

Job Analysis in Cybersecurity

My Nguyen

Old Dominion University

IDS 493 – Electronic Portfolio Project

Professor Phan

July 13, 2025

Job Analysis in Cybersecurity

Abstract

This essay analyzes a SOC Analyst Level 1 job at Competitive Range Solutions, LLC. It outlines the company's mission and the job's duties, including monitoring, alert investigation, and reporting (Competitive Range Solutions, LLC, 2025). It then details required skills—network security basics, SIEM use, and incident response—as stated in the ad (Ullah et al., 2025). Next, it “reads between the lines” to infer teamwork, time management, and adaptability traits from the ad's phrasing (Competitive Range Solutions, LLC, 2025). The paper links these needs to courses, SOC labs, and CompTIA Security+ certification (CompTIA, 2025). Industry data show a 5.5 million workforce in 2023 with 440,000 vacant roles (ISC², 2023) and a slowed growth rate in 2024 (ISC², 2024). A literature review highlights broader career requirements (Shah et al., 2022). A human–AI collaboration study shows future SOCs using AI for alert triage (Sarker et al., 2025). Finally, a report notes hiring slowdowns amid budget cuts, raising concerns for job seekers (Axios Codebook, 2024). Detailed ad review helps students tailor their academic paths and hands-on experiences to meet real SOC demands.

Introduction

A job analysis lists a role's tasks, responsibilities, and skills (Turner & Haddow, 2023). In cybersecurity, job ads guide students in shaping relevant training (ISC², 2023). This paper examines a SOC Analyst Level 1 posting from Competitive Range Solutions, LLC. It covers company context, core duties, explicit and implied skills, academic alignment, and industry trends. The thesis is that a close job-ad study lets students map coursework and labs to real SOC needs (ISC², 2024).

Company & Position Overview

Competitive Range Solutions, LLC helps the Department of Defense deploy mission-critical IT and security tools (Competitive Range Solutions, LLC, 2025). The SOC Analyst Level 1 role watches network logs, investigates potential threats, and reports events in near real time (Competitive Range Solutions, LLC, 2025). The "entry-level" label means strong academic work and some field exposure suit candidates (Competitive Range Solutions, LLC, 2025). The job requires quick mastery of DoD security frameworks like RMF (ISC², 2024).

Core Responsibilities

- **Continuous Monitoring:** Watch SIEM and IDS logs for anomalies (Competitive Range Solutions, LLC, 2025).
- **Alert Investigation:** "Investigate, analyze, and escalate security alerts" per SLAs (Competitive Range Solutions, LLC, 2025).
- **Threat Support:** Assist triage and mitigation steps (Competitive Range Solutions, LLC, 2025).
- **Collaboration:** Join SOC working groups to share insights (Competitive Range Solutions, LLC, 2025).
- **Compliance & Reporting:** Track incident steps and DoD standards (Competitive Range Solutions, LLC, 2025).

- Vulnerability Awareness: Stay updated on new threats and defenses (Competitive Range Solutions, LLC, 2025).

Stated Skills & Traits

- Network Security Basics: Firewalls, IDS, and vulnerability scans (Ullah et al., 2025).
- SIEM Proficiency: Use of Splunk, QRadar, or similar tools (Ullah et al., 2025).
- Incident Response: Knowledge of investigative workflows and escalation (Ullah et al., 2025).
- Communication: Clear report writing for technical and non-technical audiences (Ullah et al., 2025).
- Project Management: Plan tasks and meet SLAs on time (Ullah et al., 2025).

Implied Traits

- Teamwork: SOC working groups imply collaboration skills (Competitive Range Solutions, LLC, 2025).
- Time Management: “Timely escalation” demands discipline under pressure (Competitive Range Solutions, LLC, 2025).
- Adaptability: “Develop specialized knowledge” suggests quick learning (Competitive Range Solutions, LLC, 2025).
- Resilience: Fast alert rates require stress management (Shah et al., 2022).

Linking Academics & Practice

- Network Security Course: Taught TCP/IP and firewall setup, matching ad basics (CompTIA, 2025).
- SOC Lab Exercises: Students parse logs and use SIEM, mirroring “investigate alerts” duties (CompTIA, 2025).

- Security+ Certification: Validates CIA principles and report writing (CompTIA, 2025)
- Internships: Campus SOC internships hone real-world report writing and protocol use (Competitive Range Solutions, LLC, 2025).

