

Dephiant Consulting Inc, Cybersecurity Intern
Xavier Lesane
CYSE 368
Summer 2024

Table of Contents

Introduction.....	3
History	4
Orientation	4
Management.....	5
Major Work Duties	5
Specific use of skills	6
How did the ODU curriculum prepare you for the internship?	6
Objective Fulfillment	7
Motivations/Discouragements/Challenges.....	7
Recommendation for future interns	8
Conclusion	8

Introduction

To start, my name is Xavier Lesane, I am a senior cybersecurity major at Old Dominion University, and cybersecurity is in my blood. I come from a family where everyone does some sort of technology related work whether it be cybersecurity auditing, working as an IT specialist, software development, and many other technology related fields I cannot think of off the top of my head.

Besides fulfilling a degree requirement, I know how important professional experience can be when trying to get into the cybersecurity job market which is why I decided to do this internship. When discussing why I chose to do my internship with this company I will not shy away from the heavy truth that finding an internship or place of employment was difficult as I was competing against hundreds of university, bootcamp, and self-taught students attempting the same task, so frequency of application responses received was definitely a factor. There were a few factors that influenced my decision to commit to an internship with Dephiant Consulting.

As a student, and independent renter I was first and foremost intrigued by their competitive compensation as the amount offer was definitely a criteria for me as this internship meant me taking hours away from my full-time job. Throughout my career at ODU I was reminded time again about how internships could lead to full-time employment and I was reminded of this when applying for this internship as the possible of a full-time career after graduation would be a tremendous boost to my career and life goals. One final reason why I decided to intern at this company was because of how personal I was told my internship would be. Though being around since 2016, Dephiant Consulting Inc is a rather small company, and the internship was going to be a customized experience that would allow me to work in different aspects of cybersecurity, I knew this would prepare me to contribute to whatever business or organization I would find myself working for in the future.

Coming into this internship one of my primary learning objectives for this internship was to get an overview on the way the cyber security frameworks, policies, procedures, and guidelines I learned about in university were applied on the job. As a cybersecurity professional we are responsible for knowing the many policies that are applied to different aspects of society such as the HIPAA and I can say this internship helped broaden my understanding of industry standards like the HIPPA by applying these standards to the organization.

Another objective for me was to learn how to perform cyber threat intelligence integration on newly identified threats and vulnerabilities. After becoming a cybersecurity major I realized one of my first jobs would most likely be as a help desk analyst and I wanted to sharpen those skills ahead of time. I have received some training on those skills thanks to my coursework which I will mention later in this paper, but I can say this internship was an excellent way of getting hands-on training on the software used.

Working in an ever-evolving line of work I knew I had to constantly be up to date on all things cyber including attacks and vulnerabilities which is why one of my primary learning objectives were to stay updated on cyber threats and best security practices. Through team meetings, which I will mention later on, I was able to fulfill this objective and I have learned of more sources to get daily national and global cybersecurity news.

Throughout this paper I will discuss the history of the organization including a few surprising but fun facts about who they have worked with. I will also discuss my initial orientation, and the management structure that drew me in to apply for this company. I will also discuss as much, in as much detail as I am allowed, some of the work I have done for the company. I will end the paper discussing how this internship affected my personal skills, how the ODU curriculum prepared me for this role, how I met my personal goals for this position, and the hurdles I faced.

History

I worked as a cybersecurity intern for Dephiant Consulting Inc. Dephiant Consulting is a security consulting firm that specializes in corporate security consulting services. Founded in 2016, Dephiant Consulting has provided customers with their highly certified staff in counterintelligence operations, penetration testing, governance and regulatory compliance security consulting, ethical hacking, counterterrorism, cloud computing support, cyber analytics, help desk support, hardware and software support, database administration, and much more consulting services. They have team members who are specialized in and can tackle any problem a customer has. They are employed by private sector companies and government entities.

While I cannot discuss much of what is worked on in the company, a few notable facts are that they have worked behind the scenes with their government and private sector counterparts on a well-known ransomware attack. They were also involved in a global denial of service (DoS) situation and played a part in a very popular and controversial social media platform congressional regulation case study.

