Final Paper

By

Ritz Carr

Student Researcher in the Naval Research Enterprise Internship Program with Navy Surface Warfare Center (NSWC) Corona RS20E4

Summer 2023

Submitted for Partial Completion in CYSE 368

School of Cybersecurity

Old Dominion University

TABLE OF CONTENTS

INTRODUCTION

I applied for this internship through the Naval Research Enterprise Internship Program (NREIP) and was assigned directly to Naval Surface Warfare Center (NSWC) Corona. I did not know exactly what I would be doing, let alone the fact there was a small division of Corona in Norfolk and not California! It was my only offer, yes, but I precisely aimed for government-related internships that required some form of security clearance. I knew attaining a security clearance would be a good leg up in my package for a job after college. Not only that but working with a government entity and learning its risk management process would also make me a beneficial candidate.

At the beginning of the internship, my mentor and I outlined five learning objectives, mainly focusing on three given some constraints:

- Understand the DoD Risk Management Framework. Become familiar with each step, workflow, and process within our organization's implementation of RMF practices.
- Gain a foundational understanding of SEIMs tools and their application in our enterprise environment. Become a Subject Matter Expert (SME) in Cyber Threat Hunting through innovative and independent research.
- Understand the mission purpose of NCTE (Navy Continuous Training Environment) organization and its network, NETTN (Naval Enterprise Tactical Training Environment) from a security and compliance perspective.

We dabbled a little in the other two but focused more on these three objectives given the environment and time of year.

BACKGROUND OF NSWC CORONA

The beginning was a slow start, especially the first week when I did not have a laptop. So, I spent the first week observing what my mentor did on a daily basis. Take meeting calls, check and make tickets, go to other departments within our division, and ask questions about current projects. I found strong communication skills and proactive-ness are required for an environment such as Corona.

NSWC Corona is a division under the Naval Sea Systems Command (NAVSEA) and acts as the Navy's independent assessment agent regarding its warfighting capabilities. Part of the mission we help fulfill in our department is engineering and maintaining the Fleet's Live Virtual Constructive (LVC) training environment for the Navy Continuous Training Environment (NCTE) used by the Navy for virtual training exercises to train their sailors in warfighting

capabilities and readiness. Our division here in Norfolk is the Range Systems Engineering (RSE) division. Within that are smaller departments like the Cybersecurity Department RS20E4 where I am.

In the RSE division, we primarily maintain and operate the Fleet's tactical training ranges and network environment (Navy Enterprise Tactical Training Environment, NETTN)'s LVC capabilities, in addition to Naval surface and air range system technology solutions (NSWC Corona, 2023). The Cybersecurity Department is responsible for assuring all projects and solutions have cybersecurity measures and posture in mind. Given the past few years of NCTE transitioning to an Enterprise and connecting all ranges to one standard, things have been difficult to understand and communicate. Communication had been and still is sometimes vague and difficult with other departments, especially between government oversight and contractors, a work culture of its own.

Within our RSE division, there are four departments: Enterprise Services, Engineering, NETTN, and Cybersecurity; the latter two fall under the command of the Chief Information Technology Officer (CITO) as support. Both departments usually have managers. But as of late, there is an exception to this as no Cybersecurity manager is present, so the NETTN manager heads both departments. My mentor and I coordinate with her often for my mentor's needs and my progress and questions to further my experience seeing how people at her level work.

My mentor works as an Information Security Software Engineer (ISSE) and sometimes assists with project management and Assessment and Authorization (A&A). Often, though, A&A, ISSEs, and Information Security Software Officers (ISSOs) will work with one another and contractors to get projects done and pushed up for authorization, the main goal. Of course, we also work with other departments like engineering. I have found this type of workplace interesting, seeing a wide variety of jobs and projects that may have potential interest to me outside of my research. The organization of it all is still hard to grasp aside from theoretical matters, especially given one manager oversees two departments. I know a situation like this is more challenging than normal atmospheres in government workplaces. Working at this point in Corona's growth makes me feel a little more prepared for a potential government career.

THE INTERNSHIP

As for the organization, interns here are a special case. The work done here is something that, for an intern like me, I would be thrown right to the wolves. This environment requires a complex understanding of the organization and the Risk Management Process (RMP), limiting my activities. However, my mentor knew this as she was an intern at Corona. While my work wasn't essential to the business, the research I did still required me to interact with people from different roles and departments.

It was a blessing in disguise of sorts. I would research something I knew nothing about while sitting in on meetings and talking to others about topics I was researching to learn more

and understand our mission. It would also expose me to new roles that might interest me. I also knew that this division often did not have interns, so interacting with me was new for them too.

