Leidos Cyber Analyst Position

Dominic R. Clark

Old Dominion University

Abstract

This analysis examines a Cyber Threat Intelligence Analyst position at Leidos, focusing on the intersection of technical expertise and intelligence analysis within the Intelligence Community (IC). Through detailed examination of the job requirements, organizational culture, and industry context, this paper demonstrates how the role combines traditional intelligence analysis with emerging cybersecurity demands. The analysis reveals both explicit and implicit skill requirements, highlighting the importance of technical proficiency, analytical capabilities, and strong communication skills. By examining the position within the broader context of growing cyber threats and intelligence community needs, this paper illustrates how contemporary cybersecurity education and training align with the position's demands. The analysis concludes that success in this role requires a sophisticated blend of technical expertise, analytical capabilities, and strong interpersonal skills, making it an ideal opportunity for cybersecurity professionals seeking to contribute to national security objectives.

Leidos Cyber Analyst Position

In an era where cyber threats increasingly challenge national security, the convergence of cybersecurity expertise and intelligence analysis has become crucial for protecting national interests. Leidos, a Fortune 500 innovation company, seeks a Cyber Threat Intelligence Analyst to support their Intelligence Community program in Northern Virginia. This position exemplifies the evolving nature of cybersecurity roles within the intelligence sector, demanding a unique combination of technical knowledge, analytical capabilities, and policy awareness. This analysis will examine how the position's requirements reflect both current industry demands and future trends while exploring the implicit skills and organizational culture that contribute to success in this role. Through careful examination of the job posting and company context, this paper will demonstrate how the position represents a critical intersection of technical expertise and intelligence analysis, requiring both explicit and implicit skills that align with contemporary cybersecurity education.

Leidos operates as a leading technology, engineering, and science solutions provider, specifically supporting critical national security initiatives. Within their National Security Sector, the Cyber Threat Intelligence Analyst position supports the Cyber Threat Intelligence Integration Center (CTIIC), indicating its strategic importance in national cybersecurity efforts. The position's placement within CTIIC suggests a role focused on synthesizing and analyzing cyber threat information to inform policy decisions and protective measures.

The role's requirements indicate a mid-level position, as evidenced by the requirement for 4-8 years of prior relevant experience and the necessity of previous IC experience. This positioning suggests that while academic qualifications are important, practical experience in both cybersecurity and intelligence analysis is crucial for success. The organization of the job posting itself reveals key priorities, placing security clearance requirements (TS/SCI with polygraph) and experience qualifications at the forefront, indicating that immediate integration into sensitive IC operations takes precedence.

The position demands specific technical and analytical capabilities explicitly stated in the job posting. Core requirements include the ability to identify and analyze cyber threat actors' plans, intentions, capabilities, and tradecraft. This aligns directly with coursework in network security, digital forensics, and threat analysis. The emphasis on strong interpersonal, critical thinking, and communication skills highlights the position's bridge between technical analysis and policy implications.

Reading between the lines, several unstated but crucial skills emerge from the position description. The mention of a fast-paced collaborative environment and need to proactively multi-task and meet short deadlines suggests the importance of stress management, time prioritization, and crisis response capabilities. These implicit requirements align with courses in project management and incident response planning.

My academic preparation through cybersecurity coursework provides strong foundations for this position. Advanced courses in network security have developed my understanding of TCP/IP and network protocols essential for threat analysis. Digital forensics coursework has equipped me with skills in memory analysis, timeline analysis, and artifact recovery – all critical for threat attribution and investigation. Additionally, courses in cybersecurity law and compliance have provided knowledge of FISMA compliance, NIST frameworks, and international cyber law awareness.

Programming courses, particularly in Python, have developed my capabilities in automation and data analysis, essential for processing threat intelligence. The combination of technical courses with communication-focused coursework has prepared me to clearly convey complex and technical data to nontechnical customers, as required by the position.

The position exists within a rapidly expanding sector, with cybersecurity jobs projected to grow significantly. Current industry trends affecting this role include increased state-sponsored cyber operations, evolution of AI-powered threats, and growing emphasis on critical infrastructure protection. The role's placement within CTIIC reflects the government's strategic priority on cyber threat intelligence integration, suggesting long-term stability and growth potential. This aligns with Leidos's strong market position, evidenced by their $15.4 billion revenue in fiscal year 2023.

Leidos emphasizes a culture of innovation and collaboration, demonstrated through their focus on innovative solutions through the efforts of diverse and talented people. The company's commitment to doing the right thing for their customers, people, and community suggests a strong ethical foundation essential for IC work. The posting's tone reflects an encouraging and supportive environment, emphasizing professional development and work-life balance.

The position presents several significant challenges, including maintaining currency with evolving threat landscapes, balancing multiple stakeholder needs, and managing classified information requirements. However, these challenges are presented within a supportive framework, with the posting emphasizing team collaboration and professional growth opportunities. The statement "Your greatest work is ahead!" reflects an optimistic and encouraging organizational attitude toward employee development.

The Cyber Threat Intelligence Analyst position at Leidos represents a sophisticated blend of cybersecurity expertise and intelligence analysis capabilities. The role's requirements reflect both current industry demands and anticipated future needs in national security. Success in this position requires not only strong technical foundations and analytical capabilities but also the ability to operate effectively within the unique culture and constraints of the Intelligence Community. Through careful analysis of both explicit and implicit requirements, it's clear that the position offers significant opportunities for professional growth while contributing to critical national security objectives.

References

Leidos: Careers. (2024). Leidos. https://careers.leidos.com/jobs/15074198-cyber-threat-intelligence-analyst?utm_campaign=google_jobs_apply&utm_source=google_jobs_apply&utm_medium=organic

Annual Reports & Proxy Statements | Leidos. (2023). Leidos. https://investors.leidos.com/financial-information/annual-reports-proxy-statements