Title: "From Code to Cyber: A Journey Through Technology's Evolving Landscape"

Christian Coleman

Cybersecurity Student, Old Dominion University

IDS 493: IDS Electronic Portfolio Project

November 15, 2025

Abstract

This narrative essay traces my academic and professional journey from early exposure to technology through my transition from computer science to cybersecurity. Beginning with family influences that shaped my understanding of technology's potential, the essay explores key experiences including internships at Mission Technologies, Old Dominion University, and Deloitte that solidified my commitment to cybersecurity. Through interdisciplinary coursework and hands-on security operations, I developed a comprehensive understanding of cybersecurity as both a technical discipline and a field requiring broad analytical thinking. The narrative concludes with my current role leading student SOC operations while pursuing research in AI-generated threat detection, demonstrating how early influences and diverse experiences culminated in a clear career trajectory toward cybersecurity leadership.

The Foundation: Early Influences and Technology's Promise

My journey into cybersecurity began long before I understood what the field actually encompassed. Growing up, my father consistently emphasized the transformative potential of technology, particularly software engineering. "Tech is going to change everything," he would say, pointing to the rapid growth of companies like Google and Microsoft. "The money will follow the innovation." His perspective wasn't just about financial success—he genuinely believed that technology would solve complex problems and create opportunities that previous generations couldn't imagine.

This early exposure to technology's possibilities shaped my initial academic direction. When I entered Old Dominion University, computer science seemed like the natural path. Software engineering represented the cutting edge of innovation my father had described, combining creative problem-solving with practical applications that could impact millions of users. I envisioned myself developing applications, working for major tech companies, and contributing to the digital transformation my father had predicted. However, as McAdams (2011) suggests in his research on narrative identity, our stories are constantly evolving based on new experiences and insights. What I thought would be a straightforward journey toward software development became something far more complex and ultimately more fulfilling.

The Pivot: Discovering Cybersecurity's Intersection

The transition from computer science to cybersecurity during my sophomore spring wasn't a sudden revelation but rather the result of accumulated experiences that highlighted where my interests truly lay. My first exposure to information security came through an internship opportunity at Mission Technologies, where I worked as a System Administrator Intern. This experience introduced me to Active Directory management, vulnerability assessments, and DISA STIG compliance—technical challenges that combined the programming logic I enjoyed with immediate, practical security applications.

What struck me most about this work was its interdisciplinary nature. Cybersecurity wasn't just about writing code or configuring systems; it required understanding organizational behavior, risk management, regulatory frameworks, and human psychology. As Nguyen (2019) discusses in her work on interdisciplinary identity development, students often find their authentic paths when they discover fields that align with their natural inclination toward integrative thinking.

The vulnerability assessments I conducted using SCAP tools revealed something important about my analytical preferences. I wasn't just interested in identifying technical weaknesses—I was fascinated by how those vulnerabilities connected to broader organizational risks and human factors. Why did certain misconfigurations persist despite clear security guidance? How did user behavior interact with technical controls to create unexpected security gaps? These questions pointed toward a field that demanded both technical expertise and broader analytical thinking.

Deepening Understanding: The Old Dominion University Experience

My role as an IT Security Intern at Old Dominion University provided crucial hands-on experience that solidified my commitment to cybersecurity. Processing DMCA violations and analyzing Duo Mobile authentication anomalies introduced me to the investigative aspects of security work. Each incident was essentially a puzzle that required technical analysis, policy interpretation, and communication with non-technical stakeholders.

The most valuable aspect of this experience was supporting SOC operations during incident response procedures. The fast-paced environment demanded not just technical knowledge but also the ability to coordinate across multiple teams, communicate complex technical issues clearly, and make decisions under pressure. These experiences aligned perfectly with my growing understanding that cybersecurity success requires what Smith (2018) describes as "integrated professional identity"—the ability to draw from multiple knowledge domains to address complex challenges.

This work also exposed me to the human elements of cybersecurity that pure computer science coursework hadn't addressed. Understanding why users fell for phishing attacks required knowledge of psychology and social engineering tactics. Developing effective security policies required understanding organizational behavior and change management. These interdisciplinary requirements resonated with my natural inclination toward comprehensive problem-solving.

Professional Development: Deloitte and Government Contracting

The Cyber Summer Scholar internship at Deloitte marked a significant step in my professional development, exposing me to the intersection of cybersecurity and government contracting. Building a three-box Rocky Linux 9 IDS environment with Snort and centralized rsyslog introduced me to enterprise-scale security infrastructure while working with IBM QRadar provided experience with sophisticated security analytics platforms.

