Cyber Security Threat Analyst: A Reflection of Skill Expectations in the Cybersecurity Field

Anthony Gomez-Reyes

Old Dominion University

IDS 493

Dr. Phan

October 28, 2025

Abstract

This essay analyzes the Cyber Security Threat Analyst job advertisement posted by Versar Global Solutions. The ad outlines a combination of technical, analytical, and interpersonal skills that illustrate the growing complexity and interdisciplinary nature of modern cybersecurity roles. This analysis examines how the job ad reflects the professional expectations of the cybersecurity field, focusing on technical expertise, compliance awareness, communication ability, and adaptability. The discussion concludes that the ad encapsulates current trends in cybersecurity employment, emphasizing that successful candidates must demonstrate both deep technical competence and strong collaborative and communication skills.

Introduction

One of the IT industry's most dynamic and quickly changing professions is cybersecurity. Organizations in both the public and private sectors must adjust to the growing sophistication of cyber threats. The job posting form Versar Global Solutions' Cyber Security Threat Analyst position provides a thorough case study of how businesses specify and convey the competencies they look for in cybersecurity experts. The advertisement illustrates the technical and professional standards currently anticipated in the cybersecurity industry through its explanations of tasks, necessary skills, and recommended traits. In order to determine how the advertisement reflects the fundamental abilities, credentials, and professional dispositions required by the cybersecurity industry, this essay will examine it.

Role and Level within the Organization

The Cyber Security Threat Analyst role at Versar Global Solutions is presented as a high-responsibility position situated within the company’s Geospatial and Digital Solutions (GDS) Market Sector team. The job ad emphasizes leadership in “developing, implementing, and supporting cutting-edge geospatial technologies” and collaboration “to achieve specific goals and objectives.” These phrases suggest that the role is not entry-level but rather intended for professionals with substantial experience in both cybersecurity and project coordination. Reporting “directly to the Director of the Digital HUB Team” indicates that the position exists within a management-adjacent tier of the organizational structure, likely equivalent to a mid- to senior-level technical analyst. The analyst will "lead the charge" in utilizing digital tools and artificial intelligence to improve cybersecurity operations, according to the description. The assumption that this position requires more work experience than just academic preparation is strengthened by the leadership-oriented wording and the prerequisites for certifications like CISSP and CISM. In addition to technical expertise, a candidate for this role must exhibit the ability to lead teams and collaborate across departments which are qualities that are usually acquired via work experience rather than classroom instruction.

Skills, Experience, Qualifications, and Training

Versar Global Solutions structures its job advertisement to highlight technical expertise and certification before soft skills, signaling that technical capability forms the foundation of eligibility. The position requires at least “three years of experience in threat modeling, vulnerability assessments, and protocol validation for large systems.” Furthermore, it lists preferred credentials including “CISSP, CISM, [and] CEH,” all of which are industry-recognized certifications validating a candidate’s mastery of security frameworks, risk management, and ethical hacking practices. The company's emphasis on cloud computing and identity management systems is reflected in the technical capabilities that are highlighted, such as "API security, OAuth/SAML, tenant isolation, and cloud-native security." It is also necessary to understand government certification procedures, cryptographic concepts, and cybersecurity frameworks. The emphasis on practical, applied expertise and a grasp of both network security principles and compliance-driven documentation which is evident in these standards. The ad then talks about soft skills, saying that the person must have "excellent analytical and problem-solving skills" and be able to "communicate complex security concepts clearly to technical and non-technical stakeholders." This organization's emphasis on technical proficiency as the primary qualification, with communication and teamwork acting as required complements, is demonstrated by its "technical first, interpersonal second" policy.

Additional Unstated Skills and Training

Although the job posting explicitly outlines a robust technical profile, several implied competencies are also apparent. The ad’s reference to “leveraging AI solutions and digital tools to improve efficiency, scalability, and the overall digital experience” suggests that the ideal candidate should possess a foundational understanding of artificial intelligence, data analytics, and automation which are skills not directly required but essential for fulfilling the stated mission.

Fit for the Position and Academic Connections

While I am still developing the depth of expertise required for a position like this, my academic studies in cybersecurity have provided a strong starting point for building the skills Versar Global Solutions seeks. Through coursework in network security, ethical hacking, and cybersecurity fundamentals, I have gained an introductory understanding of how to identify and mitigate system vulnerabilities which are skills that relate to the ad’s emphasis on “threat modeling” and “vulnerability assessments.” My classes in cryptography and information assurance have also familiarized me with encryption protocols and data protection concepts, which connect to the company’s focus on “protocol validation” and compliance. I view this position as an opportunity to continue developing my technical knowledge while applying the foundational principles I have already learned in a real-world cybersecurity environment.

Company Culture

The job posting from Versar Global Solutions offers a number of textual hints regarding the company culture. Its Equal Employment Opportunity (EEO) statement states that it is dedicated to professional integrity, diversity, and inclusion. The phrase "committed to providing equal employment opportunities... without regard to race, color, religion, sex, national origin, age, disability, [or] sexual orientation" highlights the importance of moral behavior and respect for all workers.

Soft Skills Inferred from the Ad

While the ad explicitly mentions analytical and communication skills, it also implies several additional soft skills that are not stated outright. One such skill is time management. The preferred qualifications include “strong project management skills: ability to plan, organize, and manage multiple projects simultaneously.” This requirement indicates that the position involves juggling numerous tasks and priorities which are a hallmark of effective time management. Adaptability is another inferred soft talent. The analyst must constantly adapt to new technologies and attack vectors because the organization is looking for someone to "monitor emerging cyber threats and vulnerabilities." Although it isn't stated explicitly, adaptability is crucial because cybersecurity work is dynamic and always changing. When taken as a whole, these suggested soft skills imply that adaptability and organization are just as important for success in this position as technical proficiency.

Challenges and Overall Tone

The wording of the advertisement portrays the role as both challenging and inspiring. The analyst must “perform comprehensive threat modeling,” “lead efforts for government and industry security certifications,” and “assist in designing and maintaining incident response plans.” These tasks require technical depth, strategic judgment, and continuous vigilance and is a indication that the job will be demanding. But the advertisement also has a positive tone. A sense of purpose and goal is evoked by phrases like "join us as a Cyber Security Threat Analyst and lead the charge" and "make a difference in the world." This rhetoric presents cybersecurity as a kind of public service rather than just a technical task. Versar Global Solutions positions itself as a business that emphasizes innovation, teamwork, and meaningful effect by presenting the position in this way, which may appeal to those looking for employment with a purpose.

Conclusion

The job posting for a Cyber Security Threat Analyst at Versar Global Solutions captures the contemporary demands of cybersecurity experts. It strikes a balance between communication, leadership, flexibility, and technical rigor. Threat modeling, protocol validation, and certification are among the abilities that are specifically listed in the job, but it also suggests continued education, time management, and interdisciplinary collaboration. The organization promotes honesty, teamwork, and quality in its workers, as evidenced by its inclusive culture and mission-oriented tone. In the end, this job posting is a microcosm of the cybersecurity sector as a whole, requiring both technical proficiency and human intuition in a constantly changing digital environment.

Reference

Versar Global Solutions. (n.d.). *Cyber Security Threat Analyst*. Indeed.com. https://www.indeed.com/viewjob?jk=1aba0589b18b9dc0&from=shareddesktop_copy