 2.7% of postings, and the GIAC family (GCIH, GCIA, GSEC) collectively in roughly 7.4%, suggesting a meaningful but not dominant role for SANS-aligned credentials. The full distribution appears in Table 4.

The visible hierarchy placing CISSP at the top of an entry-level corpus is notable. CISSP requires five years of paid full-time security experience for full certification, so its appearance in postings dominated by entry- and junior-level seniority labels likely reflects either screening language inherited from senior templates, signaling about long-term career trajectory, or hiring manager use of CISSP as a generic synonym for "security knowledge."

Table 4. Certifications Mentioned

Certification	Count	% of Postings
CISSP	38	10.3%
Security+	26	7.0%
CEH	19	5.1%
CISM	18	4.9%
CompTIA (any)	16	4.3%

Certification	Count	% of Postings
CISA	15	4.1%
GCIH	13	3.5%
GCIA	12	3.3%
OSCP	10	2.7%
GSEC	7	1.9%
CRISC	7	1.9%
CCSP	6	1.6%
CCNA	6	1.6%
SSCP	6	1.6%
SANS (any)	4	1.1%

Compliance Frameworks

Compliance language tilts heavily toward defense-adjacent regimes. DoD/DISA references appear in 20.1% of postings, the highest single-item frequency in any non-domain category and NIST in 16.5%. RMF (Risk Management Framework) follows at 6.2%. Civilian and commercial frameworks appear far less often: ISO 27001 in 2.7%, CMMC in 2.2%, HIPAA in 1.9%, CIS Controls in 1.4%, and PCI DSS, FedRAMP, SOX, and GDPR each in 1% or below. The concentration of defense-related compliance signals coheres with the geographic pattern reported in Section 4.7, where Washington, DC and Virginia account for a substantial share of the postings that disclose a location.

Table 5. Compliance Frameworks Mentioned

Framework	Count	% of Postings
DoD / DISA	74	20.1%
NIST	61	16.5%
RMF	23	6.2%
ISO 27001	10	2.7%
CMMC	8	2.2%
HIPAA	7	1.9%
CIS Controls	5	1.4%
PCI DSS	2	0.5%
FedRAMP	2	0.5%
SOX	1	0.3%
GDPR	1	0.3%

Security Domain Focus

Domain-level coding produces a quite different (and substantially denser) picture than tool-level coding, because domain language tolerates synonyms and paraphrase. Threat intelligence emerges as the most-mentioned domain at 42.5% of postings, followed by incident response/SOC at 30.6% and compliance/GRC at 29.8%. Vulnerability management (22.2%) and identity and access management (18.4%) form a clear second tier, with penetration testing (14.9%), network security (13.8%), cloud security (10.0%), forensics/DFIR (6.0%), and application security (4.9%) trailing. The pattern is consistent with employer demand for blue-team (and governance-oriented analysts rather than offensive specialists, although the substantial penetration-testing share suggests an active secondary market for red-team-adjacent skills (Blue Team Glossary, n.d.)

Table 6. Security Domain Focus

Domain	Count	% of Postings
Threat Intelligence	157	42.5%
Incident Response / SOC	113	30.6%
Compliance / GRC	110	29.8%
Vulnerability Management	82	22.2%
Identity & Access Management	68	18.4%
Penetration Testing	55	14.9%
Network Security	51	13.8%
Cloud Security	37	10.0%
Forensics / DFIR	22	6.0%
Application Security	18	4.9%

Soft Skills and Competencies

Soft-skill coding produced a long, exponentially decaying distribution. "Analytical skills" dominates at 50.4% of postings a higher frequency than any technical item followed at considerable distance by communication (17.3%), documentation (13.8%), and leadership (11.7%). Problem-solving (8.7%) and written communication (8.1%) follow. Below that, attention to detail, verbal communication, and mentoring all appear in roughly 4-5% of postings. Project management, critical thinking, and interpersonal skills round out the visible tail.

