**Analysis of SOC Analyst Position at Leidos: Christian Coleman**

## Introduction

The cybersecurity landscape has evolved far beyond traditional technical silos, requiring professionals who can integrate technical expertise with strategic thinking and cross-functional communication. This transformation reflects broader workplace changes where employers increasingly value enterprise and employability skills as key recruiting factors (Clayton & Harris, 2019). Leidos's SOC Analyst position at Fort Meade exemplifies this evolution, presenting a role that, while explicitly requiring technical cybersecurity expertise and incident response capabilities, demands equally sophisticated interdisciplinary skills in communication, strategic thinking, and organizational coordination that my academic background and practical experience have uniquely developed. Success in this role depends not just on technical proficiency, but on the ability to think across disciplinary boundaries and integrate diverse perspectives to solve complex security challenges.

## Company Context and Role's Strategic Position

Leidos operates at the intersection of government contracting and cutting-edge technology solutions, with this position supporting the Defense Enclave Services contract that will "unify the DOD Fourth Estate Defense Agencies and Field Activities' common use information technology systems." This language reveals that the role extends far beyond traditional SOC operations—it positions the analyst as a key participant in organizational transformation within Department of Defense infrastructure. The mention of "interfacing across the program" and coordination with "other DISA organizations, activities, and other services" indicates this position functions as a critical node in a complex network of military and civilian cybersecurity operations.

The strategic nature becomes particularly evident considering the Defense Information Systems Agency (DISA) context, where incidents handled in this SOC have potential implications across multiple military branches and defense agencies. This organizational complexity aligns with broader workplace trends where the World Economic Forum estimates that 65% entering primary school today will end up working in completely new job types that do not yet exist (Clayton & Harris, 2019). The SOC analyst role represents exactly this type of emerging position requiring workers to navigate uncertainty and adapt to rapidly changing technological environments.

## Technical Skills Hierarchy and Communication Requirements

The advertisement reveals a carefully structured hierarchy emphasizing foundational incident response capabilities, with requirements for "DoD IAT Level II certification" and

"KQL/Office 365 Incident response experience." However, the organization of requirements tells a more nuanced story about true priorities. The emphasis on incident response in basic qualifications, contrasted with threat hunting in preferred qualifications, indicates Leidos prioritizes reactive capabilities initially while valuing long-term analytical growth.

While the advertisement never explicitly lists communication skills, nearly every responsibility involves sophisticated information translation and stakeholder coordination. This reflects research findings showing that 67% of HR managers would hire candidates with strong soft skills, even if technical skills were lacking (Henry, n.d.). Phrases like "partner with appropriate authorities in the production of security incident reports," "coordinate with other DISA organizations," and "conveying to users and other teams impact of discovered events" reveal that success depends heavily on translating technical findings into actionable intelligence for diverse audiences.

The requirement to "build timelines, documents, briefings, and other products as required to inform stakeholders" particularly emphasizes communication demands. This requires not just technical understanding but also the ability to construct narratives helping non-technical stakeholders understand both immediate impact and broader implications of security events. LinkedIn research identified creativity, persuasion, collaboration, adaptability, and time management as the five most in-demand soft skills (Henry, n.d.), and the SOC analyst role requires all of these capabilities. My experience investigating "150+ monthly phishing reports using Microsoft Defender for email threat mitigation" has developed my ability to analyze technical indicators and communicate findings to non-technical users, while my work supporting "project management operations including contract deliverables and reviewing Standard Administrative Procedures (SAPs)" during my Deloitte internship provided direct experience in translating technical work into stakeholder-focused documentation.

**Cultural Fit and Innovation Expectations**

The advertisement's final paragraph reveals Leidos's organizational culture, describing seeking someone who doesn't "fit the mold" but rather "melts it down and builds something better." This language, describing the ideal candidate as "restless," "over-caffeinated," and someone who asks "what's next?" before others finish debating current steps, signals that Leidos values innovative thinking and proactive problem-solving over rigid procedure adherence.

This cultural emphasis on innovation connects directly to interdisciplinary thinking and the ability to see patterns and solutions others might miss. The description suggests they want analysts who can not only execute standard incident response procedures but also identify process improvements and develop new approaches to emerging threats. This aligns with broader workplace trends showing urgent need for workers with transferable skills to navigate uncertain job roles and markets (Clayton & Harris, 2019).

My research background, particularly developing a "behavioral detection framework using context manipulation techniques" for server vulnerability detection, demonstrates exactly this innovative thinking. Rather than simply identifying known vulnerabilities, I've focused on developing new approaches to threat detection that could identify previously unknown attack vectors. This research mindset, combined with practical SOC experience, positions me to contribute both immediate operational value and longer-term strategic innovation.

**Leadership and Strategic Thinking Requirements**

Several aspects reveal expectations for leadership extending beyond typical analyst responsibilities. The requirement to "drive incidents from discovery to closure and reporting" indicates analysts must take ownership of entire incident lifecycles, not simply execute assigned tasks. The responsibility to "provide enterprise recommendations to Leidos and DISA leadership" explicitly positions the analyst as a strategic contributor who can identify systemic issues and propose organizational-level solutions.