There were some minor duties that I helped out with regarding project efforts. One was checking the port connectivity in conference rooms and logging it for submission to our manager or researching the supplemental guidance for security controls needed in a project submission package. Not a lot, but it was simple enough for me to do and help the team.

For the first time, I had to learn all the required knowledge on the job. My basic knowledge of foundational cybersecurity concepts, especially fresh, was helpful when researching my topics of System Information and Event Management (SIEM) systems, Cyber Threat Hunting (CTH), and the Risk Management Framework (RMF). I would say the main skill I used that I improved immensely was how to research and write a better research paper from what I have learned so far as an undergraduate; in fact, I would say that is the best experience I have gotten out of this internship that I know will be of use to me when I return to class and in writing future papers.

As for SIEMs, CTH, and the RMF, I would say this all loosely ties into cyber defense and compliance from a federal point of view that further helps my goal of being considered for government work out of college but also in understanding how a Federal organization works in the cybersecurity arena and will also be useful if I end up in the business or private sector.

The curriculum enabled me to enter this position prepared to learn about SIEMs, CTH, and the RMF. The only topic I knew beforehand was the RMF, something we heavily rely on here. One of my introductory cybersecurity classes had covered NIST SP 800-37 (RMF) enough for me to have a small grasp on it, preparing me to learn about it in depth. This included the NIST SP 800-53r4, the RMF controls.

An area I believe I was somewhat prepared in but not to the extent I would have liked, would be researching and writing academic papers. My mentor was a current doctoral student who knew how to write graduate-level papers and pushed me to learn and write in a graduate-level style. While it was difficult to get used to, I know I am ahead of my peers in writing and researching academia. I could have learned about writing some aspects of a research paper better in my previous classes, though.

One big connection I made between prior knowledge from college and CTH (ultimately something I could not use) was with Routine Activities Theory (RAT) in criminology and concepts in cybersecurity such as MITRE ATT&CK Techniques; Tactics, Techniques, and Procedures (TTPs); Common Vulnerabilities and Exposures (CVEs); and Control Correlation Identifiers (CCIs). The excerpt for this is in Appendix A.

Given the nature of this internship and how spontaneous projects can be for my mentor, some objectives were not achievable.

The first few weeks were dedicated to research and understanding the inner workings of the environment. I would learn extensively about CTH, SIEMs, the role of SIEMs in CTH, and SIEM features and capabilities. I researched the DOD RMF steps regarding our RMP, focusing on the 'Implementing Controls' step and its controls, as it was relevant to the work of my mentor as an Information Security Software Engineer (ISSE).

Throughout my entire time, I learned about NCTE and the NETTN slowly. Eventually, I would build an overall picture of their mission and purpose regarding the security and compliance perspective. Watching my mentor work and sitting alongside her in meetings would help me accomplish this. This would also help me meet my first objective of understanding the RMF and the process as packages moved from step to step throughout the 12 weeks I was there.

As for the unachieved objectives, situations such as needing a new laptop or network issues would take time away from trying to do other things like focusing on scheduling, funding, scoping, etc. I would not say I am super versed in security engineering, but with my mentor's expertise, I learned enough to understand her role.

THE HIGHS AND LOWS

I would say the motivating aspects of the internship were when I began piecing things together regarding the NCTE or the process of things at work. Or knowing the research and writing I was doing was spot on and conceptual but needed to be written in a more technical style. Another would be when we got to do in-person meetings or small tours; anything that was outside of my small cubicle and had me interacting with others was always exciting.

A few small but still motivating experiences I had where when I was asked to complete small tasks that my mentor or manager could not complete due to their busy schedules. One would consist of checking port connectivity in the conference rooms to later have more network ports installed. I would create and maintain an excel spreadsheet of each port and what room they were in. My other task would also include excel. I was given a set of controls for a project and I would need to record each control’s supplemental guidance. Since our main security controls explorer was down, I would have to find another source with Control Correlation Identifiers (CCIs) that also provided supplemental guidance to their application. I remembered that when I first began my research, I found a source that was similar to the Explorer that was running and I was able to use that while cross-referencing controls to the NIST SP 800-53r4 to check my answers. I was happy to have found a solution to getting around the Explorer being down and completing the task!

I was lucky to travel with a Technical Project Manager to the Navy Dare Bombing Range in North Carolina, 2-3 hours south of Virginia Beach. While I learned more about different parts of NSWC Corona and the functions of the bombing range, my favorite part was being out of the cubicle in a place where the nearest highway was miles away and only nature could be heard.

Where butterflies were plentiful and alligators swam freely. It was beautiful but a little disheartening that a bombing range was in the middle of an alligator wildlife refuge; however, they had an on-site environmentalist who gave safety briefings on wildlife, assuring nature was cared for.