The prominence of analytical skills relative to any specific tool is consistent with prior cybersecurity workforce research suggesting that employers prize transferable cognitive capacities at least as highly as tool-specific competence. From a curriculum-design perspective, this reinforces a long-standing argument for analytical and writing-intensive components even in technical security programs.

Table 7. Soft Skills and Competencies

Soft Skill	Count	% of Postings
Analytical skills	186	50.4%
Communication	64	17.3%
Documentation	51	13.8%
Leadership	43	11.7%
Problem-solving	32	8.7%
Written communication	30	8.1%
Collaboration	23	6.2%
Attention to detail	19	5.1%
Verbal communication	18	4.9%
Mentoring	17	4.6%
Project management	10	2.7%
Critical thinking	7	1.9%
Interpersonal skills	5	1.4%

Education, Experience, and Compensation

Education signals show a clear two-track structure, split between bachelor's required, and bachelor's preferred. A bachelor's degree is explicitly required in 47.4% of postings and explicitly preferred (but not required) in an additional 32.0%, while master's degrees are required in only 3.3%.

Table 8. Education and Experience Requirements

Requirement	Count	% of Postings
Bachelor's degree required	175	47.4%
Bachelor's degree preferred (not required)	118	32.0%
Master's degree required	12	3.3%

Field-of-study language, where present, names cybersecurity in 99.7% of postings (as expected), with information security (11.4%), computer science (10.8%), information technology (10.6%), and engineering (9.5%) appearing as recognized adjacent fields.

Table 9. Field of Study

Field of Study	Count	% of Postings
Cybersecurity	368	99.7%
Information Security	42	11.4%

Field of Study	Count	% of Postings
Computer Science	40	10.8%
Information Technology	39	10.6%
Engineering	35	9.5%

Years-of-experience signals are bimodal: a 2-year minimum is by far the most common (36.0%), with a smaller cluster at 5 years (9.2%) and a thin tail extending to 10+ years (3.0%).

Table 10. Years of Experience

Years of Experience	Count	% of Postings
1 year	7	1.9%
2 years	133	36.0%
3 years	15	4.1%
5 years	34	9.2%
7 years	7	1.9%
10 years	11	3.0%

Compensation disclosure is sparse: only 46 of 369 postings (12.5%) include a salary figure that can be reliably annualized. Among these postings, the mean annual salary is $104,673, while the median is $88,186. The higher mean relative to the median indicates that a smaller number of relatively high-paying postings raise the overall average. Salaries vary substantially, with a standard deviation of $33,555 and a reported range from $49,500 to $238,200. Because postings that disclose salary may differ systematically from those that do not - for example, because of pay-transparency requirements in particular states - these results should be interpreted as describing only the 46 postings with disclosed salary information, not the full corpus of 369 postings.

Table 11. Salary Statistics (n = 46 postings with salary data)

Metric	Value
Postings with salary data	46 (12.5% of N)
Mean annual salary	$104,673
Median annual salary	$88,186
Standard deviation	$33,555
Minimum	$49,500
Maximum	$238,200

Geographic data are even more constrained. Only 46 postings (12.5%) yielded an identifiable U.S. state, reflecting both the high prevalence of remote-only listings and the brevity of many postings. Within that

subset, Washington, DC and California each account for 13.0% of located postings, followed by Virginia (10.9%), Texas and Alabama (8.7% each), and Illinois (6.5%). The combined DC-Virginia share underlines the defense-contracting tilt already visible in the compliance-framework distribution; Alabama's appearance is consistent with Huntsville's defense-and-aerospace cluster.

Table 12. Top States Among Located Postings (n = 46)

State	Count	% of Located
Washington, DC	6	13.0%
California	6	13.0%
Virginia	5	10.9%
Texas	4	8.7%
Alabama	4	8.7%
Illinois	3	6.5%
Colorado	2	4.3%
Georgia	2	4.3%
Pennsylvania	2	4.3%
Utah	2	4.3%

Discussion

Read across categories, the corpus paints a coherent portrait of an entry-level cybersecurity analyst labor market dominated by remote work, anchored in blue-team operations, and rhetorically anchored in defense-adjacent compliance. Three findings deserve particular emphasis.