Reading Between the Lines

The ad's focus on "SLAs" shows accountability and time focus (Competitive Range Solutions, LLC, 2025). Repeated "collaborative environment" calls point to strong teamwork (Competitive Range Solutions, LLC, 2025). "Mission-essential" suggests a culture of precision and duty (Competitive Range Solutions, LLC, 2025). Stress and burnout risk appear from high alert volumes (Shah et al., 2022).

Industry Trends & Workforce Gap

The global cyber workforce reached 5.5 million in 2023 but lagged by 440,000 roles (ISC², 2023). In 2024, growth slowed amid budget cuts and hiring freezes (ISC², 2024). Skills gaps remain in software security and compliance (Shah et al., 2022). A human-AI collaboration study shows future SOCs will use AI to boost alert triage and reduce fatigue (Sarker et al., 2025). A report notes hiring slowdowns raise longer-term concerns for new analysts (Axios Codebook, 2024).

Career Fit & Motivation

I seek to secure DoD systems, matching the ad's mission focus (Competitive Range Solutions, LLC, 2025). My network security projects taught firewall tuning and intrusion checks (CompTIA, 2025). SOC labs gave me hands-on SIEM and log analysis practice. My Security+ credential proves core cyber skills (CompTIA, 2025). Group projects and internships built my teamwork and time-management strengths (Ullah et al., 2025).

Company Culture & Values

Phrases like “collaborative, congenial environment” show team support and shared learning (Competitive Range Solutions, LLC, 2025). “Mission-essential” and “established protocols” point to a rules-based, duty-driven culture (Competitive Range Solutions, LLC, 2025). My respect for guidelines and friendly teamwork style fit this culture.

Challenges in the Role

Strict SLAs and constant alert volumes will test new analysts (Competitive Range Solutions, LLC, 2025). Fast incident handling demands clear judgment under stress (Shah et al., 2022). Yet detailed tasks and SOC support give newcomers a clear path for growth (Competitive Range Solutions, LLC, 2025).

Conclusion

A detailed job-ad review helps students align coursework and labs to real SOC demands. Hard skills in network security, SIEM use, and incident response map to classes and Security+ certification (CompTIA, 2025). Soft traits like teamwork, time management, adaptability, and stress resilience arise from stated and implied requirements (Ullah et al., 2025; Shah et al., 2022). Workforce data on gaps and hiring slowdowns highlight the need for targeted upskilling (ISC², 2023; ISC², 2024). Human–AI teaming points to future SOC workflows (Sarker et al., 2025). By linking academic work, labs, and certification to these demands, aspiring analysts build profiles that meet current SOC roles and adapt to future challenges.

References

- Arora, S., & Hastings, J. D. (2024). A survey-based quantitative analysis of stress factors and their impacts among cybersecurity professionals. arXiv.
<https://arxiv.org/abs/2409.12047>
- CompTIA. (2025). Security+ (SY0-601) certification overview. Retrieved from
<https://www.comptia.org/certifications/security/>
- Competitive Range Solutions, LLC. (2025). SOC Analyst Level 1 [Job posting].
ZipRecruiter. Retrieved July 9, 2025, from *<https://www.ziprecruiter.com/.../SOC-Analyst-Level-1>*
- International Information System Security Certification Consortium. (2023). 2023
Cybersecurity Workforce Study. ISC² Insights.
<https://www.isc2.org/Insights/2023/11/ISC2-Cybersecurity-Workforce-Study-Looking-Deeper-into-the-Workforce-Gap>
- International Information System Security Certification Consortium. (2024). 2024
Cybersecurity Workforce Study. ISC² Insights.
<https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study>
- Sarker, I. H., Suryotrisongko, H., & Camtepe, S. (2025). A unified framework for human–AI collaboration in SOC operations. arXiv. *<https://arxiv.org/abs/2505.23397>*
- Shah, M., Beck, T., & Hung, D. (2022). Cybersecurity career requirements: A literature review. *International Journal of Information Security Education*, 5(4), 77–92
- Ullah, F., Ye, X., Fatima, U., Akhtar, Z., Wu, Y., & Ahmad, H. (2025). What skills do cybersecurity professionals need? arXiv. *<https://arxiv.org/abs/2502.13658>*