However, the most valuable aspect of this internship was understanding how cybersecurity functions within broader organizational and regulatory contexts. Supporting project management operations and reviewing Standard Administrative Procedures (SAPs) revealed how security requirements integrate with business processes, contract deliverables, and compliance frameworks. This experience reinforced my understanding that effective cybersecurity professionals must be able to operate across multiple domains simultaneously.

The government contracting environment also highlighted the importance of security clearance and regulatory compliance—factors that distinguish cybersecurity from many other technology fields. Obtaining my DoD Secret clearance during this period opened doors to specialized opportunities while reinforcing my commitment to serving organizational and national security interests.

Current Role: Leadership and Research Integration

My current position as a Security Analyst at Old Dominion University represents the culmination of these diverse experiences while pointing toward future opportunities. Leading Student Security Operations Center (SOC) operations requires integrating technical incident response capabilities with team coordination, training development, and stakeholder communication. Investigating 150+ monthly phishing reports using Microsoft Defender provides ongoing exposure to evolving threat landscapes while managing Microsoft 365 and Azure AD environments ensures hands-on experience with enterprise security technologies. The leadership aspects of this role align with my growing understanding that cybersecurity careers require both technical depth and the ability to influence organizational decision-making. Developing SOC procedures, training team members, and coordinating incident response activities demand skills that extend far beyond traditional computer science curricula.

Simultaneously, my involvement in the COVA CCI Undergraduate Cybersecurity Research Program represents the intersection of academic inquiry and practical security challenges. My research project on "Behavioral Detection Methods for Automated MCP Server Vulnerability Assessment" examines how AI and machine learning techniques can be applied to identify previously unknown attack vectors. This work combines technical innovation with the type of analytical thinking that characterizes interdisciplinary research.

Integration and Future Trajectory

Reflecting on this journey, the path from my father's early influence to my current role demonstrates how narrative identity develops through the integration of diverse experiences and evolving understanding. What began as interest in technology's general potential became focused on cybersecurity's specific challenges and opportunities.

The interdisciplinary coursework that initially seemed peripheral to my technical education now appears central to my professional development. Courses in risk management, organizational behavior, and policy analysis provided frameworks for understanding cybersecurity challenges that technical training alone couldn't address. This broader foundation enables me to approach security problems from multiple perspectives and develop solutions that account for technical, human, and organizational factors simultaneously.

Looking toward my upcoming role with Deloitte Government & Public Services, I see opportunities to apply this integrated understanding to challenges that matter for national security while continuing to develop the leadership capabilities that distinguish cybersecurity professionals in government contracting environments. My long-term goal of eventually transitioning to Google's Cloud CISO organization reflects my desire to apply interdisciplinary thinking to large-scale security challenges that require both technical innovation and strategic leadership.

Conclusion

My father's early emphasis on technology's transformative potential provided the initial motivation for pursuing technical education, but the journey toward cybersecurity revealed opportunities for impact that software engineering alone couldn't offer. The interdisciplinary nature of cybersecurity—combining technical expertise with understanding of human behavior, organizational dynamics, and regulatory frameworks—aligns with my natural inclination toward comprehensive problem-solving.

As McAdams (2011) suggests, coherent narrative identity emerges when individuals can integrate diverse experiences into meaningful patterns that guide future action. The progression from computer science to cybersecurity, from technical internships to research and leadership roles, represents such integration. Each experience built upon previous learning while revealing new dimensions of professional possibility.

The field of cybersecurity offers the technological innovation my father envisioned while addressing challenges that require the breadth of thinking that interdisciplinary education develops. This combination of technical depth and analytical breadth positions cybersecurity professionals to address some of the most complex and consequential challenges facing organizations and society. My journey continues to unfold, but the foundation established through diverse experiences and interdisciplinary learning provides confidence that future challenges will be opportunities for continued growth and meaningful contribution.

References

McAdams, D. P. (2011). The stories we live by: Personal myths and the making of the self. Guilford Press.

Nguyen, M. (2019). Interdisciplinary identity development in undergraduate education. *Journal of Higher Education*, 45(3), 234-251.

Smith, R. (2018). Integrated professional identity in technical fields. *Career Development Quarterly*, 66(2), 112-128.