Kael Cepak

4/17/2026

Supervisor: Charles Cepak

Company: KALO

Teresa Duvall

CYSE 368 Spring 2026

Introduction

I decided to pursue an internship with KALO because I wanted to gain hands-on experience in cybersecurity that extended beyond the classroom and into a real professional environment. While my coursework at Old Dominion University provided me with a strong theoretical understanding of cybersecurity concepts, I recognized that applying those concepts in real-world scenarios is essential for truly mastering the field. Cybersecurity is not just about understanding systems and vulnerabilities; it is also about making decisions under pressure, communicating risks effectively, and adapting to constantly evolving threats. This internship offered me the opportunity to explore those aspects while contributing to meaningful work.

Before beginning my internship, I identified several key learning objectives outlined in my Memorandum of Agreement (MOA). First, I wanted to gain a deeper understanding of how cybersecurity is implemented in a business setting, particularly in environments involving international communication and potential exposure to foreign threats. Second, I aimed to improve my ability to communicate cybersecurity concepts to individuals without a technical background, as this is a critical skill in any professional setting. Third, I sought to develop the ability to evaluate cybersecurity technologies not only from a technical perspective, but also in terms of business value and regulatory compliance. These objectives guided my approach throughout the internship and allowed me to measure my progress.

KALO is a cybersecurity-focused organization that works on evaluating and implementing secure technologies, particularly those that may be used in government or defense-related environments. The company emphasizes integrating cybersecurity into overall business strategy, ensuring that security is considered in every aspect of decision-making. Its work often involves assessing new technologies, analyzing their potential applications, and ensuring compliance with strict standards. This makes KALO a unique environment where cybersecurity intersects with business, policy, and innovation.

My initial orientation at KALO was relatively informal, which required me to quickly adapt and take initiative. I was introduced to my responsibilities, which included cybersecurity training, network monitoring, and research projects. At first, I found the lack of structured onboarding to be somewhat challenging, but it also encouraged me to become more independent and proactive. This early experience set the tone for the rest of my internship, as I learned to take ownership of my work and approach each task with a problem-solving mindset.

Management Environment

The management environment at KALO was notably different from what I initially expected, particularly when compared to larger, more traditional corporate structures. Instead of a rigid hierarchy with multiple layers of management, KALO operates with a more streamlined and direct approach. This allowed for open communication between myself and my supervisor, making it easier to ask questions, share ideas, and receive feedback. From the beginning of my internship, I noticed that communication was informal yet purposeful, which created a comfortable learning environment while still maintaining professionalism. This structure encouraged active participation and made it easier for me to feel engaged in the organization's work.

One of the most valuable aspects of the management environment was the balance between guidance and independence. My supervisor provided direction when necessary, particularly when introducing new concepts or assigning projects, but I was also given a significant amount of autonomy in completing my work. For example, when conducting research on cybersecurity technologies or analyzing potential risks, I was often expected to explore the topic independently and present my findings. This approach required me to take initiative and develop my own problem-solving strategies, which ultimately strengthened my confidence and ability to think critically. While this level of independence was initially challenging, it became one of the most beneficial aspects of the internship, as it prepared me for the expectations of a professional cybersecurity role.

Another defining characteristic of the management environment was the emphasis on trust and accountability. I was treated as a contributing member of the organization rather than just an intern observing from the sidelines. This meant that my work was expected to be accurate, thorough, and meaningful. Knowing that my contributions had real value motivated me to approach each task with a high level of responsibility and attention to detail. It also reinforced the importance of professionalism, as I understood that my work could directly influence decision-making within the organization.

In addition, the collaborative nature of the environment allowed for continuous learning and improvement. Feedback was provided in a constructive manner, which helped me refine my work and better understand expectations. Rather than simply being told what to do, I was encouraged to think about why certain approaches were effective and how they could be improved. This focus on learning rather than just task completion made the internship more educational and engaging. Overall, the management environment at KALO was highly effective in fostering both personal and professional growth, as it combined independence, accountability, and support in a way that encouraged development.