The Centrality of Analytical Skills and the Brevity Problem

That "analytical skills" appears in 50.4% of postings more than four times the frequency of the most-cited technical tool is not, on its own, a novel finding; analyst job titles by definition foreground analysis. What is striking is the gap between this single soft-skill mention and the granularity of the technical landscape below it. The pattern is partly an artifact of corpus brevity: when 72% of postings are shorter than 100 words, generic skill language displaces specific tooling. For curriculum designers, the lesson is not that tools do not matter, but that postings under-signal them and that direct conversations with hiring managers, supplemented by alumni surveys and capstone-project sponsors, will likely produce a more reliable picture of demanded tooling than postings alone.

The CISSP Paradox in an Entry-Level Corpus

CISSP appears in 10.3% of postings, but 66.1% of postings carry entry- or junior-level labels. Because full CISSP certification requires five years of cumulative paid experience in two of the credential's eight domains, the prevalence of CISSP in an entry-skewed corpus is postulated to reflect employer signaling about preferred long-run development, or imprecise use of CISSP as shorthand for "a serious security person." The pedagogically actionable response is twofold: programs should help students understand the

realistic timeline for CISSP eligibility, and they should ensure that the Security+ credential second in the corpus at 7.0% is well-supported as a more realistic entry-level target.

Defense-Adjacent Compliance as a Geographic Story
The 20.1% prevalence of DoD/DISA language and the concentration of located postings in DC, Virginia, and Alabama suggest that defense contracting exerts a meaningful gravitational pull on the public-facing cybersecurity analyst posting environment. Programs whose graduates are geographically mobile may benefit from explicit exposure to NIST 800-53, RMF, and the basics of DoD security control inheritance; programs anchored in non-defense regional economies may reasonably weight commercial frameworks (ISO 27001, PCI DSS, HIPAA, SOC 2) more heavily, even though those frameworks appear less frequently in this particular corpus (NICE 2020 and 2026; NIST 2020).

Implications for Curriculum Design
Synthesizing across results, three curriculum-design implications are visible. First, the SOC-analyst archetype cloud, SIEM, threat intelligence, EDR, IAM, scripting is the most defensible "core" technical skill bundle for an entry-level cybersecurity analyst track. Second, certification preparation should be calibrated to realistic eligibility: Security+ as a near-term anchor, with CISSP positioned as a five-year career goal rather than a graduation requirement. CISSP certification is designed for long-term practitioners and unable to be obtained without multi-years of high-level experience (CISSP certified). Third, communication and writing instruction captured here through the combined 17.3% communication, 13.8% documentation, and 8.1% written communication shares should be treated as core technical infrastructure rather than as ancillary general-education content.

Limitations

The corpus is a single-source convenience sample from PostJobFree.com and is not representative of the cybersecurity analyst labor market as a whole. Three boundary conditions deserve emphasis. First, brevity: with a median of 75 words and 72% of postings under 100 words, the corpus systematically under-represents tools and frameworks that hiring managers consider important but do not write down. Frequency counts should therefore be read as lower bounds, not point estimates of true demand. Second, source selection: PostJobFree, a free-posting aggregator that may attract different employer mixes than premium platforms such as LinkedIn or Indeed; defense-contracting and staffing-agency postings appear to be over-represented. Third, disclosure bias: salary data are present in only 12.5% of postings and geographic data in only 12.5%, both subject to systematic non-disclosure shaped by state-level pay-transparency laws and the rise of remote-only listings. The compensation and geographic findings are best treated as descriptive of the disclosed subset only. A full manual validation and required/preferred re-coding were not feasible at this stage of research and is a limitation of the study,

Although the analysis relies on text matching, it is not intended as a simple word-count exercise. Each posting was mapped to a structured, theory-informed taxonomy derived from the NICE Workforce Framework, ESCO classifications, and prior job-posting research. Curated aliases and concept groupings were used to consolidate variant language into analytically meaningful categories, allowing the analysis to examine patterns in employer signals across tools, credentials, compliance regimes, security domains, and workforce characteristics.

