Old Dominion University

CYSE 368: Final Paper

City of Virginia Beach Department of Information Technology
Cybersecurity Internship - Security Operations Center
Supervisor: Robert Branch

Noah Salafranca
April 12, 2025; Spring 2025

Table of Contents

Introduction

As a senior at Old Dominion University, I pursued an internship with the City of Virginia Beach Department of Information Technology. I wanted to gain valuable hands-on experience to follow a career path in cybersecurity. My interest in the technical elements and service aspects of cybersecurity made working with Virginia Beach's cybersecurity team an ideal chance to contribute to the digital security of my community. In addition to gaining work experience, I hoped to deepen my knowledge of security operations, apply what I had learned in class in real-life scenarios, and develop as a young professional in the cybersecurity field.

Initially, I struggled to secure an internship. I applied for numerous internships, but I discovered that several cybersecurity internships were extremely competitive or targeted at students with prior experience. This was often discouraging, and I began to worry about finding an internship that would fulfill the CYSE 368 requirement. Fortunately, with the help of the ODU internship office and some professional networking, I was able to connect with the City of Virginia Beach's Department of Information Technology. After back-and-forth correspondence with Bob Branch, the Chief Information Security Officer (CISO), over winter break, I was interviewed. I learned more about the city's IT infrastructure and cybersecurity team. It was an excellent opportunity for me to assist Bob and the cybersecurity team in their initiatives. This internship experience was much more fulfilling than a credit requirement; it became a significant academic and professional experience in my cybersecurity journey.

My primary learning objectives for this internship were:

1. Learn how to identify, analyze, and respond to cybersecurity incidents.
2. Learn the SOC infrastructure.
3. Develop skills in using network monitoring tools.
4. Participate in vulnerability assessments.

This paper outlines my internship experience from start to finish, detailing the organization, my duties and responsibilities, the skills and knowledge I applied and gained, and how this experience has influenced my academic progress and future career plans. Additionally, it provides reflections and insights into what challenged and motivated me, offers recommendations for future interns, and offers an overall evaluation of what I've learned from this internship opportunity.

Beginning of Internship

The organization where I interned is the Department of Information Technology for the City of Virginia Beach. This department is responsible for maintaining and securing the city's technology infrastructure by "proactively delivering a dynamic and evolving set of core services and innovative technologies that the City and its constituents demand" (Information Technology, n.d.). Virginia Beach relies on a strong and secure IT infrastructure to provide public services across various departments, such as public safety, utilities, emergency services, and public works. The IT department supports various core service areas, including applications, operations, information security, systems support, geospatial information services, data and analytics, and infrastructure.

A specialized team handles the IT department's cybersecurity initiatives, split into two main parts: the Governance, Risk, and Compliance (GRC) team and the Security Operations Center (SOC) team. The SOC team focuses on identifying threats, responding to incidents, and managing triage, while the GRC team works to ensure compliance with cybersecurity frameworks, manage risk, and develop policies. I chose to intern with the SOC team because my interest in the technical side aligned more with its focus. Interning with the SOC team opened my eyes to how the city addresses cybersecurity threats.

I underwent an orientation and onboarding process with supervisors and team members to kick off my internship. I was introduced to Bob, the CISO, Kris, the SOC team manager, and Tatum, the cybersecurity analyst, who was my primary mentor throughout the internship. During the orientation, I was introduced to the team's security tools and applications, including Microsoft Azure, Microsoft Defender, ServiceNow, Splunk, and several OSINT tools. I was also briefed on cybersecurity protocols, the various platforms used, and the security permissions I need to activate to access the security tools and manage incidents.

My first impression of the IT department was overwhelming but exciting. Despite having little professional cybersecurity experience as a student, I received a warm welcome. There was a lot of information to take in from the beginning, especially regarding the tools and terminology, but the team was willing to teach me through the learning process. My first day provided valuable information and hands-on learning through real-world cybersecurity tasks, which helped me quickly adapt to the environment. I was impressed by the team's knowledge, professionalism, and laid-back attitude. Each member had diverse backgrounds and experiences that complemented one another to protect the city's digital infrastructure. From the outset, it became clear that this internship would be a valuable opportunity to challenge me in beneficial ways and enable me to contribute to the team's mission.

Management Environment

The management environment is well-structured and organized. The cybersecurity team has a well-defined hierarchy, yet working with the team is open and collaborative.