Orientation

Dephiant Consulting's orientation divides the onboarding process into four levels--compliance, clarification, culture, and connection. First few days included sessions on company background, values, missions, engagement opportunities, and missions. The final days of orientation primarily focuses on rules and regulations of the various departments and an overview of the duty responsibilities of each rotation. Before being granted network access, I had to pass a background check, complete onboarding paperwork, and sign an NDA. My unit coordinator/mentor helped me navigate the background check process and request network access on my behalf; followed by the completion of Prevention of Workplace Harassment Training, Computer Safety Awareness Training. I was later assigned a badge and had to attend virtual sessions that were conducted on addressing daily workflow, documentation, presentation skills, and utilization of the various systems, services, and tools. As I transitioned to various roles, my access permissions were granted and/or disabled depending on the assignment; I was

informed that it was to ensure a non-repudiation, separation of duties, and preventing insider threats.

The team has taught me much more than I've learned on my own. Before this internship I was only able to learn about cybersecurity concepts through internet resources, such as the website TryHackMe.com, different videos and books, and the concepts taught to me during my university courses. The opportunity to be an intern has enabled me to grow my skills and knowledge through hands-on experience, interviewing the team leads, and shadowing. I am grateful for the opportunities to engaged with the teams, their objectives, and their tasks. I felt as if I was a contributing part of the teams from the beginning, rather than an outsider or the novice. From the beginning I was informed of the special tasks I'd complete, and the technical skills I were to develop, and I was recognized for all my achievements and how I contributed to the overall mission of the organization.

Management

I have observed that the management teams have a diplomatic/coaching type of leadership. We would have weekly department and section meetings or "huddles" to discuss what was being focused on that week and any new information we had to know. I also had one-on-one sessions with my mentor, they are always collaborative unless there's an immediate need that must take place. I have had exposure to/conversations with the CEO, CISO, CIO, department heads, and colleagues from various backgrounds, agencies, and sectors and I admire their synchronicity and that they all learn from each other. We are told that everyone is a Subject Matter Expert in something so we all must be open to learning from anyone about anything at all times. I also liked that there was a huge emphasis on showing humanity and decency, and that achieving the overall mission trumps titles in this organization.

This internship allowed me to gain a vast amount of knowledge on cybersecurity practices and responsibilities all in a personalized environment. I felt comfortable asking questions and with the many different departments I shadowed I feel that I have developed my skill set dramatically and I have more confidence in applying for a help desk or cyber security analyst after I graduate. I liked that I was able to fully immerse myself in my assignments and I will now be able to comprehend the ever-changing nature of cyber threats in the real world. Every day I've been able to practice communication and collaboration with many different team members and greatly I have greatly improved my problem-solving and technical skills.

Major Work Duties

During my first week at the internship, I was made to sign an NDA so while I will discuss the work I completed in this session, due to the nature of the work I completed I cannot go into specifics. Through my time at Dephiant Consulting I was given many assignments that seemed like my usual course work which I realize was only meant to ensure I had the background knowledge to complete task given further down the line. One of my first and personally one of my favorite assignments involved reading policies. In my university course I was made aware of

many of the industry standards I would need to know and admittedly I did not take the time to read those standards past what was required for assignments. One of my first assignments at this internship had me familiarizing myself with six industry standards, three of which included the NIST cybersecurity framework, ISO standards, and PCI security standards. Though this seemed like monotonous reading on my part I was then able to use this knowledge, with the help of my mentor, to update the security plan on the company based on the services listed on their site with those three standards specifically.

As mentioned in the history section, Dephiant Consulting outsources many of its employees to other entities and doing so requires the employee and those they work with know the risk involved in the cyberspace. One of the assignments I was given involved developing a communication plan. In this assignment I was able to work with a small team of colleagues to develop a security awareness communication plan and I had to give a presentation on cybersecurity. Given the highly certified nature of the company I believe this assignment was more a benefit to my ability to work with others, my knowledge of cybersecurity concepts, and my ability to teach these concepts.

Specific use of skills

Through the internship I learned a lot of technical skills but I was able to bring some skills to the team that I had before. Though much of the work I will be doing post-graduation will be analyzing and sorting security alerts, I was able to use my programming knowledge in my journey. I was able to quickly pick up things such as KQL, which was an entirely new language to me but with my knowledge of C++ and SQL from my college courses I was able to grasp the concept quickly. My knowledge of firewalls and LAN networks allowed me to grasp security concepts quickly as well but through asking question I was able to improve my knowledge of exactly how firewalls worked, I learned how to memorize commonly used port numbers, and I received a more thorough understanding of the TCP model/ OSI layers of which I admitted I struggled to memorize the functions of.