Additional analytic limitations should be noted. Keyword-and-alias coding cannot fully capture compositional context ("experience with Splunk preferred" vs. "Splunk experience required" are treated identically). The taxonomy, while developed against established frameworks, embeds the author's

judgments about category boundaries; alternative taxonomies for example, NICE work-role mappings would produce different aggregate counts. Finally, the analysis is descriptive: no inferential tests are reported, and no causal claims are made about the relationship between posting language and downstream hiring or compensation outcomes.

Conclusion and Future Work

This study has documented the surface features of one slice of the cybersecurity analyst labor market in mid-2026: a remote-heavy, entry-skewed posting environment in which analytical skills, cloud and SIEM tooling, CISSP and Security+ credentials, defense-adjacent compliance language, and threat-intelligence and SOC-domain emphases dominate. The findings are descriptive and bounded, but they offer a structured baseline against which curriculum designers, career-services professionals, and students can interpret aspirational competency frameworks.

Three extensions of this work suggest themselves. First, a longitudinal repeat of the same coding pipeline across multiple quarters would convert the current snapshot into a time series capable of detecting shifts in tooling, certification prevalence, and remote-work norms. Second, comparison across aggregator platforms for example, PostJobFree, Indeed, LinkedIn, and ClearanceJobs would quantify the source-selection bias identified above. Third, integration with the NICE Workforce Framework and the European ESCO classification would allow direct comparison between aspirational competency standards and observed posting language, contributing to ongoing debates about framework-curriculum-employer alignment. Further, the findings of Ramezan et al. (2026) who suggest the integration of textual analysis of job advertisements with qualitative data such as interviews, questionnaires, or surveys of current cybersecurity analysts and hiring managers could provide richer, context-aware insights into how cybersecurity analyst roles differ across industries and evolve over time should also be a pursuit of further research.

Acknowledgements

AI Use Declaration: During the preparation of this work the author(s) used Anthropic Claude in order to assist in statistics, graphics development, and content review. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the published article.

References

Anderson Sr, K. E. (2025). *The Cybersecurity Workforce and Skills Shortages: Origins, Responses, and Future Strategic Solutions* (Doctoral dissertation, Marymount University).

Aken, A., Litecky, C., Ahmad, A., and Nelson, J. (2009). Mining for computing jobs. IEEE Software 27 (1):78–85. https://doi.org/10.1109/MS.2009.150.

Anieto, N. (2026). Developing a Structured Entry Pathway into Cybersecurity: Certification Mapping, Skill Development, and Workforce Alignment. *Skill Development, and Workforce Alignment (March 30, 2026)*.

Blue Team - Glossary | CSRC. (n.d.). https://csrc.nist.gov/glossary/term/blue_team

CISSP Certified Information Systems Security Professional | ISC2. (n.d.-c). https://www.isc2.org/Certifications/CISSP

European Skills, Competences, Qualifications and Occupations (ESCO). (n.d.). Classification of skills and occupations. European Commission.

Evans-Uzosike, I. O., Okatta, C. G., Otokiti, B. O., Ejike, O. G., & Kufile, O. T. (2025). Closing the Cybersecurity Talent Gap: A Strategic Workforce Readiness Framework. *World Journal of Innovation and Modern Technology*, *9*(6), 230-241. https://doi.org/10.56201/wjimt.v9.no6.2025.pg230.241.

Graham, C. M., & Lu, Y. (2023). Skills expectations in cybersecurity: semantic network analysis of job advertisements. *Journal of Computer Information Systems*, *63*(4), 937-949. https://doi.org/10.1080/08874417.2022.2115954.

Khaouja, I., Kassou, I., & Ghogho, M. (2021). A survey on skill identification from online job ads. *IEEE Access*, *9*, 118134-118153. https://doi.org/10.1109/ACCESS.2021.3106120.