The expectation to "conduct continuous exercises and dry runs to improve response outcomes" demonstrates this role involves proactive leadership in developing team capabilities. This requires not just technical knowledge but also understanding of adult learning principles, team dynamics, and continuous improvement methodologies. Research from the Hay Group showed that managers incorporating soft skills in their leadership approach increase team performance by about 30% (Henry, n.d.), particularly relevant in SOC environments where team coordination during high-stress incidents directly impacts security outcomes.

My experience leading "Student Security Operations Center (SOC) operations" at Old Dominion University provided direct experience in the operational leadership this position requires. Managing SOC operations involves not just technical incident response but also coordinating team activities, ensuring consistent procedures, and continuously improving effectiveness.

**Integration of Interdisciplinary Skills**

The complexity of this SOC Analyst position perfectly illustrates why modern cybersecurity roles require interdisciplinary thinking rather than purely technical expertise. Success requires integrating insights from computer science and information security (for technical incident response), psychology (for understanding user behavior and threat actor tactics), organizational behavior (for effective multi-agency coordination), communication studies (for stakeholder engagement), and strategic management (for enterprise-level recommendations and process improvement).

This interdisciplinary requirement reflects broader workforce changes where industry expects students to possess generic skills enabling them to work as part of organizations, with

some studies finding these skills more sought after in new entrants than technical skills (Clayton & Harris, 2019). Many employers report that their priority in applicants is personality, drive and passion, and that they can address technical deficiencies post-recruitment (Clayton & Harris, 2019). This perspective particularly applies to cybersecurity, where rapid threat evolution means specific technical skills become obsolete quickly, but underlying analytical thinking and adaptability remain valuable throughout careers.

My academic background in cybersecurity provided not just technical knowledge but also exposure to the interdisciplinary nature of modern security challenges. Courses in risk management taught me to think systematically about how individual security incidents connect to broader organizational vulnerabilities, while practical experience across different organizational contexts developed my ability to adapt communication styles and operational approaches to different organizational cultures and stakeholder needs.

**Skills Development and Future Implications**

The evolution toward interdisciplinary cybersecurity roles has important implications for how professionals develop and maintain relevant skills. Research from MIT Sloan showed that soft skills training may improve productivity within organizations, returning roughly 250% on investment within eight months (Henry, n.d.). This becomes particularly relevant in cybersecurity, where security incident costs can be enormous and effective incident response coordination can mean the difference between minor disruption and major organizational impact.

The position's emphasis on continuous improvement through "exercises and dry runs" aligns with research showing ongoing skills development remains crucial in rapidly changing fields. VET and skills development have assumed greater policy priority driven by skills mismatch, changing employment nature, and new skill demands from globalization and new technologies (Clayton & Harris, 2019).

My commitment to continuous learning, demonstrated through pursuing additional certifications like "AWS Certified AI Practitioner (In Progress)" and conducting independent research projects, reflects the proactive skills development this position requires. The cybersecurity field demands professionals who can not only apply current knowledge but also continuously acquire new capabilities as threats and technologies evolve.

**Conclusion**

The Leidos SOC Analyst position represents cybersecurity's evolution from a purely technical discipline to an inherently interdisciplinary field requiring integration of technical expertise with strategic thinking, communication skills, and organizational understanding. While technical requirements are substantial, deeper analysis reveals that success depends equally on

the ability to think across traditional boundaries and synthesize diverse perspectives into comprehensive security solutions.

The broader context of workforce transformation, where multiple factors interact to create new jobs and render others obsolete, makes this role's interdisciplinary nature particularly relevant. Employees with strong soft skills have the ability to grow and flourish in any environment due to experience and interpersonal skills that make adapting easier (Henry, n.d.). This adaptability becomes crucial in cybersecurity, where threat landscapes change constantly and effective response requires coordination across multiple organizational levels and technical domains.

My combination of hands-on technical experience, SOC leadership, research background in innovative threat detection, and exposure to diverse organizational contexts has prepared me to contribute immediately to Leidos's operational needs while bringing the interdisciplinary thinking necessary for long-term strategic impact. The position offers an ideal opportunity to apply both technical cybersecurity expertise and broader analytical capabilities to challenges that matter for national security, while continuing to develop the leadership and strategic thinking skills that will define the future of cybersecurity operations.

**References**

Clayton, B., & Harris, R. (2019). Editorial: The importance of skills – but which skills? Journal of Vocational Education & Training, 71(2), 195-199. https://doi.org/10.1080/14480220.2018.1576330

Henry, H. (n.d.). The importance of soft skills in the workplace. Junior Achievement USA.

Leidos. (2025, October 21). SOC Analyst - Fort Meade, MD. LinkedIn. https://www.linkedin.com/jobs/collections/recommended/?currentJobId=4318162883&discover=recommended&discoveryOrigin=JOBS_HOME_JYMBII&start=24