Another exciting aspect was near the end when my work was finally coming together. The majority of my writings acted as notes for the research I was doing to ultimately write my final paper for the internship. At the time of writing all those 'notes,' I thought it would be in my final paper. Not until my mentor started steering me in the direction of the topic I would actually write about did I realize it was the Learning Phase of the internship. Discouraging at first, but I understood that it was necessary and helpful for future research.

Discouragement came when I first started. I had begun a month before all the other interns and was a fresh new face in the office. Naturally, I had hardly anyone to socialize with. When the other interns did start, I did not get many opportunities to connect with them either. They were able to do multiple full-day tours and after-work activities together that were non-work-related. It was probably the most discouraging and difficult part of the internship, being the only intern that would make days long and often uneventful. But I knew my hard work would pay off: I had gotten to work the longest out of all the interns.

It also came when I would have to start a new paper, realizing all my written content were notes yet again. A lot of notes, often 14 or more-page papers! I eventually grew accustomed to the cycle, knowing it was necessary and better to have more content then less. In fact, in the end, I would go back to the notes I still had to pick and sculpt pieces for my final paper. Some large sections would only become a line in the final paper while others would stay or disappear completely. It was definitely a new experience researching a topic I would have to learn from a blank slate before writing an in-depth paper on it all in 12 weeks.

The challenge arose when my first laptop needed a new motherboard. I would then spend the entire week trying to get another working laptop. One destroyed hard drive and 21 hours of updates later would I finally have a new and functioning laptop on a Friday afternoon, just as the week ended. This happened 9 weeks into my time and I could only salvage a limited number of files saved to Microsoft Teams. The rest had been wiped from the drive upon replacement of the motherboard.

It did not put me back, though. That was the turning point in my writing when I would finally start writing the draft for my final, piecing all the concepts together into the bigger picture. It was daunting, knowing my work was lost, but it felt like a transition or turn in my journey. Not the turn I was expecting!

RECOMMENDATIONS AND PREPARATIONS

My main recommendation to interns in my internship specifically: there will be journeys in life that you will have to do alone and it will be difficult but sometimes necessary to accomplish the end goal. If you are interning alongside other interns, socialize! Get to know your peers and work alongside them proudly.

If you are serious about your major, do not be afraid to ask questions, no matter how small! While you are there to accomplish your assigned goal, the internship is for you to gain experience and explore potential career paths. Your mentor and people around you are there to help and will only help if you ask, so use your resources wisely. One question or experience can open a door to a whole new world and impact your path.

The preparations needed before starting this internship would be considered extensive by some, as a security clearance is required. Before applying, potential candidates should know if they can attain one. Questionnaires and interviews need to be conducted, making the process lengthy. Travel may be required, too, so be prepared.

CONCLUSION

Overall, I really enjoyed my internship. I feel it was necessary to dictate the career options for my major as I was unsure of what I wanted to do after college. I still am, but this gave me a lot of insight into a potential choice. However, I knew taking a government-related internship would be vital to good job prospects for those requiring a security clearance, influencing my search for job openings as I near my graduation.

The cyber environment I worked in during my internship was related to the field that fits my major, as it was not very technical but more policy and compliance-focused. It was a new perspective requiring a different mindset but provided me with a potential career path.

The remainder of my semesters are very open to different paths regarding classes I can take. Right now, it may be an unofficial minor in law. Another path may be starting a Master's degree in Cybersecurity, something my mentor inspired me to look into. ODU even has an RMF and NIST compliance cybersecurity concentration for the Master's program that would be perfect for working at NSWC Corona.

Lastly, in Appendix B I will include an excerpt from the final paper I wrote during my time at Corona. It is about SIEMs, their role as CTH tools, policies needed for the system to be DOD-compliant, and implications in implementation.

REFERENCES

NSWC Corona. 2023. "Corona Division Departments". *NAVSEA.* https://www.navsea.navy.mil/Home/Warfare-Centers/NSWC-Corona/What-We-Do/

APPENDIX A

UNDERSTANDING THE BEHAVIOR OF ADVERSARIES

In order to be an innovative and combative threat hunter, it is important to understand the motivations and behavior of our adversaries.

In criminology, there are many theories to describe the behavior of offenders and why they offend. One well-known theory, Routine Activities Theory (RAT) developed by Lawrence Cohen and Marcus Felson in 1979. This theory requires three elements in order for an attack/crime to occur: a motivated Offender (O), a suitable target/threat (T), and the absence of a capable guardian (G); compiled as OTG (Averdijk, 2011).

How does this apply to Cyber Threat Hunting (CTH)?

