Internship: The Ducats Group

William Redman

CYSE 368

Summer 2024

Table of Contents

Introduction

I decided to intern with the Ducats Group, a business consulting company, to gain practical experience in cybersecurity within a consulting environment. This internship presented a unique opportunity to enhance my technical skills in cybersecurity while also learning about various aspects of business operations, especially in the consulting domain. My goal was to get my foot in the door in the cybersecurity field and understand the broader context of how businesses operate and succeed, especially in the cybersecurity and IT space. Additionally, I aimed to improve my client communication abilities to effectively convey complex technical information in an accessible manner, which is very important, especially when you move up the ranks.

My specific learning outcomes included enhancing my technical skills through hands-on experience, understanding the practical application of cybersecurity measures within different business environments, and improving my ability to communicate effectively with clients. The internship at Ducats Group provided a platform for me to work on real projects, interact with experienced professionals, and contribute meaningfully to the company's operations. Gaining work experience through this internship was also a strategic step toward securing a full-time job. This paper provides an overview of my internship experience, detailing the projects I worked on, the skills I developed, and the insights I gained.

The Beginning of the Internship: Company Dexcription

The Ducats Group is a premier consulting firm specializing in C-suite advisory and strategic business consulting. Our primary focus is assisting private equity companies with their acquisitions and providing day-to-day advisory services to support their operations. This includes high-level strategic guidance and oversight in various aspects of business and operations, not just cybersecurity. For example, I worked on the cybersecurity side of an HVAC roll-up project, where small HVAC companies were brought together under one umbrella, requiring comprehensive business and operational oversight that included implementing effective cybersecurity policies and technologies.

Founded in 2017, the Ducats Group has established itself as a leader in delivering innovative solutions and strategic guidance to its clients. Our primary services include C-suite advisory, strategic planning, mergers and acquisitions support, and business optimization. We cater to a diverse client base, including private equity firms, small to medium-sized businesses, and large corporations, helping them navigate complex business environments and achieve their objectives. While the company's primary offerings are big-picture advisory services, my role as an intern was focused on the technical side, specifically in vulnerability and network security. This involved implementing and managing cybersecurity measures to protect our clients' IT infrastructure, ensuring their operations run smoothly and securely. The Ducats Group prides itself on integrating IT and cybersecurity measures with broader business strategies, providing holistic

support that drives growth and efficiency. The Ducats Group helps clients achieve long-term success by combining technical expertise with strategic advisory.

Internship Onboarding

The onboarding process at the Ducats Group was thorough and personalized, ensuring that I was well-prepared for my role. During the initial week, I shadowed my mentor, who provided a comprehensive overview of the company's structure, operations, and business model. I learned about the various companies we collaborate with and the specific services we offer to our clients, including high-level C-suite advisory, strategic consulting, and IT and Cybersecurity solutions. The company's effort to understand my background and previous experience was an essential aspect of the onboarding process. They asked me about my experience and combined it with on-the-job training to determine the tasks and projects that best suit my skills and interests. This empowering approach demonstrated the company's commitment to leveraging individual strengths for optimal performance.

During this foundational period, I was introduced to the specifics of my role, which primarily involved vulnerability and network security. I identified a significant gap in our vulnerability scanning process, particularly in how the results were stored and accessed. The existing system, using ConnectSecure, only allowed us to view the most recent scan results, which needed to be improved for tracking progress over time. I proposed and implemented a new system for organizing and storing scan results to address this issue. I created a series of folders and spreadsheets designed to archive monthly results comprehensively. This organizational method enables us to present a clear and detailed progress report to our clients, showcasing improvements and areas that need attention. By systematically saving the results, we can now provide a historical perspective crucial for strategic decision-making and demonstrating the effectiveness of our services. This initiative enhanced our internal processes and highlighted the importance of continuous improvement and proactive problem-solving in consulting. I am proud of my contribution in these first 50 hours and look forward to further refining my skills and positively impacting the company and its clients.

