The Work Behind the Portofolio

Nehemia Araia

The University of Old Dominion

IDS 493: Electronic Portfolio Project

Dr. Phan

May 5, 2026

Abstract

This reflection essay examines the skills, artifacts, and academic experiences that shaped my development as a cybersecurity student and emerging professional at Old Dominion University. Drawing on coursework across cybersecurity, data science, ethics, and interdisciplinary studies, I reflect on how three core skills, Cybersecurity Operations, Cloud Computing and DevSecOps, and AI and Automation, were developed and demonstrated through nine artifacts collected during my undergraduate program. Using frameworks from McAdams (2001), Nguyen (2013), Repko and Szostak (2017), and the NIST AI Risk Management Framework (Tabassi, 2023), this essay explores how an interdisciplinary approach to education prepared me for a career in AI security. The artifacts discussed range from professional interviews and industry certifications to hands-on technical projects and academic papers, each representing a different dimension of my growth. This portfolio is not a finished document but a reflection of where I started, what I built, and where I am headed.

The Work Behind the Portfolio

Introduction

When I started at Old Dominion University, I did not have a clear direction. I came in undecided and spent my first year going through the motions without a real reason to be there. The decision to switch into the cybersecurity program changed everything. From that point forward, my academic and professional experiences started building on each other in ways I did not expect. What I did not fully realize at the time was that the degree I was pursuing was not just a cybersecurity degree. It was an interdisciplinary one, pulling from ethics, data science, writing, and systems thinking to shape how I approach problems. Repko and Szostak (2017) describe interdisciplinary research as a decision-making process that is heuristic and iterative, meaning it requires drawing from multiple disciplines and refining your thinking as you go. That description fits my experience at ODU better than anything else I could say about it. This essay reflects on three skills I developed throughout my program, Cybersecurity Operations, Cloud Computing and DevSecOps, and AI and Automation, and the nine artifacts that demonstrate them.

Cybersecurity Operations

Security+ Certification

The CompTIA Security+ certification was one of the first formal validations of what I had been learning in the classroom. Studying for it pushed me to go deeper into areas like threat detection, identity and access management, and risk management than my coursework alone required. It gave me a structured way to think about cybersecurity as a field rather than just a collection of tools and techniques. More importantly, earning it gave me confidence that the knowledge I was building was real and applicable. It was an early signal that I was moving in the right direction.

Interview with Edmond Cook, Security Engineer

One of the most valuable things I did during my time in the SOC was to interview Edmond Cook, a Security Engineer at ODU's Information Security Office, and ask him how he got where he is. His path was not a straight line. He started in a call center, moved into desktop support, and eventually made his way into security engineering by taking opportunities as they came and building a strong foundation along the way. What stood out to me most was when he said that great engineers understand their tools deeply and can think ahead, not just execute. That idea stayed with me. Working in the SOC every day, I started paying closer attention to patterns, not just alerts. I started thinking about why something was happening, not just what to do about it. This interview helped me connect the daily work of security operations to the longer arc of building a career in this field.

Interview with Edward Scott, Sr. Cloud Security Engineer

The interview with Edward Scott gave me a different perspective on the same question. His career moved through systems administration and network engineering before landing in cloud security, and his main advice was simple: be proactive. He described proactive security as identifying weaknesses before they become problems, not waiting for something to break. That mindset directly influenced how I approach my work in the SOC. When I am reviewing phishing alerts or investigating endpoint activity, I am not just checking a box. I am trying to understand what the attacker was attempting and whether there is something in the environment that made it possible. Working in security operations taught me to think that way, and Edward's perspective reinforced why it matters. McAdams (2001) argues that identity is built through the stories we tell and revise about ourselves. Both of these interviews became part of the story I am building about who I want to be professionally.

Cloud Computing

AWS Solutions Architect Associate Certification

The AWS Solutions Architect Associate certification pushed me to think about infrastructure at a level I had not reached before. Designing systems that are highly available, fault tolerant, and cost efficient requires you to hold a lot of moving parts in your head at once. It also requires you to think about security at every layer, not as an afterthought. The exam and the preparation behind it gave me a structured mental model for cloud architecture that I carried directly into my internship at Amazon Web Services and into every project I built afterward.

AWS Certified AI Practitioner Certification

The AWS Certified AI Practitioner certification validated my understanding of artificial intelligence and machine learning concepts as they apply to cloud environments. It also deepened my understanding of responsible AI development, which became increasingly relevant as I started building AI-powered tools myself. The NIST AI Risk Management Framework (Tabassi, 2023) emphasizes that managing AI risks requires thinking about trustworthiness, safety, and accountability from the design stage forward. That framing is one I took seriously as I moved from learning about AI to actually building with it. This certification helped me connect the conceptual side of AI governance to the practical work I was doing in my projects.