Major Work Duties and Projects

Throughout my internship, I was responsible for a variety of tasks that evolved in both complexity and scope over time. One of my primary responsibilities was training my supervisor on cybersecurity awareness and best practices. This involved explaining concepts such as phishing attacks, password management, social engineering tactics, and multi-factor authentication. While these topics are fundamental in cybersecurity, teaching them required me to translate technical knowledge into practical advice that could be easily understood and applied. This responsibility was critical to the organization because it directly addressed one of the most common sources of security vulnerabilities: human error. By improving awareness and encouraging better security habits, my work helped reduce the likelihood of successful attacks.

Another significant duty was monitoring network activity while my supervisor conducted business with foreign entities. This task introduced me to the real-world application of cybersecurity principles in an operational environment. I was responsible for analyzing communication patterns, identifying potential risks, and ensuring that secure communication methods were being used. This required constant attention to detail and the ability to recognize subtle indicators of suspicious activity, such as unusual email behavior or unexpected changes in communication patterns. Given the risks associated with international business, including targeted phishing campaigns and potential exposure to foreign threat actors, this responsibility played an important role in maintaining the security of the organization's operations.

In addition to these tasks, I worked on a research project involving Goldilock and its product, Firebreak. This project required me to evaluate the technology from multiple perspectives, including its technical reliability, potential profitability, and compliance with military standards. I analyzed how the product functions, its strengths and limitations, and its potential value to the organization. This project was particularly important because it contributed to decision-making regarding whether the company should pursue a partnership or investment in the technology. It also required me to think beyond purely technical considerations and evaluate the product in terms of business impact and regulatory feasibility.

Another notable aspect of my internship was my involvement in discussions related to the development of secure AI software. While this was not my primary responsibility, it provided valuable exposure to the process of integrating cybersecurity principles into emerging technologies. The focus of these discussions was on ensuring that security is built into the system from the beginning, rather than added as an afterthought. This experience gave me insight into the importance of proactive security design and the challenges associated with securing new technologies.

Overall, my work duties during the internship were diverse and provided a comprehensive view of cybersecurity in practice. Each task contributed to the organization in a meaningful way,

whether by improving security awareness, protecting ongoing operations, or supporting strategic decision-making. At the same time, these responsibilities allowed me to develop a wide range of skills and gain a deeper understanding of the field.

Use of Cybersecurity Skills and Knowledge

During my internship, I had the opportunity to apply many of the cybersecurity skills and concepts I had learned in my coursework while also developing new competencies through hands-on experience. Prior to the internship, I had a solid understanding of foundational topics such as network security, encryption, system vulnerabilities, and risk management. These concepts provided a useful starting point, but applying them in a real-world environment required a deeper level of understanding and the ability to adapt to dynamic situations. One of the key differences I observed was that real-world cybersecurity often involves incomplete information and uncertainty, requiring careful analysis and judgment rather than relying solely on predefined solutions.

One of the most significant ways I applied my cybersecurity knowledge was through monitoring network activity and identifying potential threats. This task required me to analyze patterns in communication, recognize anomalies, and assess whether certain behaviors could indicate a security risk. While my coursework had introduced me to the concept of threat detection, applying it in a live environment helped me understand the nuances involved in distinguishing between normal and suspicious activity. This experience improved my analytical skills and reinforced the importance of vigilance in maintaining system security.

Another important application of my cybersecurity knowledge was in training my supervisor on best practices. This required me to take complex technical concepts and present them in a way that was accessible and practical. For example, instead of simply explaining how phishing attacks work, I focused on how to recognize suspicious emails and what actions to take in response. This experience not only reinforced my own understanding of these concepts but also helped me develop strong communication skills, which are essential in professional cybersecurity roles. Being able to effectively communicate risks and solutions is just as important as understanding the technical aspects of security.