- Robert Branch, Chief Information Security Officer
- Kristopher Hava, SOC Manager
- Samuel Flores, Cybersecurity Analyst II
- Tatum Evans, Cybersecurity Analyst I

As an intern, I worked directly under Tatum. Tatum was my primary mentor on a day-to-day basis, who taught me how to perform my duties, helped me manage tasks and prioritize my work, and offered professional feedback on my findings during investigations. Tatum began as a cybersecurity intern for the city and progressed to an entry-level analyst position. Tatum related to my experience and consistently took the time to clarify tools, techniques, and the reasoning behind our tasks. Additionally, Taum graduated from ODU, which was another thing I could relate to her with. Knowing that we shared a similar educational background and she successfully transitioned into the field made her mentorship even more impactful.

My interactions weren't exclusively with the SOC side. I also had the chance to meet Sam, the level II Cybersecurity Analyst on the GRC side of the team. I regularly witnessed how Sam's work with policies, frameworks, and compliance furthered the city's cybersecurity approach. Similar to Tatum, he is also an ODU graduate and is currently pursuing his master's degree. Sam's background showed how professionals in cybersecurity can diversify their skill sets and branch out into other specialties.

Additionally, I communicated regularly with Kris, the SOC team manager, who played a key role in handling incidents and overseeing the day-to-day workflow. Before taking on a leadership position, Kris had experience as a cybersecurity analyst with the city and as a SOC analyst at Domino's. His technical expertise provided a strong foundation for security operations, and his approachable leadership style encouraged interns to ask questions and seek guidance. Kris emphasized building my skill set and often pointed me toward the best certifications and resources to help my development.

Above the SOC and GRC teams is Bob, the CISO, who oversees the city's broader cybersecurity strategy and IT infrastructure. Bob plays an active role in developing policy and strategy while being approachable and involved in daily operations. Furthermore, he offers insight into the department's long-term objectives and how each team member's work will contribute to the overall mission.

Overall, the management environment was organized and flexible. There was a structured hierarchy, along with teamwork built on communication, learning, and development. It was

motivating to see the opportunities and progressions available within the department. The team's experiences made a career path in cybersecurity feel more attainable and exciting, while their guidance offered a solid foundation for my internship.

Major Duties and Assignments

During my internship, I took on various tasks and responsibilities that supported the operations of the SOC teams. These opportunities enabled me to apply my academic knowledge and gain hands-on experience with the tools, investigative processes, and decision-making involved in incident response and threat analysis.

Risky User Investigations in Microsoft Azure (Entra ID)

One of my primary duties was to triage low-level alerts generated by the security systems. This involves investigating risky user sign-ins detected in the Microsoft Azure Entra ID environment. Investigating risky users and distinguishing between legitimate and potentially malicious activity required a lot of analytical attention to detail.

When clearing out risky users, I would begin by filtering out and dismissing low-risk sign-ins, which typically consisted of remediated or repetitive alerts. Most of my work on risky users was concentrated on medium and high-risk sign-ins that required more thorough analysis. For each identified user, I gathered the following crucial information:

- Application accessed
- IP address
- Date, Time, and Location where the login attempt took place
- Whether the attempt was successful, interrupted, or failed

Next, I access the user's profile to gather more information and context, like their position and department. I checked both the sign-in and audit logs to identify the flagged specific activity, verifying if the sign-in coincided with a password change or exhibited signs of impossible travel or other suspicious behaviors. I further examine the reason behind the flagged sign-in attempt: incorrect credentials, failure to complete multi-factor authentication, or a suspicious token. I also examine the user agent to determine the type of device and browser from which the user logged in.

Open-source intelligence (OSINT) tools are regularly used to assist in investigations. I was introduced to the following OSINT tools during the internship:

- VirusTotal - for scanning malicious files, IPs, or URLs
- Scamalytics and AbuseIPDB - to check the reputation of IP addresses
- URLScan and urlquery - to analyze the safety of URLs before clicking or investigating further
- ANY.RUN - to run dynamic analysis on suspicious files in a controlled malware sandbox

I scanned the user's IP address in VirusTotal, Scamalytics, and AbudeIPDB to assess whether it has a record of malicious activities, abusive behavior, or usage through anonymizing VPNs. Additionally, I examined which conditional access policies flagged the sign-in attempt, such as whether the login was initiated from outside the country or breached other security policies.

If an event wasn't flagged as a risky sign-in but still exhibits suspicious behavior, then it is an anomalous token that triggered the alert. For instance, this can include tokens being used from unfamiliar or foreign locations inconsistent with the user's activity, such as a scenario of impossible travel, where a token is accessed in two different countries in a short time frame. An anomalous token may also involve abnormal usage, such as a prolonged lifespan or a reused token over multiple sessions, which could indicate a security compromise. When I encounter malicious activity, I report my findings to a senior team member for further investigation, revoke the session, require reauthentication, or implement conditional access and remediation processes to protect the city network.