How did the ODU curriculum prepare you for the internship?

My course taken at Old Dominion University were of great help during this internship but there were also many areas where I felt I was learning more than what I brought to the company. The knowledge of network topology was invaluable in grasping concepts such as cloud architecture from the security engineers at the company. I was able to apply my knowledge of firewalls and software such as Wireshark to analyze traffic and while I did not use Wireshark to analyze traffic, the key terms present in traffic I captured in my university courses were relevant in analyzing alerts and finding important information in SIEM security alerts.

When discussing SIEM alerts I bring to the attention of the university the lack of the discussion or use of practical software in the classroom. I learned many things such as Splunk dashboards and I was made aware of software such as ServiceNow being used in the real world and before joining this internship I had no idea what SOC teams did or what a SIEM dashboard was. I

believe these skills are more important to know when securing an entry level job in today's market and will put me above other students who did not have the opportunity to get hands on experience with this software in the classroom.

Objective Fulfillment

One of my primary learning objectives for this internship was to get an overview of cyber security frameworks, policies, procedures, and guidelines. I believe the internship fulfilled this goal by ensuring I understood the policies governing our industry and using those policies in actual assignments.

Another objective for me was to learn how to perform cyber threat intelligence integration on newly identified threats and vulnerabilities. I believe this internship greatest succeeded in helping me fulfilled this objective. As mentioned in the curriculum section, I entered this internship with the knowledge of firewalls and programs such as Wireshark. Leaving this internship, I will be aware of other tools used such as Splunk SOAR and other SIEM dashboards that use tools such as endpoint security to analyze threats past anything Wireshark can do on its own.

My final learning objective was to learn to stay updated on cyber threats and best security practices. While I did learn how to scan for vulnerabilities in a system and had weekly meetings that kept me up to date on security practices, most of what I learned on how to stay updated came from asking my colleagues how they stay up to date. I feel like this objective was fulfilled more by the people working in the company and not the company itself.

Motivations/Discouragements/Challenges

Through the internship I gained an abundance of new knowledge on cybersecurity practices and techniques. The most exiting aspect of this internship was the fact that I got to network with leading executives and like-minded peers. I was able to learn so much about the industry and I believe I have left a mark on the company. Talking to my colleagues about how they got into cybersecurity, hearing their stories of coming from completely different fields, any unconventional routes they took, and the struggles and doubts they faced really motivated me to stay in this career path.

I cannot say I had many discouraging aspects in this internship. As mentioned in the introduction, this internship was highly customized as so I would be introduced to multiple aspects of the industry and such the work done was not disheartening but instead, I was invited to reach out for help when needed and to use my mentor. If I had to choose the most disheartening moment it had to be when I was assigned an assignment where I had to reach an Apache log file and I could not find the line that showed an intrusion had occurred. I was forced to ask for help and while that may make some disheartened, I instead just felt happy to improve my log analyzation skills.

The most challenging aspect of my internship was definitely when I had to analyze security alerts. I was given simulated challenges in the company network and there were times where I struggled to find adequate enough information to pass judgment on an alert. There were also times where I followed the correct procedure on the analyzation process but was told I forgot to do a specific step and I realized how challenging an analyst's job actually is and how much of a difference the simplest step can make in protecting a network's defenses.

Recommendation for future interns

For students looking to intern here in the future I recommend being willing to ask lots of questions. This company has a great community/culture, and they are willing to listen to all of your concerns and will never put you down for it. I highly recommend mastering the most common ports and protocols and how they are used in networks as it will make the analyzing assignments drastically easier. I would also recommend coming with an open mind as you will be introduced to a plethora of cybersecurity roles and while many students have an idea of what they want their career to be post-grad, you may find that you enjoy doing the work of another role.

Conclusion

My internship at Dephiant Consulting Inc. was overall a very enlightening, educational, and enjoyable experience. Through hands-on learning I have been able to advance my threat detection, policy making, command-line usage, and many more cybersecurity skills. Engaging with industry professionals and the assignment given helped solidify my desire to pursue this career field. The mentorship I received and the collaborative culture at Dephiant Consulting helped meet my learning objectives. I am now confident in my skills, and I believe I am prepared to secure my first entry level cybersecurity job and I am ready to pass on this knowledge. Completion of this internship marks a monumental check off of one of my graduation requirements and the beginning of my post-graduate life. I will use the knowledge learned here to better understand and be able to contribute more to classroom discussions, lectures, and assignments.