Internship Retrospective Analysis

Jordan Hernaez

Defense Intelligence Agency

CYSE 368

Summer 2024 Term

07/28/2024

Table of Contents

Internship Retrospective Analysis

Through my pursuit and completion of an internship with the Defense Intelligence Agency (DIA), I was able to contribute directly to national security as well as apply much of what I have learned in a real-life environment. With focuses on Identity, Credential, and Access Management (ICAM), I assisted in planning network architecture, researching Zero Trust (ZT) strategies, and designing features and implementation for DIA applications. The key takeaways from this experience include flexibility, the importance of a strong foundation of knowledge, and seeking opportunity in the face of adversity. Although challenging, the experience realigned my goals, and provided me with specialized insights into employment within the government.

Introduction

When beginning my search for an internship, I had only one requirement: working within the government. I am highly driven by not only my own personal academic and professional ambitions, but also by my desire to contribute towards something bigger than myself. Having an opportunity to contribute towards national security in pursuit of my own interest is something that I deeply respect and cherish. More specifically, I chose to work within the Defense Intelligence Agency (DIA) because I wanted to focus my efforts on protecting our nation. The DIA's motto is "Committed to excellence in defense of the nation". No organization could have goals more closely aligned with mine than the DIA.

Prior to the start of my internship, I outlined three specific outcomes and goals. They are as follows:

1. Work with Identity, Credential, and Access management (ICAM) lead to establish a plan for network architecture
    o As I initially had limited knowledge into the ICAM sphere, I was to learn more about ICAM in general as well as government specific issues and implementations
2. Research other government agency Zero Trust strategies to determine the best fit solution for DIA
    o In addition to understanding ICAM, I was also tasked with understanding how other agencies implemented Zero Trust within their own ICAM infrastructure to best determine how to implement Zero Trust within DIA's own ICAM infrastructure

3. Assist with software design and feature and implementation
   o Because there are several proprietary applications and implementations of software within the DIA, there are several specific adjustments and modifications to existing software and applications that required specialized knowledge

This paper will outline my initial foray into government Cybersecurity, how management within the DIA contributed towards my achievement of my learning outcomes, my contributions towards the DIA, and what aspects of my knowledge gained at ODU contributed towards my success as a DIA intern. In addition, I will also outline some of the motivating, discouraging, and challenging aspects of the internship, as well as a retrospective look at what advice I would provide future DIA interns to ensure their success.

The DIA and my Internship

The DIA was founded in 1961 to help facilitate interagency intelligence sharing as well as to gather and analyze foreign intelligence in defense of the nation. Prior to the DIA, existing intelligence agencies were having trouble coordinating amongst themselves and intelligence efforts were being duplicated amongst them. The DIA's main function is to collect and analyze foreign intelligence to facilitate informed decisions by the Secretary of Defense and the Director of National Intelligence. Today, the DIA employs over 16,000 officers around the world and is the leading all-source intelligence agency for the U.S. government.

Prior to starting my internship, I was unsure of what to expect. I have worked in many a career field, but none as unique and intimidating as the federal government. Working within the government essentially enlists you as a public servant, and the impact of your decisions reverberate far beyond your immediate sphere of influence.

When beginning this internship, the orientation team took a significant amount of time to break down government specific ideas and methodologies. For instance, the importance of information classification determines the potential damage to the security of the nation. In addition to this, during the orientation we were frequently reminded of the importance of networking, and we were provided with numerous opportunities to do so. Taking the time to decompress and speak to others in the internship cohort allowed me to secure numerous connections with interns with varying fields and interests that I don't think I would have made otherwise. I believe that taking the time to lay a solid foundation of understanding by the DIA contributed heavily to my easing into this new environment and helped significantly in furthering my understanding of the intelligence community.

The Management Environment

The management structure at the DIA has allowed for effective communication of successes, and failures, as well as providing support when needed. One of my favorite aspects of the internship was the relative hands-off mentality of my leadership team. When needed, leadership was there to support me, but also provided me the opportunities to find answers on my own. My main management points of contact were my supervisor, and my technical lead. While my supervisor helped provide administrative support such as facilitating leave requests and assisting with questions regarding pay, my technical lead provided technical support on the projects I had worked on. With credit due to DIA, they provided numerous points of contact, some even redundant, to ensure I had all the support I needed regardless of what I needed it for.

