Reflection on my Academic Experience

Kristina Gamache

Department of Cybersecurity

APA Citation

IDS 493

Dr. Gordon-Phan

08/07/2025

Introduction

Pursuing and earning my Bachelor of Science in Cybersecurity at Old Dominion University has provided me with both the technical experience and interdisciplinary problem-solving skills that are needed to be successful in the vast and constantly evolving industry that is cybersecurity. Through my coursework, and internships with the City of Virginia Beach, I have developed a professional foundation that integrates proficiency with communication, collaboration, and analytical thinking. My academic journey and experiences have prepared me for my ultimate career goal of becoming a Cybersecurity Analyst, with a focus on threat detection, incident response, and secure systems management. This reflection looks at my three skillsets: cybersecurity analysis, technical documentation, and interdisciplinary problem-solving. Each skillset is supported by evidence that demonstrates my readiness and abilities for the cyber workforce. From real-world incident response using Microsoft Defender for Endpoint, Splunk, and XSIAM, to documenting operational procedures for cloud-based environments, to applying the NIST Cybersecurity Framework across departments, these skills reflect both my technical knowledge and the ability to adapt in diverse, collaborative environments. By integrating knowledge from IT, policy, and business disciplines, I possess the ability to address complex cybersecurity challenges within a real-world setting.

Skill 1: Cybersecurity Analysis

Cybersecurity analysis has been at the core of my academic and professional training. During my internship as a Cybersecurity Analyst for the City of Virginia Beach, I was responsible for identifying, investigating, and mitigating security threats in real time. One of the most important things I learned from this experience was how to conduct incident response using Microsoft Defender for Endpoint. This assignment involved monitoring and analyzing endpoint

alerts, classifying threats, and implementing remediation steps. From this opportunity, I gained insight into malware behaviors, phishing indicators, and lateral movement patterns within an enterprise network. The hands-on experience reinforced my academic learning on threat detection systems and improved my ability to prioritize threats in a high-volume alert environment.

Another application of knowledge obtained during my academics at ODU was how I applied the Cyber Kill Chain model to recognize and disrupt adversarial activities early in the attack lifecycle. Understanding each stage of the kill chain allowed me to proactively identify indicators of compromise (IOC) and intervene before threats escalated into full-scale attacks (What is the Cyber Kill Chain?, 2024). A good understanding of this framework enhanced my incident detection capabilities by structuring analysis around attacker tactics and techniques, supporting more effective mitigation strategies aligned with industry best practices.

A key project involved event monitoring using Security Information and Event Management (SIEM) platforms, specifically Splunk and Palo Alto's XSIAM. My work involved interpreting security event data and correlating incidents across different log sources to detect potential coordinated attacks. This artifact reflects my ability to integrate technical analysis with pattern recognition skills, combining data from multiple security domains. Through this process, I applied the NIST Cybersecurity Framework's "Detect" and "Respond" functions in a live environment, which exemplifies my understanding of industry best practices (National Institute of Standards and Technology, 2018).

Skillset 2: Technical Documentation

Skillset 3: Interdisciplinary Approach

Conclusion

References

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. *Framework for Improving Critical Infrastructure Cybersecurity, 1.1(1). https://doi.org/10.6028/nist.cswp.04162018*

What is the Cyber Kill Chain? (2024, August 8). SentinelOne. https://www.sentinelone.com/cybersecurity-101/threat-intelligence/cyber-kill-chain/