**Internship Report (Port of Virginia)**

**Stephen Antwi**

**CYSE 368-** **Summer Class, 2023**

**Old Dominion University**

**Professor Karahan**

Table of Contents

[Introduction 3](#_Toc140779855)

[Beginning of Internship 3](#_Toc140779856)

[Overview of Port of Virginia 3](#_Toc140779857)

[Initial Orientation/Training 4](#_Toc140779858)

[Management Environment 5](#_Toc140779859)

[Work Duties, Assignments, and Projects 6](#_Toc140779860)

[Application of Cybersecurity Knowledge 7](#_Toc140779861)

[ODU Curriculum 8](#_Toc140779862)

[Evaluation of Internship 9](#_Toc140779863)

[Motivating Aspects of the Internship 9](#_Toc140779864)

[Discouraging Aspects of the Internship 10](#_Toc140779865)

[Challenging Aspects of the Internship 10](#_Toc140779866)

[Recommendations 10](#_Toc140779867)

[Conclusion 11](#_Toc140779868)

[References 11](#_Toc140779869)

Internship Report

# Introduction

Currently, I am doing my internship at the Port of Virginia, in Norfolk, Virginia. The Port of Virginia is the third biggest container port on the East Coast. I am working in the Cybersecurity department. I decided to complete an internship in the Port of Virginia because of three main reasons. First, considering that the Port of Virginia is one of the largest ports on the East Coast it would prepare me to work in a large organization in the future by exposing me to the cybersecurity issues facing large organizations. The Port of Virginia can allow me to gain valuable work experience that can help me to secure a job in a large organization.

Second, I was attracted by Port of Virginia`s core values – innovation, helpfulness, fortitude, accessibility, mindfulness, and sustainability. I desire to embody these values because they would help me succeed in my career. Third, I decided to do my internship at the Port of Virginia because this organization can offer me a chance to network. Taking into account that one of the reasons for internships is to immerse one in opportunities, I decided to complete my internship at Port of Virginia because it has a good reputation for introducing interns to various individuals who may help me find employment later.

The first learning outcome or objective I hope to achieve in my internship is applying the knowledge I have learned about monitoring Microsoft Sentinel/Microsoft Defender. The other learning objective I desire to achieve in my internship is learning to review applicable cyber threats intelligence from cyware. Another learning objective I hope to achieve is familiarizing myself with Microsoft's approach to detecting, protecting, and responding to cyber-attacks. The fourth learning objective I hope to realize is to develop my ability to audit cybersecurity policies.

This paper highlights the beginning of my internship at the Port of Virginia, a description of the management environment at the internship, and my work duties, assignments, and projects. It also includes a discussion about the use of knowledge or skills of cybersecurity in the internship and how the ODU curriculum prepared me for the internship. Besides, the paper highlights how the internship fulfilled the four learning objectives. A description of the most motivating, discouraging, and challenging aspects of the internship is also included. Lastly, the paper highlights the recommendations for future interns in this internship.

# Beginning of Internship

## Overview of Port of Virginia

The history of Port of Virginia can be traced back more than 400 years. In the past, it was operated by the city government of Virginia. However, in 1952 it became an autonomous agency belonging to the Commonwealth of Virginia. This port moves cargo via first-class facilities into and out of the nation. It has six terminals and occupies 1,864 acres. This port shelters the largest naval base globally. It also shelters the biggest shipbuilding and repair base in the world. Besides, this port handles bulk trade cargo and coal for export. In tonnage, the Port of Virginia is the second biggest port on the United States East Coast. It is also the third biggest port in terms of container volume. The port provides fifty-foot channels, outbound and inbound. It is a strategic hub port serving many shipping lines providing services to and from Virginia connected to more than 200 nations internationally (Virginia Port Authority, 2023).

The major customers the Port of Virginia targets are local and international commercial ships shipping goods into and out of the United States. It offers services to international containers, tankers, bulk, breakbulk, and roll-on/off vessels. The port offers direct services to more than forty-five nations. It also offers indirect services to at least 200 nations. Some of the major trading partners of the Port of Virginia include Germany, China, the Netherlands, and Belgium (Hampton Roads Alliance, 2023).