It is clear to me that the DIA is not only invested in success, but self-sufficiency of its employees. At one point, I was stuck on implementing HTTPS for a server I was to be implementing. I reached out to my technical lead, and he immediately responded to assist. When speaking to him, I made it clear that I wanted assistance, but only enough to push me in the right direction as opposed to a direct answer. He obliged, and I was able to complete my task. This left me with a great sense of satisfaction as I was able to complete the task without being given the answer. This example and many others demonstrated the effectiveness of management within the DIA during my internship.

Major Work Duties and Projects

The team and project I joined during my intern tenure were somewhat unique to me and to the DIA. This resulted mainly from where my team was in certain projects as I joined the team. As it typically takes significant time to obtain all accesses and accounts needed when initially onboarding, my access to information and resources were relatively limited. As a result, my technical lead assigned me numerous readings and videos on understanding my main application of focus, as well as ICAM in general.

After I spent a few weeks understanding the DIA's ICAM environment, I began work specifically on understanding how the DIA implements Single Sign On (SSO) within their computing environments. I created a server and began experimenting and testing various ideas to further understand how SSO is implemented and managed to become a SME for implementation questions.

Once I felt comfortable with the DIA's SSO application, I began to involve myself in Zero Trust (ZT) implementations of SSO. I worked with project leads and teams to better understand the requirements of the DIA and how we can integrate both ZT and SSO without conflict.

My goal during this internship was to become a SME on SSO and identity federation to assist other DIA officers and project contractors to implement ZT within ICAM architecture without incident. I also worked to outline a plan for implementation and consulted with the Risk

Management team to ensure our application adhered by all DIA/DoD guidelines and policies. With the tasks I completed, the DIA was more easily able to coordinate the implementation of ZT within their ICAM environment and I was able to gain a thorough understanding of DoD ICAM implementation.

Cybersecurity Knowledge Application

Before starting this internship, I was not sure what if anything I previously knew would be applicable to the specific tasks and responsibilities I would have on the job. I have heard from others before that many times, the skills you have prior to beginning a job are not nearly as useful as the ability to learn skills in general. I realized quickly that all that I had known regarding ICAM prior to the internship provided very little in the way of preparation for what was to come.

My main skillset prior to the internship was focused within the ethical hacking domain. Shell scripting, network mapping applications, and penetration testing software were the main tools with which I was most familiar. I had also a minor background in simple task automation utilizing the Python and Java programming languages. Most of this, although helpful in being a well-rounded Cybersecurity expert, was not directly applicable to the tasks that lay ahead of me. I was required to become proficient in understanding concepts such as SAML, OAuth, and OIDC to better solve problems and provide insight. I was also required to understand JavaScript, as well as JSON (JavaScript Object Notation), as the main SSO application with which I had focus leaned heavily into JSON Web Tokens (JWT) for authentication and authorization delegation and management.

After I had spent a few weeks on studying and applying ICAM concepts, I realized just how ICAM inept I was. Prior to this internship, I knew very little if nothing regarding ICAM infrastructure, along with its importance. It is easy to not think about something that just works, and in many ways, ICAM does just that. However, once you begin to delve deeper into how it works (or does not work), you learn to appreciate on a much deeper level its importance and the overall importance of how ICAM is able to control access to information to those who need it, and those who do not.

ODU's Curriculum and the Internship

To ODU's credit, I felt very well prepared for most Cybersecurity fields going into this internship. Unfortunately, when I first signed onto this internship I was advised that I may not be placed into a field within my current academic focus. This is exactly what happened. Fortunately for me, I quickly began to take interest in and appreciate ICAM, and now feel incredibly passionate about the work which I did during my internship tenure.