Use of Cybersecurity Skills

During my internship at the Ducats Group, I worked directly under the Chief Information Security Officer (CISO), who offered CISO advisory services to multiple companies we advise. My role was to assist him with day-to-day tasks that would otherwise take up too much of his time, freeing up his schedule for more strategic activities. The CISO has over 20 years of IT security experience and has worked at multiple Fortune 500 companies, providing a wealth of knowledge and insights that greatly benefited my learning experience. In addition to the CISO, I worked under our Vice President of Cloud Services, who managed all Microsoft products like Entra and Microsoft 365 (M365). His previous experience working for Microsoft made him incredibly knowledgeable and a valuable mentor. His expertise in cloud services and enterprise solutions

offered me an in-depth understanding of cloud architecture, migration strategies, and security considerations.

Although I did not work directly under our Networking Manager, I frequently communicated with him, as security and networking are closely related. He managed a team in the Philippines, and it was fascinating to meet them remotely and learn about networking and Filipino culture. Their assistance was invaluable, and it broadened my perspective on global collaboration. I also coordinated with individuals in the business operations space, such as our CEO and COO. They worked directly with private equity firms to drive success in their investments. While this was not my primary role, I had the opportunity to sit in on meetings and coordinate with them, gaining practical business experience. This exposure to high-level strategic planning and business operations complimented my technical work, providing a well-rounded internship experience.

Projects during the Internship

Throughout my internship at the Ducats Group, I was involved in several significant projects and tasks that contributed to both the company's and the client's success. These projects enhanced my technical skills and provided valuable insights into the practical application of cybersecurity measures in a consulting environment.

One of the primary areas of focus during my internship was the vulnerability scanning process. I identified a significant gap in how the results were stored and accessed. The existing system, using ConnectSecure, only allowed us to view the most recent scan results, which needed to be improved for tracking progress over time. I proposed and implemented a new system for organizing and storing scan results to address this issue. I created a series of folders and spreadsheets designed to archive monthly results comprehensively. This organizational method enabled us to present a clear and detailed progress report to our clients, showcasing improvements and areas that needed attention. By systematically saving the results, we could now provide a historical perspective crucial for strategic decision-making and demonstrating the effectiveness of our services.

Continuing the scanning program, I discovered a vulnerability in one of our websites, specifically an open port 21. Recognizing the potential security risk, I quickly contacted the support team responsible for the server hosting our website and successfully had the port to enhance our security posture. This experience taught me the importance of swift action in cybersecurity. Additionally, I met with various managers, including the Networking Manager and the Cloud Director, gaining valuable insights into network monitoring, incident response, cloud architecture, and security considerations.

I advanced the scanning program by initiating monthly scans to ensure our records remained current and comprehensive. Collaborating closely with the networking team, I gained hands-on experience with Cisco Meraki, a powerful network management and security tool. Meraki allowed for efficient monitoring and control of network devices, which was pivotal for

ensuring robust security protocols. Alongside Meraki, I utilized ConnectSecure to generate detailed graphs and insights, providing a comprehensive view of network activity. To effectively communicate our efforts and results to clients, I created a PowerPoint presentation showcasing how our network security measures were blocking unauthorized users and protecting client networks.

During the internship, I was involved in two significant events: the migration from Mimecast to Microsoft 365 (M365) and a cybersecurity incident involving a client's payroll system. The migration project required intense pricing negotiations with Mimecast and careful planning to transition to M365's enhanced in-house functionalities. Observing these negotiations taught me the importance of assertive communication and strategic compromise. The cybersecurity incident highlighted the critical importance of two-factor authentication (2FA). Despite previous recommendations, the client had resisted implementing 2FA, but the breach underscored its necessity, leading to its eventual adoption.