## Initial Orientation/Training

I was warmly welcomed into the organization on the first day. During the initial orientation, I had a chance to learn more about the Port of Virginia, its mission, vision, and values. Also, I learned the organization`s structure as well as the functions of each department. The other essential information about the organization I was given included its procedures, policies, and operations. Besides, HR reviewed with me the working hours, dress codes, and safety requirements and regulations. My responsibilities were defined, and I was taught some terminologies that would help me in undertaking my duties as Security Operations Center (SOC) analyst. In addition, the communication platform or channel that I used throughout the internship was outlined.

Moreover, I was introduced to the staff members working in the Cybersecurity department. A special arrangement was also made for me to meet and interact with my mentor. I was also given the necessary resources I require to work successfully at the Port of Virginia. Another important thing to mention is that during the initial orientation, I was allowed to determine the learning and professional growth goals I hope to achieve.

The initial training, I received focused on training me according to the actual work culture. I was given weekly projects that helped me learn the technicalities associated with the SOC assistant position. The goals I was given were clear and I later learned that they were set according to the organization`s benchmarks. I was also trained in the Risk Management Framework (RMF). This framework split cyber risk management into 6 major phases – categorizing the system, selecting security controls, implementing security controls, assessing security controls, authorizing the system, and monitoring security controls.

The Port of Virginia made a great initial impression on me since I was warmly welcomed by the HR, given an initial orientation of the organization and a complete tour of various departments before joining other interns. One of the things I noted was that all the employees were exemplifying the organization`s values and were supportive, an aspect I liked. After the initial orientation, I managed to log in and began working. Everything I needed to work such as e-mail, settings, and programs worked efficiently and seamlessly. Therefore, the organization was ready to onboard me, and it ensured I comprehended that it valued and welcomed me to be part of its workforce. The warm reception made me tentatively conclude that I made the right decision to join the Port of Virginia. Regarding my initial impressions about the internship, I must attest that I felt glad that I could achieve my objectives since the organization's management and employees seemed welcoming and ready to assist. The first impressions made me feel the urge to work hard during the internship for the organization to reciprocate the warm welcome. Also, the welcome instilled confidence in me that I could complete my internship at the organization.

# Management Environment

The management environment at the internship is good. The managers and supervisors at various levels in the leadership hierarchy are friendly and seem to follow the CEO’s leadership management. They highly value relationship development with the people working under them since they understand that having good relations with the employees is essential for the organization`s prosperity. At the Cybersecurity department, the head of the department always focuses on building good relations with all the staff working in this department. When I first joined this department, I noticed that the head of the Cybersecurity department was free to all the employees since they could interact freely. I later learned that the department maintains an open-door policy because it strives to enhance employee-management relationships. During the departmental meetings, the head of the department reminds us about the organization`s mission, vision, and values. This is done deliberately because if everybody in the department comprehends the organization`s directional strategies they can recognize how their efforts contribute to the organization`s success. Also, the head of the department reminds us about the need to be innovative to secure the organization`s network infrastructure from cyber-attacks.

Besides, my supervisor plays a key role in developing my skills as a SOC analyst. Through training and offering directions to complete assigned tasks, my supervisor helps me learn and complete my work. Before the supervisor assigns me any duty, he trains me on how to perform it. The training helps me to complete the tasks efficiently and faster. It also encourages me to undertake my assignments diligently. Whenever I experience challenges the supervisor is always ready to help me. In addition, the supervisor has been motivating me during my internship, an aspect that makes me work hard in executing my responsibilities. The motivation I have been receiving includes being allowed to make extensive contributions to the department and getting assigned larger projects. Apart from this motivating me, they offer me a chance to apply my skills and hence, prove myself. The communication within the department and the organization is superb. Good communication can be attributed to a good employee-management relationship. The head of the Cybersecurity department communicates the directives from the organization`s top managers to all employees in the department and reports feedback.