Interestingly, I did realize that during the relatively broad coverage of Cybersecurity concepts in school, the one we seemingly spent the least on were the principles of ICAM. Looking back, I

realize this as an opportunity for ODU, as ICAM is founded upon and reinforces all three pillars of the CIA triad, with specific emphasis on confidentiality and availability. Without a secure and reliable ICAM infrastructure, not only will those who require access to information not be able to access it, but those who are not authorized could access it.

Regarding reinforcement or identification of deficiencies in school, I didn't particularly identify either. As the field I entered within this internship dealt less with what I focused on in school, it wasn't as simple as making one to one comparisons between concepts. I will say though that the general, relatively surface level cybersecurity concepts I learned in school did provide a good foundation of understanding of how and why to conduct operations in a secure manner.

Achievement of Learning Outcomes

Below is a list of the three main learning goals of my internship, and how each were or were not fulfilled:

1. Work with Identity, Credential, and Access management (ICAM) lead to establish a plan for network architecture
   - During my tenure as an intern, myself and my technical lead successfully established and began working a plan to implement Zero Trust architecture within the DIA ICAM environment through collaboration with the Risk Management Framework (RMF) team as well as numerous contractors and vendors
2. Research other government agency Zero Trust strategies to determine the best fit solution for DIA
   - Through numerous collaborative meetings, DIA identified points of interest that could provide technical guidance to implementing other agency's strategies to our own network architecture
3. Assist with software design and feature and implementation
   - I provided significant advice and guidance on ICAM and ZT best practice to ensure the configuration of each application abided by DoD guidelines while remaining open and "future-proof" for further feature implementation

Motivating and Exciting Aspects

I will say that easily the most motivating and exciting aspect of the internship was my ability to contribute to our nation's national security. In prior jobs, although my efforts were important, I didn't feel a strong connection to them. While working with the DIA, I knew that every advancement or achievement made was one not just for me, but for our country.

Aside from this, I thoroughly enjoyed working in an environment that was completely foreign to me and required a significant amount of assimilation and understanding. When working within

the government, it almost felt as if I was learning two separate jobs. The first was obvious – learning how to implement ZT strategies in an ICAM environment. The second, however, was not so easily apparent. The government infrastructure is a world all its own. There is so much to learn about how it operates, what motivates it, and of course, the endless acronyms. This made me feel challenged in a way that I have never been before.

On a more granular level, I enjoyed working with the ICAM team to further improve and integrate existing DIA systems into a more secure and cohesive environment. Being able to improve user experiences for thousands of employees is something that I felt a strong connection to and desire to achieve to my own satisfaction.

Discouraging Aspects

Fortunately, and unfortunately, there was only one major discouraging aspect while working within the DIA. While interning, the HR team within the DIA left something to be desired. Any technical or administrative question I had was so easily and promptly answered by my support staff, but when it came to contacting HR, it seemed as if I was deemed not important enough to find answers for. Seemingly, this is due in a large part to the inherent difficulty in navigating government bureaucracy.

Specifically, I have voiced my interest in becoming a full-time employee with the DIA since the start of my internship and have inquired on how to make this a reality. There were many answers to this end that would require HR input, and as such I reached out to seek these answers. When doing so, HR had advised me answers would be coming, but they never did, not until I had multiple higher up employees intervene.

It almost felt as if DIA was intentionally making it difficult for me to obtain a job, which runs directly contradictory to the entire point of hiring on interns. This was incredibly frustrating, and if I did not have the support of my supervisor, along with my project and technical leads, I don't know if I would have ever obtained the answers I sought.

Challenging Aspects

All aspects of the internship provided some level of challenge which necessitated unique and novel approaches. I would say that the most challenging aspect of the internship was the most discouraging aspect, for the simple fact that I was unable to find the solution on my own, and there was no clear path to success.

With that aside, one of the more difficult and challenging aspect of the internship was assimilating into the government and military environment. It is a unique experience that I can only describe as "other-worldly". This is because almost every aspect of the environment is different than working at what one would consider a typical job. The work language, the

environment itself, the credentials required to obtain the employment, and the level of discretion all make the experience one that I would not easily forget.