I assisted in setting up a portal for employee logins using open-source software. This project involved conducting a thorough vulnerability scan and reviewing the open-source code to ensure security. We also tested the software in a virtual machine (VM) environment to confirm its functionality before live deployment. This process emphasized the importance of security measures and thorough testing in software deployment. Additionally, I engaged in an ERP rollout for a client using SAP, gaining hands-on experience with ERP software. This exposure highlighted the challenges of implementing such a comprehensive system. I also dealt with a worldwide Microsoft outage affecting one of our largest clients. This experience highlighted the importance of disaster recovery plans and quick response to minimize downtime.

The final phase of my internship focused on enhancing email security by setting up DMARC, DKIM, and SPF protocols for clients and transitioning existing clients to DMARCLY. I coordinated with DMARCLY customer support to set up accounts, overseeing all our clients' email security. Although DMARC technology initially confused me, I gradually better understood its importance in securing business emails. Additionally, I worked on a BI dashboard project with Resultant, revising our third-party vendor questionnaire to ensure it suited the project's requirements. We met with the Resultant to review the questionnaire and ensure all security measures were addressed. Lastly, I participated in a roundtable meeting with our clients and their associates, discussing various IT security scenarios and conducting training sessions to enhance their understanding of cybersecurity.

Overall, these projects were essential to the company's operations, contributing to improved security measures and client satisfaction. They provided a comprehensive learning experience, allowing me to apply my cybersecurity knowledge in practical settings and develop valuable skills that will benefit my future career.

My Education at Old Dominion University

My education at Old Dominion University (ODU) provided a solid foundation of knowledge that was essential for my internship at the Ducats Group. Basic networking and IT security courses gave me the fundamental skills needed to start the job. For example, my experience creating the vulnerability scanning program was directly related to the training I received in my cyber operations class. This class equipped me with the skills to conduct vulnerability scans and interpret the results, enabling me to implement a comprehensive system for organizing and storing scan results at the Ducats Group.

Additionally, my AWS class at ODU gave me practical experience with cloud technology. Although we used Entra during my internship, the concepts and skills I learned in the AWS class were similar and greatly aided my understanding of cloud architecture and security. This background allowed me to quickly adapt to working with Entra and other cloud services managed by our VP of Cloud Services.

While ODU prepared me well in many areas, I had yet to encounter specific technologies and systems, such as SAP and DMARC, during my coursework. However, the baseline information on IT security that I gained at ODU allowed me to adapt to these new technologies quickly. My ability to understand and apply security principles in various contexts was a testament to the solid theoretical grounding provided by my university education.

Old Dominion's Curriculum and the Internship

In addition to the technical skills, ODU's curriculum emphasized the importance of continuous learning and problem-solving, which were crucial in my role. Whether I learned about cloud architecture from our VP of Cloud Services or understood the intricacies of email security with DMARC, the foundational knowledge from ODU enabled me to approach these challenges with confidence and curiosity.

The practical application of the skills I learned at ODU and the new knowledge I gained during my internship reinforced the relevance and importance of my academic training. This experience has not only solidified my understanding of cybersecurity principles but also highlighted the areas where I need to continue learning and growing.

My internship at the Ducats Group successfully fulfilled the learning outcomes I had set at the beginning of the program, which included enhancing my technical skills in cybersecurity, understanding the practical application of cybersecurity measures within different business environments, and improving my client communication abilities. One of my primary goals was to enhance my technical skills through hands-on experience. This was achieved through various projects, such as creating a comprehensive vulnerability scanning program and gaining hands-on experience with tools like Cisco Meraki and ConnectSecure. These projects allowed me to apply my knowledge in real-world settings, deepening my understanding of network security, vulnerability management, and IT infrastructure. Additionally, working on setting up DMARC,

DKIM, and SPF protocols and transitioning clients to DMARCLY provided further technical learning opportunities. Although I had yet to encounter these specific technologies in my coursework, the foundational knowledge I gained from my classes enabled me to adapt and learn quickly.

What do I take away from this experience?