After gathering the necessary information, I contacted the user directly to confirm whether they were responsible for the login attempt. If it is confirmed legitimate, I dismiss the user risk in Azure. If the activity appears malicious or cannot be verified, I confirm the user compromise, which automatically blocks the user from accessing the city network and resources. In confirmed cases, I report the incident to Kris, who then initiates a password reset and credential refresh for the user.

Phishing and Spam Email Investigations in Microsoft Defender

Another of my primary duties was investigating phishing and spam emails reported by city employees using Microsoft Defender. I start each case by filtering out phishing simulations generated for cybersecurity training. Once filtered, I assess the queue of reported emails to scan for any legitimate threats at first glance. Based on my evaluation, emails reported by city employees will be classified as either phishing, spam, or no threats detected.

For each email, I record the following information:

- Sender name and email address
- Source IP address
- Domain

I further analyze the following:

- Full email entry (including the entire message body)
- Embedded URLs
- Attachments

I then scanned the URLs and IP addresses in OSINT tools. The IP addresses were analyzed using AbuseIPDB, Scamalytics, and VirusTotal. The URLs were analyzed through URLScan, urlquery, and ANY.RUN to determine whether they led to malware, phishing kits, or questionable redirects.

Based on these investigations, I have made a final determination regarding the classification of the email. If an email appears suspicious and is identified as malicious by OSINT tools, it will be classified as phishing. Furthermore, assessing the email entry can help in making this determination. Along with containing malicious links, the message may also employ notable social engineering tactics, such as creating urgent or overly promising scenarios, to steal personally identifiable information (PII) or financial data. If multiple reports and emails are part of a broader phishing campaign in Defender, I report it to Kris for further analysis. Kris will then

add IPs and domains to a block list and add to the city's threat intelligence database by recording common senders or methods. If an email isn't a threat but is unwanted, it will be classified as spam. Spam emails typically consist of advertising and unwanted offers. Finally, if an email isn't a threat and is relevant correspondence to the user, it will be classified as 'no threat detected.'

Digital Forensics and Compromised Device Support

In certain cases, I also supported the SOC team in investigating compromised city devices. When a device was identified to be exhibiting unusual or malicious behavior, I helped gather and analyze evidence using Autopsy, a digital forensics tool, on the infected device.

Using Autopsy, I examined and searched for:

- File access history to detect anomalies
- Suspicious scripts and executables
- Evidence of data exfiltration or lateral movement

These investigations helped me gain a better understanding of incident response, from triage for alerts to in-depth forensic analysis. I saw how digital forensics improves the SOC team's capabilities by providing insights to prevent future breaches after an incident.

Alongside responding to alerts and assisting in investigations, I independently studied Splunk, a Security Information and Event Management (SIEM) tool used by the department to gather and analyze security data from various endpoints and services. While I wasn't yet executing complex queries, Tatum taught me some of the Splunk search queries and familiarized me with the interface.

Curriculum Connection and Use of Cybersecurity Skills and Knowledge

This internship allowed me to apply the skills and knowledge I gained at ODU in a real-world work environment. Before starting the internship, I had a solid foundation in network security, ethical hacking, and digital forensics, gained through courses such as Cybersecurity Techniques and Operations, Digital Forensics, and Ethical Hacking. However, this hands-on experience taught me how the concepts I learned in school are used in a professional setting while deepening my understanding of cybersecurity.

Before the internship, I was familiar with cybersecurity principles, frameworks, and security tools; however, I had never worked in a security operations center. Throughout the internship, learning Microsoft Azure and Defender improved my skills in analyzing user behavior, recognizing phishing attempts, and managing alerts. Using these tools required me to analyze logs, evaluate risk levels, and take appropriate action for each situation. The knowledge and habits I've learned at ODU have helped me in these situations. Furthermore, working with Entra ID (Azure Active Directory) to examine risky sign-ins allowed me to apply my knowledge

of authentication, multifactor access, and audit logging to protect systems. Collecting and analyzing user metadata, IP addresses, user agents, and sign-in patterns strengthened my ability to detect unauthorized access attempts.

Additionally, I expanded my knowledge in digital forensics. My previous courses familiarized me with forensic investigation techniques and tools, such as Autopsy. However, during the internship, I participated in actual investigations involving compromised devices. This experience required me to use my knowledge of disk analysis, file recovery, and behavioral anomaly detection. Working in Autopsy helped me better understand how to analyze file metadata, timelines, and system logs during incident response and investigation. Furthermore, my coursework in Network and Security introduced me to the flow of data within networks and the potential threats that can emerge in network traffic. This knowledge proved useful when investigating alerts and login attempts in Azure. I knew which indicators to look for in IP data and how to identify suspicious behavior.