McGuan, C., Vijaya Raghavan, A., Mandapati, K. M., Yu, C., Ray, B. E., Jackson, D. K., & Kumar, S. (2025). Bridging Cybersecurity Practice and Law: A Hands-On, Scenario-Based Curriculum Using the NICE Framework to Foster Skill Development. *Journal of Cybersecurity and Privacy*, *5*(4), 106. https://doi.org/10.3390/jcp5040106.

National Initiative for Cybersecurity Education (NICE). (2020). Workforce Framework for Cybersecurity (NIST SP 800-181 Rev. 1). National Institute of Standards and Technology. https://www.nist.gov/itl/applied-cybersecurity/nice.

National Institute of Standards and Technology. (2020). Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5). https://doi.org/10.6028/NIST.SP.800-53r5.

Nice Workforce Framework for cybersecurity (NICE framework) | NICCS. National Initiative for Cybersecurity Careers and Studies. (2026, April 16). https://niccs.cisa.gov/tools/nice-framework

Office of the Under Secretary of Defense for Acquisition and Sustainment. (2021). Cybersecurity Maturity Model Certification (CMMC) Model. https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview_V2.0_FINAL2_20211202_508.pdf.

Ozyurt, O., & Ayaz, A. (2024). Identifying cyber security competencies and skills from online job advertisements through topic modeling. *Security Journal*, *37*(4), 1339-1359. https://doi.org/10.1057/s41284-024-00420-w.

PostJobFree. (n.d.). PostJobFree. https://www.postjobfree.com/

Rahman, M. S., Chavarria, J., Shah, D., & Rashid, M. (2025). Strengthening Cybersecurity Education: Analyzing Curriculum Alignment with NICE Workforce Framework. https://aisel.aisnet.org/amcis2025/is_education/is_education/21/.

Ramezan, C. A., Ahmad, M. J., Schaupp, L. C., Hatten, F. W., & Starling, M. A. (2026). The Modern Cybersecurity Analyst: An International Position Analysis. *Computers & Security*, 104825. https://doi.org/10.1016/j.cose.2026.104825.

Romanko, O., & O'Mahony, M. (2022). The use of online job sites for measuring skills and labour market trends: A review. *Economic Statistics Centre of Excellence (ESCoE) Technical Reports*, (ESCOE-TR-19).

Tessema, T. (2025). *A Competency Based Approach for Minimizing the Shortage of Cyberskills* (Doctoral dissertation, Marymount University).

Appendix A. Coding Taxonomy Categories

The full coding taxonomy comprises seven top-level categories. Each item listed below was assigned one or more textual aliases against which posting text was matched.

Category	Representative Items
Technical Tools & Platforms	Cloud platforms (AWS, Azure, GCP), SIEM products (Splunk, Sentinel, QRadar, Elastic), EDR/XDR (CrowdStrike, generic), scripting (Python, PowerShell, Bash), network (Firewall, IDS/IPS, VPN), scanners (Nessus, Qualys), MITRE ATT&CK, Zero Trust
Certifications	CISSP, Security+, CEH, CISM, CISA, CRISC, CCSP, CCNA, SSCP, OSCP, CompTIA family, GIAC family (GCIH, GCIA, GSEC), SANS-aligned credentials
Compliance Frameworks	DoD/DISA, NIST, RMF, ISO 27001, CMMC, HIPAA, CIS Controls, PCI DSS, FedRAMP, SOX, GDPR
Security Domain Focus	Threat Intelligence, Incident Response/SOC, Compliance/GRC, Vulnerability Management, IAM, Penetration Testing, Network Security, Cloud Security, Forensics/DFIR, Application Security
Soft Skills	Analytical skills, communication (verbal/written), documentation, leadership, problem-solving, attention to detail, collaboration, mentoring, project management, critical thinking, interpersonal skills
Education & Experience	Bachelor's/Master's required vs. preferred, field of study (Cybersecurity, Information Security, Computer Science, Information Technology, Engineering), years of experience (1–10+)
Geographic & Work Arrangement	U.S. states and abbreviations, Washington DC, remote/hybrid/on-site language, security clearance levels (Secret, Top Secret, TS/SCI), DoD references