AI Driven Cloud Threat Analysis and Compliance Mapping

This project was one of the most technically demanding things I built during my time at ODU. I deployed a fully automated cloud incident processing pipeline using AWS CloudFormation that uses Amazon Bedrock to generate AI summaries of GuardDuty findings, correlates them with CloudTrail logs, maps each threat to NIST 800-53 and CIS controls, and sends structured email alerts automatically. Building it required me to combine cloud architecture, security operations knowledge, and AI integration in a way that felt genuinely new. It was not a class assignment. It was a problem I identified and decided to solve. Nguyen (2013) describes the ePortfolio as a living portal through which students work out who they are becoming. This project, more than almost anything else in this portfolio, shows where my head has been and where I want to take my career.

AI and Automation

AI SOC Assistant

The RAG-Based SOC Assistant started as a chatbot prototype that could not handle real incident response questions. Once I recognized that limitation, I rebuilt the entire system around a retrieval-based approach that pulls answers from approved documentation including NIST SP 800-61, CISA playbooks, and MITRE ATT&CK rather than generating generic responses. The result was a tool that gives analysts structured, policy-aligned guidance during live incidents with citations to the exact documents used. Building this project taught me more about the gap between AI outputs and operational trust than any class I took. It is one thing to build something that sounds right. It is another to build something that can be trusted when something is actually going wrong in a security environment.

Security AI Agent for Vulnerability Assessment

The Security AI Agent project took a different approach to the same underlying idea: using AI to make security work faster and more reliable. I fine-tuned a language model with LoRA, built a RAG pipeline that pulls OWASP and CWE documentation, and connected the output to real scanners like Semgrep, Tfsec, and Checkov so findings could be validated rather than just flagged. The hardest part of this project was not the AI component. It was building the validation layer and making sure the system produced results that a real analyst could act on. This project pushed me the most out of everything in this portfolio because AI security is the area I have the least experience in, even though it is where I most want to grow. Getting through it gave me a clearer sense of what I am capable of when I commit to figuring something out.

Meta's AI Training and the Ethics of Public User Data

This paper came from a philosophy course on ethics and data, and it challenged me to think about AI from a completely different direction. Rather than asking how to build AI systems, it asked whether certain uses of AI are ethical at all. Analyzing Meta's decision to use public social media content to train its models without meaningful user consent pushed me to think about power, transparency, and the responsibilities that come with building systems that affect people. Kerkhoff (2020) argues that interdisciplinary learning expands how students understand problems by exposing them to multiple frameworks at once. That is exactly what this course did for me. It is one thing to know how a system works. It is another to think critically about whether it should exist in the form it does. That kind of thinking is something I bring into my AI security work now, and I think it makes my approach more thoughtful.

Conclusion

Looking at this portfolio as a whole, the thread running through all of it is the same one that runs through my personal narrative. I found something I actually cared about and kept building on it. The skills I developed did not come from any single class or experience. They came from combining what I learned in the classroom with what I experienced in internships, personal projects, and conversations with people already doing the work I want to do. Repko and Szostak (2017) describe interdisciplinary thinking as a process of drawing from multiple disciplines to reach a more complete understanding of a problem. That is what an interdisciplinary degree taught me to do, and it is what I find myself doing every time I sit down to solve a security problem. Courses like IDS 300W reinforced that writing clearly and thinking across disciplines are not soft skills. They are essential ones. Being able to explain a security risk

to a non-technical audience, or to think about the ethical implications of an AI system, makes me a more complete professional than someone who only knows the technical side. As AI continues to reshape the cybersecurity landscape, that interdisciplinary foundation is going to matter more, not less. This portfolio is not a finished document. It is a record of where I started, and a starting point for everything still ahead.

References

Kerkhoff, S. N., & Cloud, M. E. (2020). Equipping teachers with globally competent practices: A mixed methods study on integrating global competence and teacher education. *International Journal of Educational Research*. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7320918/

McAdams, D. P. (2001). The psychology of life stories. *Review of General Psychology, 5*(2), 100-122. https://doi.org/10.1037/1089-2680.5.2.100

Nguyen, C. F. (2013). The ePortfolio as a living portal: A medium for student learning, identity, and assessment. *International Journal of ePortfolio, 3*(2), 135-148. https://files.eric.ed.gov/fulltext/EJ1107805.pdf

Repko, A. F., & Szostak, R. (2017). *Interdisciplinary research: Process and theory* (3rd ed.). Sage.

Smith, E. E. (2017, January 12). The two kinds of stories we tell about ourselves. *TED Ideas*. https://ideas.ted.com/the-two-kinds-of-stories-we-tell-about-ourselves/

Tabassi, E. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-1