In addition to applying existing knowledge, I also developed new skills during the internship, particularly in the area of compliance and regulatory frameworks. Learning about the Risk Management Framework (RMF) and Department of Defense requirements introduced me to a side of cybersecurity that I had not previously explored in depth. This required me to learn how to interpret complex policies and apply them to real-world systems. It also expanded my

understanding of cybersecurity beyond technical defense, emphasizing the importance of governance, documentation, and continuous monitoring.

Overall, my internship allowed me to both apply and expand my cybersecurity knowledge in meaningful ways. It helped me bridge the gap between theory and practice, develop new skills, and gain a more comprehensive understanding of the field. This experience has been instrumental in preparing me for a future career in cybersecurity, as it has provided both practical experience and a deeper appreciation for the complexities of the profession.

ODU Curriculum Preparation

My coursework at Old Dominion University provided a strong and necessary foundation for my internship, particularly in areas such as network security, system vulnerabilities, and basic risk management concepts. Classes in cybersecurity introduced me to how attacks occur, how systems are structured, and the importance of protecting data through techniques such as encryption and access control. These concepts were extremely valuable when I began my internship because they gave me a baseline understanding of the technical environment I was working within. Without this academic preparation, it would have been much more difficult to contribute meaningfully to tasks such as monitoring network activity or analyzing potential cybersecurity risks.

At the same time, my internship revealed that classroom learning alone does not fully prepare students for the complexities of real-world cybersecurity work. In many cases, the scenarios presented in class are controlled, structured, and focused primarily on technical problem-solving. In contrast, my internship required me to deal with ambiguous situations where there was no clear right answer. For example, when monitoring communications or evaluating potential threats, I often had to rely on judgment rather than a defined procedure. This highlighted the importance of critical thinking and adaptability, skills that are difficult to fully develop without practical experience.

Another area where the internship expanded my understanding beyond the classroom was in the application of cybersecurity frameworks and compliance standards. While I had been introduced to the idea of frameworks such as risk management models, I had never worked with them in a practical, applied setting. During my internship, I was exposed to the structured nature of compliance requirements, particularly in relation to government and Department of Defense standards. This experience demonstrated that cybersecurity is not just about implementing protective measures, but also about documenting and validating those measures to meet regulatory expectations.

Overall, my experience showed that my education at Old Dominion University provided a strong theoretical base, but that hands-on experience is essential for developing a complete understanding of cybersecurity. The internship reinforced many of the concepts I learned in class while also introducing new challenges that required me to think beyond what I had previously encountered. This combination of academic and practical learning has been critical in preparing me for a future career in cybersecurity.

Learning Outcomes and Objectives

The learning objectives I established at the beginning of my internship served as a valuable framework for evaluating my progress throughout the semester. One of my primary goals was to gain a deeper understanding of how cybersecurity is implemented in a business environment. Through my work at KALO, I was able to see firsthand how security decisions are influenced by factors such as cost, efficiency, and organizational priorities. This experience helped me understand that cybersecurity is not just a technical discipline, but also a strategic one that must align with broader business goals.

Another objective I set for myself was to improve my ability to communicate cybersecurity concepts to non-technical individuals. This was an area where I saw significant growth during my internship. Early on, I realized that simply explaining technical details was not effective when working with individuals who did not have a cybersecurity background. Over time, I learned to focus on the practical implications of security risks, such as financial loss or operational disruption, which made my communication more impactful. This skill will be extremely valuable in my future career, as cybersecurity professionals must often act as a bridge between technical teams and business leadership.

My third objective was to develop the ability to evaluate cybersecurity technologies from multiple perspectives. This goal was largely achieved through my research on the Firebreak product and other related tasks. I learned how to assess not only the technical capabilities of a system, but also its potential profitability, reliability, and compliance with regulatory standards. This holistic approach to evaluation is essential in professional settings, where decisions must consider both technical and business factors.