Inspired by the scholarly papers "Linking Common Vulnerabilities and Exposures (CVEs) to MITRE ATT&CK Techniques" and "A Criminology-Based Simulation of Dynamic Adversarial Behavior in Cyberattacks", it became evident that OTG can be applied the TTPs, CVEs, and CCIs that we use in CTH:

> O, a motivated offender, is represented by the TTPs used by our adversaries
>
> T, a suitable target or threat, is represented by the CVEs in our system
>
> G, the absence of a capable guardian, is represented by the CCIs and other controls we use to mitigate CVEs and TTPs.

Without the presence of all three of these elements, an attack cannot happen; however, that does not mean one is imminent! The end goal is to mitigate as many threats as possible with controls to eliminate the T and G in RAT. Without suitable targets (CVEs) and a capable guardian (CCIs and controls), our system will not be attractive to offenders (adversaries using TTPs) (Aouad, et al., 2021) (Temple University, 2017).

REFERENCES

Aouad, Lamine. Kuppa, Lamine. Le-Khac, Nhien-An. Aug, 2021. "Linking CVE's to MITRE ATT&CK Techniques." *ACM Digital Library*. https://dl.acm.org/doi/fullHtml/10.1145/3465481.3465758.

Averdijk, Margit. 2011. "Routine Activities Theory: Definition of the Routine Activity Approach to Crime." *Criminology Web*. https://criminologyweb.com/routine-activities-theory-definition-of-the-routine-activity-approach-to-crime/.

2017. "EAGER: Collaborative: A Criminology-Based Simulation of Dynamic Adversarial Behavior in Cyberattacks." *Temple University - Of The Commonwealth System of Higher Education & National Science Foundation*. https://www.nsf.gov/awardsearch/showAward?AWD_ID=1742747&HistoricalAwards=false.

APPENDIX B

INTRODUCTION

According to the InfoSec Institute, there are two approaches to strengthening cybersecurity posture: proactive and reactive. Cyber Threat Hunting (CTH) is an example of the proactive approach for network defense. The reactive approach is associated with detection as the trigger is the catalyst for defense. This is accomplishable by a System Information Event Management (SIEM), which alleviates the difficulty monitoring entire network for irregularities. The DOD's process for implementing new tools, systems, and concepts is rigorous and abundant, requiring an Authorization To Operate (ATO) and continuous compliance with DOD policy. With this, the system will have permission to operate on the network. SIEMs are difficult systems to integrate due to implications such as reliance on human factors such as advanced threat intelligence and correlation rules (Cinque et al., 2018). Both proactive and reactive approaches can be used in concert to make a resilient network.

The goal of this proposal is to understand the importance of evaluating what our network requires for a SIEM to be implemented and consistently compliant with DOD policy. The policy helps with making the SIEM an effective network defense and monitoring tool. In the Navy Enterprise Tactical Training Network (NETTN), how can a SIEM be implemented while abiding by DOD policy to make it an effective network defense tool?

PURPOSE

LogRhythm is the current SIEM used by the NETTN. Over the past few years, NETTN has shifted to an enterprise scale that has increased the volume of data ingestion. The current configuration of LogRhythm cannot support this increase nor data storage requirements and Data At Rest (DAR). It is no longer DOD-compliant, requiring NCTE to search for another SIEM solution increasingly scalable. Without LogRhythm being DOD-compliant, network defense fails to be optimal.

Despite selecting a new SIEM, the implementation process is different from when LogRhythm was acquired. This is due to a multitude of factors including those that outdate LogRhythm for our network. To achieve an ATO, SIEM capabilities and implications must be understood in addition to organizational policies.

SCOPE

The SIEMs solution needs to be adaptive to the NETTN environment, not possible with the current solution, LogRhythm. It is unable to meet all organizational and DOD requirements given the new configuration of NETTN.

The scope of this study is limited to Naval Surface Warfare Center (NSWC) Corona Controlled Unclassified Information (CUI), the World Wide Web (WWW), and the professional testimony of personnel in the Range System Engineering Division of NSWC Corona. Due to the rapid evolution of the cybersecurity field, sources besides policies are limited to, at most, five years before this document.

INTENDED AUDIENCE

This research is intended for those with knowledge of federal cybersecurity compliance and SIEM solutions apart of Navy Continuous Training Environment (NCTE)'s NETTN and other Federal institutions to consider possible implications in implementing a SIEM such as Splunk Enterprise Security (ES) following DOD policy.

REFERENCES

Cinque, Marcello; Cotroneo, Domenico; Pecchia, Antonio. Oct, 2018. "Challenges and Directions in Security Information and Event Management (SIEM)." *IEEE*. https://ieeexplore.ieee.org/abstract/document/8539170.