Generally, the good management environment of Port of Virginia is highly effective for my internship because it has positively impacted my stay at the organization and my progress in accomplishing the objectives of the internship. I can attest that the management approach makes me feel part of the organization, encouraging me to do my best in completing the assignments. Equally essential to underscore is that because of good management, I have been exposed to exciting work assignments within my job function. Also, the good management of Port of Virginia facilitates the establishment of networking opportunities with other employees, helping me build helpful relationships. Additionally, the two-way communication style method provides an effective way of communication since I can share my concerns about my work and project with my supervisor and other employees. Therefore, a good management environment helps me to collaborate with other employees in the organization in carrying out my tasks. The collaboration has also helped me to learn how to perform certain tasks accurately and effectively.

# Work Duties, Assignments, and Projects

One of my major work duties is reviewing incidents to keep the Port of Virginia safe from cyber-attacks. This duty encompasses collaborating with other security analysts in detecting and responding to information security incidents. Also, reviewing incidents entails defining the review`s objectives and scope. It is essential to note that the scope includes the risk type, severity, and duration. Apart from defining the review, the incident review involves gathering and analyzing the relevant data from the incident. In reviewing the incidents, I usually collect data from logs, reports, alerts, emails, tickets, surveys, and feedback from the external sources, affected parties, and the incident response team. I have learned how to use charts, diagrams, tables, and timelines to document, organize and correlate gathered data. Also, incident review encompasses identifying and prioritizing findings and generating and implementing recommendations. Reviewing incidents is necessary for the organization because it helps the security team know some of the cyber threats the organization faces so that it can lay out adequate measures to prevent them.

The other major work duty I performed at my internship is monitoring the organization`s security using Microsoft Sentinel and Microsoft Defender. With the help of the reference architecture, I have learned how to use Microsoft Sentinel and Microsoft Defender to monitor the organization`s security configuration and Azure Stack workloads. This duty is necessary to the organization because it helps in securing the organization`s network system. Monitoring the network system is a critical function to detect and prevent security cyber threats. The third major duty I perform in my internship is reviewing all quarantine emails. In performing this duty, I usually follow the Microsoft 365 Defender guidelines for finding and viewing the quarantine emails. Reviewing the quarantine emails is important because it helps protect the organization`s network infrastructure and users from malicious programs sent through email.

The fourth major work duty I perform is reviewing applicable cyber threat intelligence from cyware. Cyber threat intelligence refers to the evidence-based knowledge or information of the existing or emerging threat`s resources, capabilities, motives, and goals (Cyware Labs, 2023). This duty is crucial because it provides an appropriate context for the organization`s security team to better comprehend and pinpoint the adversaries in addition to informing decisions concerning responding to security hazards. The fifth major work duty I perform as an intern is to monitor Virtual Private Network (VPN) traffic and add pattern correlation documents. Typically, performing this duty involves monitoring and optimizing the organization`s VPN performance by analyzing the VPN logs. Some of the software applications I employ include SolarWinds, Splunk, and LogRhythm. Monitoring VPN traffic is important because it helps in assessing the effectiveness of the organization`s VPN in securing incoming and outgoing traffic.

The sixth and last major work duty I performed in my internship is reviewing policies, updates, and tracking. This duty entails scanning the macro environment for any changes in the regulation of information technology and determining if the organization`s policies comply with the policies. It also entails identifying some of the updates that should be made to the existing policies to enhance their effectiveness in addressing security issues facing the organization. Performing this duty is imperative in the organization because the organization needs to ensure its security policies are up to date. That way, the organization will efficiently secure its infrastructure.

Concerning my major assignments and projects, I am currently working on a project about MITRE ATT&CK Framework. MITRE ATT&CK stands for MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK). It refers to “a curated knowledge base that tracks cyber adversary tactics and techniques used by threat actors across the entire attack lifecycle” (CrowdStrike, 2022). In other words, MITRE ATT&CK Framework is a model an organization uses for virtual adversary behavior, mirroring different phases of an enemy`s attack lifecycle as well as the platforms they target. This model is used to strengthen the security position of an organization. The techniques abstraction and tactics in this framework offer a taxonomy of the individual adversary activities known as the offensive and defensive phases of cybersecurity. So, the MITRE ATT&CK Framework offers an organization the appropriate categorization level for adversary action together with techniques to defend against it. The MITRE ATT&CK Framework has three primary components. These components include tactics designating short-term, tactical adversary goals, techniques relating to strategies adversaries realize tactical objectives, and adversary`s documented techniques (Trellix, 2023). Therefore, MITRE ATT&CK Framework helps the security teams to better fathom the adversaries facing the organization, assess the organization`s defenses, and harden security.