While I made significant progress in achieving my objectives, the internship also showed me that learning is an ongoing process. There are still many areas where I can continue to improve, particularly in gaining deeper expertise in compliance frameworks and advanced cybersecurity techniques. However, I feel confident that I have built a strong foundation that will support my continued growth in the field.

Most Motivating Aspects

One of the most motivating aspects of my internship was the opportunity to work on real-world cybersecurity challenges. Unlike classroom assignments, which are often hypothetical, my work at KALO had direct implications for actual business operations. This made the experience more engaging and meaningful, as I could see the impact of my contributions. Knowing that my work played a role in improving security and supporting decision-making gave me a strong sense of purpose and motivation.

Another motivating factor was the variety of tasks I was able to work on throughout the internship. From training my supervisor on cybersecurity awareness to conducting research on advanced technologies, each assignment presented new challenges and learning opportunities. This variety kept the experience interesting and allowed me to develop a broad range of skills. It also helped me discover which areas of cybersecurity I find most engaging, such as analyzing emerging technologies and understanding their potential applications.

The opportunity to work on forward-looking projects, such as secure AI development, was particularly exciting. Being involved in discussions about how to design secure systems from the ground up gave me insight into the future of cybersecurity. It also reinforced the importance of staying current with technological advancements, as the field is constantly evolving. Overall, these motivating aspects of the internship strengthened my interest in cybersecurity and confirmed my desire to pursue a career in this field.

Most Discouraging Aspects

While my internship was overall a positive experience, there were certain aspects that I found discouraging at times. One of the most significant challenges was the complexity of compliance-related tasks. Learning about Department of Defense requirements and frameworks such as RMF required a high level of attention to detail and often involved interpreting complex documentation. At times, this process felt overwhelming, especially when I encountered unfamiliar terminology or concepts that required additional research.

Another discouraging aspect was the lack of structured guidance in some areas of the internship. Unlike traditional classroom environments, where instructions are clearly defined, I often had to rely on self-directed learning to complete my tasks. While this ultimately helped me develop independence and problem-solving skills, it could be frustrating when I was unsure of the best approach or had limited direction.

Additionally, there were moments when progress felt slow, particularly when working on research-intensive tasks. Analyzing cybersecurity technologies or compliance requirements often involved reviewing large amounts of information, which could be time-consuming and mentally demanding. Despite these challenges, I recognized that they were a natural part of the learning process and ultimately contributed to my growth as a cybersecurity professional.

Most Challenging Aspects

The most challenging aspect of my internship was learning how to balance technical analysis with business considerations. In many cases, cybersecurity decisions cannot be made based solely on technical performance. Instead, they must also take into account factors such as cost, usability, and regulatory compliance. This required me to think more broadly and consider how different elements interact within an organization.

Another major challenge was developing the ability to communicate effectively with non-technical stakeholders. Translating complex cybersecurity concepts into language that is easy to understand requires a different skill set than simply understanding the material. I had to learn how to focus on the practical implications of security risks and present information in a way that is relevant to the audience. This was particularly challenging at first, but it became easier with practice and experience.

Additionally, adapting to the level of independence required in the internship was initially difficult. Without a highly structured environment, I had to take responsibility for managing my time, setting priorities, and ensuring that my work was completed accurately. Over time, this challenge helped me develop greater confidence in my abilities and improved my ability to work independently.

Recommendations for Future Interns

Based on my experience at KALO, there are several important recommendations I would offer to future interns who are considering or preparing for this opportunity. One of the most important things to understand is that this internship requires a high level of independence and self-motivation. Unlike highly structured internship programs, where tasks and expectations are clearly outlined step-by-step, this environment expects interns to take initiative, seek out information, and actively engage in problem-solving. Future interns should be prepared to work in a setting where they may not always be given detailed instructions, and instead must rely on their ability to think critically and adapt to new challenges. Developing this mindset before

starting the internship will make the transition much smoother and allow interns to contribute more effectively from the beginning.