Outside of this, also having to learn a new aspect of Cybersecurity through ICAM was not a monumental task, but it was difficult, nonetheless. The combination of the above factors truly made this the most difficult challenge I have faced yet in my lifetime. Fortunately, through this challenge, a newfound motivation to succeed arose. I found that the more difficult the task, the more I worked to overcome it. As a result, I was able to achieve that which I would have never fathomed achieving prior to this internship.

Recommendations for Future Interns

My number one recommendation for any interns who would wish to complete this internship in the future would be emphasizing the importance of a strong foundational knowledge, and insight on how to efficiently obtain knowledge. For myself, I focus less on the knowledge I have gained, and more on how it was gained. It is likely that during tenure as an intern, or within a position, that you will find yourself needing to learn a new task or modify existing knowledge to apply it in unique ways. To do this, you need not existing knowledge but experience on how to obtain knowledge. With this said, it is still important to ensure you have a solid foundational understanding of cybersecurity, as with this you can ensure you will build a strong framework from which to enhance and increase your specialized knowledge.

Outside of knowledge, it is important to remember to surround yourself with people who are more knowledgeable than yourself. Internships are opportunities to learn, so whenever possible you want to ask questions, get answers, and integrate this information with your own understanding to provide novel solutions to concept problems currently facing your organization.

Lastly, being patient and flexible are two concepts that are required to be successful in any capacity, not just internships like my own. There were many opportunities where I had downtime, either waiting for someone to touch base with me, or even when I had finished all I had set out to do for the day. Taking spare time and making it productive is an essential skill to ensure your time is filled with opportunities for learning and growth. It would be easy to complete all tasks for a given day and then mentally "check out" for the remainder. Instead, remember why you are in the internship, and ask around to help someone, or learn something knew that maybe isn't required for your job functions, but could help you better understand them. It will only be of benefit to you.

Conclusion

There are a few main key takeaways from my time as an intern that I would like to share:

1. Build a strong foundation

- To be successful in any career field, it is important to have a solid understanding of the basics. When first joining an organization, it will be assumed that many of the things discussed on a basic level will already be known. With that in mind, do not be afraid to ask questions
2. Be flexible
   - As Helmuth Von Moltke famously said, "No plan survives contact with the enemy". Always be prepared to shift your strategy and ensure that when plans do not go as expected, that contingencies will always be in place to adapt the situation to your advantage.
3. Network
   - There is a commonly held belief that it is not what you know, it is who you know, that defines your success. Knowing people within your organization can not only benefit your ability to complete tasks, but can provide insights previously unknown to you based on their position or experience in their field
4. Take every opportunity to learn
   - Every opportunity is one to learn; it is important to keep this in mind. Whenever down time arises, think about what you can do with this time to benefit yourself, and your employer
5. Seek every opportunity in the face of adversity
   - When situations become difficult or seem impossible to address, it becomes crucial to further your resiliency. These types of circumstances are what breed the most innovative and creative of solutions, and with these epiphanies come great success and achievement

Although my time at ODU is drawing to a close, I feel that I have gained valuable insight on how to proceed through my final semester. Prior to this internship, my goals were to gain as much knowledge as possible while taking classes, but this has since changed. My focus now is primary on ensuring that I learn how and where to obtain information when I need it, as this resource will be utilized for years to come. Although the things I am learning now are important, much of it will be lost to time or rarely utilized. The ability to find information when needed will always be a valued skill.

In the same vein, my professional goals have changed to follow the above philosophy. Prior to the internship I had determined that I wanted to narrow my educational focus as much as possible to become proficient in one specific field. After the internship, my career goals have shifted 180 degrees to the contrary. I now wish to gain surface level knowledge on as many topics as possible, giving myself a perfect opportunity to delve further into each topic as necessary while in my career field to set myself up for success.

With this being said, my internship with DIA has been an incredible experience that I could never forget. It has provided invaluable insights and lessons that I will carry with me through all my academic and professional endeavors. Having the opportunity to apply much of what I learned in a real-life setting was a transformative experience that will guide my future for years to come.