The MITRE ATT&CK Framework project is necessary to the organization because of the following reasons. Firstly, it helps the organization to carry out security gap analysis as well as plan security enhancements. It also helps the organization to strengthen its cyber threat intelligence and speed up Alert Triaging and Investigation. Moreover, the MITRE ATT&CK Framework helps in creating more realistic situations for adversary emulations and reading team activities. In addition, the framework assists in evaluating the maturity of SOC. Furthermore, the framework is important in enhancing communication with the stakeholders.

# Application of Cybersecurity Knowledge

Before the internship some of the skills or knowledge of cybersecurity I had included risk analysis, information security, handling and responding to security incidents, and security audit. Regarding risk analysis, I possess some knowledge about identifying, managing, and mitigating cyber security risks. Concerning information security skills, I possessed some knowledge to protect electronic data from unauthorized access. Pertaining to handling and responding to security incidents, I had some insights into handling and responding to the security incidents. I could identify, manage, record, and analyze information security threats. Besides, I could analyze and manage security information and event management tools. Lastly, before joining the Cybersecurity department of the Port of Virginia I knew some cybersecurity regulations, defining how to safely use the internet and safeguard organizations from becoming cybercrime victims.

The first skill I had to learn on the job is how to use the Microsoft approach to detect, protect and respond to cyber-attacks. My supervisor trained me on how to use various Microsoft security services to detect, protect, and respond to cyber threats. Some of the Microsoft security services I learned include Microsoft Defender for Office 365, Microsoft Defender for Identity, Microsoft Defender for Cloud Apps, and Microsoft Defender for Endpoint. I also received training on RMF, a template for identifying, eliminating, and minimizing risks. RMF is an important guideline for protecting an organization`s information systems. Its components include identifying the organization`s risks, measuring and assessing risks, mitigating risks, risk reporting, and risk governance. During the training on RMF, I learned how to prepare a formal risk management strategy, categorize identified risks, select security controls, implement selected security controls, assess the efficacy of security controls, authorize continuous use of security controls, and monitor security controls. Additionally, I was trained in phishing attacks. Considering that phishing is a significant challenge in cybersecurity I was trained on what to look for to detect this cyber threat. Some of the warning signs I learned during the training include urgency, site security, incorrect URL, and display of low-resolution images. Most importantly, I learned how to protect the organization and myself from phishing.

My job experience in the content area has improved significantly. The internship has helped me to acquire the necessary experience to undertake various tasks as a SOC analyst. It has exposed me to the real environment, allowing me to apply what I have learned so far in performing assigned duties. The internship has introduced me to the day-to-day rigors as well as tasks that one completes under my area of specialization. In other words, the job experience has allowed me to polish my skills by allowing me to gain practical experience.

# ODU Curriculum

The ODU curriculum equipped me with the necessary theoretical knowledge I need to perform most of the assigned tasks as a SOC analyst. It covered nearly all the most important concepts that touch on the duties of a SOC analyst. Therefore, the ODU curriculum adequately prepared me for the internship. Also, considering that the ODU curriculum is comprehensive it helped me to avoid experiencing much anxiety about what to expect at the Port of Virginia in the Cybersecurity department.

The knowledge I learned in school and the knowledge or skills used at the internship are highly related. So far, I have not identified any skill used at the internship that conflicts with what I learned in school, a demonstration that what I learned in school is what is applied in the corporate environment. For example, the procedures involved in identifying and minimizing security risks to the Port of Virginia`s network system are similar to what I learned in school. Also, the way this organization reviews the cyber threats, incidents, and audits policies is the same as what I covered in class.