Understanding the practical application of cybersecurity measures was another significant objective. The internship provided numerous opportunities to see how cybersecurity principles are implemented in a consulting environment. For instance, working on migrating from Mimecast to Microsoft 365 (M365) and addressing a cybersecurity incident involving a client's payroll system demonstrated the complexities and challenges of implementing and maintaining robust security measures in dynamic business contexts. These experiences underscored the importance of proactive security strategies and swift response to incidents.

Improving my client's communication abilities was also a key learning outcome. Creating and presenting a PowerPoint presentation to clients, which showcased our network security measures and their effectiveness, helped me develop the skills to convey complex technical information in an accessible and reassuring manner. Additionally, coordinating with DMARCLY customer support and participating in meetings with Resultant and clients further enhanced my ability to communicate effectively with various stakeholders. These interactions were invaluable in teaching me how to articulate cybersecurity concepts and strategies to non-technical audiences, ensuring they understood our work's importance and impact.

Overall, the internship at the Ducats Group not only met but exceeded my learning outcomes. The combination of technical projects, practical applications, and client interactions provided a comprehensive learning experience that significantly contributed to my professional development. This experience has equipped me with the skills and confidence to pursue a career in cybersecurity consulting and has solidified my commitment to continuous learning and improvement.

The most motivating aspect of my internship at the Ducats Group was the opportunity to contribute meaningfully to the company's security efforts and see the tangible impact of my work. Implementing a new system for organizing vulnerability scan results and observing its positive impact on client reporting was particularly rewarding. Collaborating with experienced professionals, such as our CISO and VP of Cloud Services, and learning from their vast knowledge and expertise was incredibly inspiring. The practical experience gained through hands-on projects like setting up DMARC, DKIM, and SPF protocols and transitioning clients to DMARCLY provided a strong sense of accomplishment. Additionally, the exposure to high-level strategic planning and business operations, such as meeting with the CEO and COO, offered invaluable insights into the broader business context.

Conversely, the most discouraging aspect of the internship was encountering the complexity of specific technologies and processes that needed to be covered in my coursework, such as SAP and DMARC. Although I was eventually able to grasp these concepts, the initial learning curve was steep and sometimes frustrating. Additionally, the repetitive nature of some administrative tasks, like completing third-party security questionnaires, could have been more engaging.

The most challenging aspect was mastering the technical details of email security protocols and balancing multiple projects simultaneously. Despite having a basic understanding, the intricacies of DMARC, DKIM, and SPF required significant effort to comprehend fully. Time management and prioritization skills were essential in handling various tasks and ensuring timely project completion.

Recommendations for Future Interns

For future interns, I recommend familiarizing themselves with basic cybersecurity concepts and tools before starting. A solid understanding of vulnerability scanning, network security, and cloud services will benefit greatly. Additionally, gaining knowledge of SAP and DMARC protocols can provide a head start. Strong organizational and time management skills will also be crucial for managing multiple projects effectively. Lastly, being open to learning and adaptable to new technologies will significantly enhance the internship experience.

My internship at the Ducats Group has been an incredibly enriching experience that has significantly shaped my understanding of cybersecurity and business operations. The main takeaway from my internship is the importance of integrating technical expertise with strategic business insights to provide comprehensive solutions. The hands-on projects and collaborative environment allowed me to apply my academic knowledge in real-world settings, enhancing my technical skills and practical understanding of cybersecurity measures.

This experience will significantly influence the remainder of my college time at ODU. It has highlighted the areas where I need to focus my studies and motivated me to seek additional coursework and practical opportunities in cybersecurity and business strategy. The internship has reinforced the value of continuous learning and staying updated with the latest industry trends and technologies.

Looking ahead, my internship at the Ducats Group has solidified my interest in pursuing a career in cybersecurity consulting. The exposure to various aspects of business operations and the opportunity to work closely with experienced professionals have provided valuable insights into the consulting industry. This experience has equipped me with the skills, confidence, and determination to pursue a career path that combines technical expertise with strategic advisory, ultimately aiming to contribute to the success and security of businesses.