In addition to independence, having a strong foundation in core cybersecurity concepts is essential. Future interns should be comfortable with topics such as network security, common cyber threats, and basic risk management principles. Understanding concepts like phishing, social engineering, encryption, and authentication methods will be particularly useful, as these are directly applicable to many of the tasks performed during the internship. While it is not necessary to be an expert in every area, having a solid baseline knowledge will allow interns to focus more on applying concepts rather than learning them from scratch. This preparation will also help interns feel more confident when engaging with real-world cybersecurity challenges.

Another key recommendation is to develop strong communication skills, particularly the ability to explain technical concepts in a clear and relatable way. A significant portion of the internship involves interacting with individuals who may not have a technical background, which means that being able to translate complex ideas into practical advice is extremely important. Future interns should practice communicating cybersecurity risks in terms of real-world impact, such as financial loss, operational disruption, or reputational damage. This skill not only improves effectiveness during the internship but is also highly valuable in the cybersecurity field as a whole.

It is also important for future interns to familiarize themselves with cybersecurity frameworks and compliance standards, especially those related to government or Department of Defense requirements. While it is not expected that interns will have an in-depth understanding of these frameworks beforehand, having a basic awareness of concepts such as the Risk Management Framework (RMF) will provide a significant advantage. This knowledge will make it easier to understand tasks related to compliance and regulatory requirements, which can otherwise be complex and time-consuming to learn.

Finally, I would encourage future interns to approach the experience with curiosity and a willingness to learn. This internship offers exposure to a wide range of topics, from cybersecurity awareness to emerging technologies such as artificial intelligence. Taking advantage of these opportunities and actively seeking out new knowledge will maximize the value of the experience. By staying engaged, asking questions, and taking initiative, future interns can gain not only technical skills but also a deeper understanding of the cybersecurity field and its real-world applications.

Conclusion

My internship at KALO has been a transformative experience that has significantly shaped my understanding of cybersecurity and my future professional goals. Throughout the course of the semester, I was able to move beyond theoretical knowledge and engage directly with real-world challenges that required critical thinking, adaptability, and effective communication. From training my supervisor on cybersecurity awareness to analyzing emerging technologies and navigating complex compliance requirements, each aspect of the internship contributed to my growth both technically and professionally. This experience has reinforced the idea that cybersecurity is not just about protecting systems, but about understanding how technology, people, and business processes interact.

One of the most important takeaways from this internship is the realization that cybersecurity is inherently interdisciplinary. It requires a combination of technical expertise, strategic thinking, and the ability to communicate effectively with a wide range of stakeholders. I have learned that successful cybersecurity professionals must be able to evaluate risks, make informed decisions, and adapt to changing circumstances. This understanding has given me a more comprehensive perspective on the field and has helped me appreciate the complexity of real-world cybersecurity challenges.

This internship will have a lasting impact on the remainder of my time at Old Dominion University. It has motivated me to seek out additional opportunities for hands-on learning and to continue developing my skills in areas such as compliance, risk management, and emerging technologies. I now have a clearer understanding of the topics I want to focus on in my future coursework and projects, and I am more confident in my ability to apply what I have learned in a professional setting. Additionally, this experience has encouraged me to take a more proactive approach to my education, recognizing that continuous learning is essential in a field that evolves as rapidly as cybersecurity.

Looking ahead, this internship has also influenced my future career planning by providing a clearer picture of what it means to work in cybersecurity. It has shown me the importance of adaptability, problem-solving, and communication in professional environments. It has also reinforced my interest in pursuing a career in cybersecurity, particularly in areas that involve government compliance and emerging technologies. I now feel better prepared to enter the workforce, with a stronger foundation of knowledge and a greater sense of confidence in my abilities.

In conclusion, my internship experience has been both challenging and rewarding, providing me with valuable insights and practical skills that will benefit me throughout my career. It has helped me grow as a student, a professional, and an individual, and it has confirmed my commitment to the cybersecurity field. The lessons I have learned and the experiences I have gained will continue to influence my academic journey and professional development long after the internship has ended.

Table of Contents