The internship experience has reinforced what I learned in school. By allowing me to put into practice the different concepts I learned in school, the internship has helped me to enhance my understanding of these concepts. It has also given me a good opportunity to build on what I had learned in school by applying it in the business environment. Also, the SOC analyst internship has supplemented my knowledge of Cybersecurity with hands-on experience. Moreover, I have gained some helpful knowledge concerning the work of the SOC analyst I believe has enabled me to be a better professional. In this connection, it is pertinent to pinpoint that over the internship period, I have received some training on performing certain duties that accompany the role of a SOC analyst. The training has helped me to gain new knowledge or insights of performing some duties. For example, I have gained valuable insights into phishing attacks. These insights would help me to perform my duties at the workplace now and in the future. I have also learned more about how to use Microsoft Defender for Office 365.

Some experiences during my internship at the Port of Virginia have revealed new concepts, techniques, or skills that I have not yet encountered in school. For example, the use of Microsoft Sentinel at the Port of Virginia to monitor the organization`s security configuration revealed to me new techniques that I have not experienced in my academic journey. My supervisor introduced me to the unique architectural design and workflow the organization uses in monitoring its security system. I was able to learn how the organization applies Microsoft Sentinel and adapts it to fit its requirements. The other experience that has revealed new techniques to me is the monitoring of a VPN network. This experience enabled me to learn how to apply SNMP to monitor the organization`s VPN traffic, connections, and users. I also learned how to perform various test failures like authentication and self-test failures.

# Evaluation of Internship

The internship helped me fulfill all my four of my objectives. First, it has helped me fulfill my first objective of wanting to apply my knowledge about monitoring Microsoft Sentinel and Microsoft Defender. The internship offered me an opportunity to apply the two in defending the Port of Virginia against cyber threats. In applying Microsoft 365 Defender I was able to gain deeper insights into the nature of the threats the Port of Virginia faces and how the organization can harden its security protocols. I was also able to apply Microsoft Sentinel and it helped me detect security alerts, recognize threats, and perform proactive hunting. This security solution also enabled me to gather security data across the entire organization from servers, cloud, apps, devices, and users.

Regarding the second objective I was able to learn how to review applicable cyber threats intelligence from cyware with the help of my supervisor. The supervisor helped me learn different types of cyber threat intelligence, such as strategic threat intelligence, tactical threat intelligence, technical threat intelligence, and operational threat intelligence.

Concerning familiarizing myself with Microsoft's approach to detecting, protecting and respond to cyber-attacks I was able to fulfill this objective by learning from some of the employees working in the Cybersecurity department. These employees explained to me how to use Microsoft 365 Defender to investigate and respond to security threats. I learned how Microsoft 365 apps and services generate alerts when they detect malicious activity. Also, I fulfilled the third objective by learning how to analyze security incidents, alerts, and accompanying data to help contain and eradicate cyber threats.

Eventually, regarding the fourth objective I was able to fulfill it by performing audits of cybersecurity policies. I was able to develop my ability to perform audits by learning the various steps one needs to follow to perform a comprehensive audit of an organization`s security policies.

# Motivating Aspects of the Internship

One of the motivating aspects of the internship is the support I receive in completing the MITRE ATT&CK Framework from my supervisor. I was nervous about starting this project when I learned that I was to complete it. Nevertheless, the immense support I have received from my supervisor has driven me to complete some of the milestones of this project. The more I complete more milestones the more I feel motivated to continue with the project. Whenever I encounter some challenges, my supervisor is always ready to aid me. Therefore, my supervisor`s help is one of the most motivating aspects of my internship.

The other most motivating aspect of my internship is that it equips me with invaluable hands-on skills that I need to be fully prepared to enter the job market as a SOC analyst. Although my academic journey has prepared me for the job, the internship has supplemented my knowledge. Therefore, each day I spend at the Port of Virginia in the Cybersecurity department I know that I am learning something valuable that can greatly benefit me in my career.

Another motivating aspect of my internship is that it offers me a chance to watch how experienced SOC analysts perform their work. The internship has allowed me to collaborate with other employees in the Cybersecurity department in performing some assignments. This collaboration has allowed me to learn many new skills and techniques for performing the assignments. Apart from watching how they perform certain tasks I often ask them many questions besides proposing new ideas. That way, I can learn and develop my competence to perform SOC analyst responsibilities.

# Discouraging Aspects of the Internship

The most discouraging aspect of the internship is that sometimes my supervisor forgets that I am new and assigns me some tasks without clarifying to me the directions. Although my supervisor provides feedback sometimes, they fail to make sense to me. This makes me experience challenges in completing the assignments. However, I do not shy away from asking for help from my supervisor because I know it is my right as an intern to ask instead of assuming.

The second most discouraging aspect of my internship is the lack of feedback. Unlike the full-time employees in the Cybersecurity department who are usually scheduled for performance evaluations, sometimes my work is not evaluated. This makes me feel confused and unsure of my work. Whenever I feel that my supervisor has not evaluated my work I do ask if they have some time to look at my work. This approach has helped me to learn more from my supervisor on how to diligently execute the SOC duties.

# Challenging Aspects of the Internship

The most challenging aspect of the internship is that sometimes I am required to perform menial tasks in the department. At first, I used to feel bad performing these tasks, but I later learned that they are important in the process of learning the culture of the organization and its core values. It also dawned on me that mundane tasks are the basis of the organization.

The steep learning curve is another challenging aspect of my internship. Considering that my organization often expects me to participate at a level similar to that of the full-time employees, despite lacking the on-the-job training I sometimes become overwhelmed. However, I have learned to overcome this problem by openly speaking to my supervisor.

# Recommendations

Some of the recommendations for interns aspiring to take the SOC analyst internship include:

* Reviewing the position description to learn about what one expects during the internship.
* Creating the learning objectives for the internship.
* Reviewing the organization`s organizational structure, values, and directional strategies if they are listed on the organization`s website.
* Taking a rational attitude to the learning curve problem can help one overcome some of the challenges of completing an internship in this profession.
* Being assigned mundane tasks should not discourage one from continuing with their internship. Performing such tasks is critical to helping one learn more about the organization`s directional strategies and core values.
* Considering that one might feel overwhelmed in performing the assigned tasks, it is important to persevere during the early phases of the internship. Nevertheless, if the feelings of being overwhelmed persist it is advisable to talk to the supervisor or manager about the issue.
* One should be prepared for their work performance not to be evaluated sometimes because the supervisor might overlook their work. However, if one’s work is often not evaluated they should ask the supervisor to assess their work.

# Conclusion

One of the main takeaway thoughts from my internship experience is that internship is an important part of the learning process because it equips one with hands-on experience. Besides, it allows one to interact with experienced employees, helping one learn how to relate and interact with other employees at the workplace. The other takeaway from my internship experience is that an intern should be open and maintain good relations with their supervisor and other people at the workplace. Being open and maintaining good relations helps one to settle faster and to manage workplace stress.

My internship experience will influence the remainder of my college time by making me focus on learning some of the concepts I have not learned in class but are necessary at the workplace. Also, apart from learning the requisite concepts I will try to build on organizational behavior because this is important to work effectively in an organization. Lastly, my internship experience will help me build my career by taking more cybersecurity-related courses and attending seminars focusing on cybersecurity to acquire more knowledge to meet the demands of this profession.

# References

CrowdStrike. (2022). *What is the MITRE ATT&CK Framework?* crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/mitre-attack-framework/

Cyware Labs. (2023). *What is cyber threat intelligence?* <https://cyware.com/security-guides/cyber-threat-intelligence>

Hampton Roads Alliance. (2023). *Port of Virginia.* <https://hamptonroadsalliance.com/port-of-virginia/>

Trellix. (2023). *What is the MITRE ATT&CK framework?* <https://www.trellix.com/en-us/security-awareness/cybersecurity/what-is-mitre-attack-framework.html>

Virginia Port Authority. (2023). *About the Agency*. Virginia.gov. https://www.virginia.gov/agencies/virginia-port-authority-/