Speaking with Tatum and Sam, cybersecurity analysts and ODU graduates, helped me understand which ODU courses and curriculum align with real-world jobs. Their experiences were similar to mine, and seeing how they expanded upon their academic background after college was reassuring. Tatum's path from intern to full-time analyst and Samuel's current work towards his master's degree both emphasize the value of continuous learning.

Overall, this internship built upon the skills I developed at ODU and introduced me to numerous tools and procedures not covered in my courses. This internship confirmed the importance of network monitoring, authentication, cybersecurity awareness training, and more. Furthermore, it highlighted the importance of security operations and taught me how to work effectively in a collaborative team environment.

Internship Goals and Learning Objectives

At the start of my internship with the City of Virginia Beach IT Department, I established four primary goals:

1. Learn how to identify, analyze, and respond to cybersecurity incidents.
2. Learn the SOC infrastructure.
3. Develop skills in using network monitoring tools.
4. Participate in vulnerability assessments.

All of these goals were addressed in significant and practical ways during my time with the cybersecurity team.

1. Learn how to identify, analyze, and respond to cybersecurity incidents

This was the most crucial aspect of my internship experience. I was responsible for investigating and addressing Microsoft Defender and Azure alerts, including risky sign-in

attempts, phishing incidents, and suspicious activities on city devices. I found my systematic approach to managing and reporting incidents through this role. I learned how to analyze audit logs, evaluate sign-in patterns, and determine whether an alert is a genuine threat or a false positive. Furthermore, I assisted in investigating potentially compromised devices by utilizing digital forensics tools to uncover suspicious files and user activities. These experiences exposed me to detection and triage.

2. Learn the SOC infrastructure

I became more familiar with the SOC team operations as my internship progressed. The cybersecurity team has a separation of duties between the SOC and GRC sides. Additionally, I learned how the team combines multiple tools, including OSINT, Azure, and Microsoft Defender, to create a comprehensive overview of security incidents. Receiving training from team members like Tatum and working under Kris let me see how a SOC analyst contributes to the city's cybersecurity framework.

3. Develop skills in using network monitoring tools

This objective was accomplished through the consistent use of security platforms and OSINT tools. Within Azure, I monitored and responded to alerts regarding suspicious user activities, evaluated login attempts, and assessed conditional access policies. In Microsoft Defender, I examined reports of phishing and spam, analyzed email metadata, and utilized resources such as VirusTotal, URLScan, AbuseIPDB, and ANY.RUN to gauge threat levels. I also started familiarizing myself with Splunk, a SIEM platform for log analysis and alert generation.

4. Participate in vulnerability assessments

Although my primary role is in incident response, I had the opportunity to observe the team conducting vulnerability assessments. I learned how the SOC team handles vulnerabilities by tracking malicious IPs and domains in a block list that spans the entire city network and continuously updates the Palo Alto firewall. Although I wasn't directly involved in conducting assessments, I expanded my knowledge of the processes involved and how vulnerability management contributes to incident prevention and mitigation.

Overall, I achieved my internship learning objectives to varying degrees, with some exceeding my expectations. As a result of this experience, I now have a stronger foundation for a career in cybersecurity.

Motivating and Exciting Aspects

One of the most motivating aspects of my internship was the level of trust and responsibility I was assigned as a member of the cybersecurity team. From the beginning, I was given real assignments that impacted the security of the city's network and supported the team's operations. I had the chance to investigate alerts, analyze malicious emails, and respond to risky users, which made my efforts feel meaningful.

Another positive aspect of the experience was working with a team of diverse backgrounds, knowledge, and levels of expertise. Each team member was not only knowledgeable and approachable, but they were willing to help me develop my own skill set. Tatum consistently provided mentorship and valuable guidance on technical skills, career strategies, and life. Sam offered a unique perspective on the compliance and policy aspects of cybersecurity. Kris shared experiences from his career journey and discussed how he worked his way up to the management position. The diverse backgrounds of the team and the collaborative work environment motivated me to continue learning and building my skill set. Furthermore, exploring a variety of tools was also exciting. It was enjoyable to work in Azure and Defender, use OSINT tools, and explore Splunk. Each tool and platform was another aspect of cybersecurity operations, and the hands-on experience made for an engaging learning experience.

Finally, one of the most exciting aspects of the internship was working in a continuously evolving field. Each day brought a new experience. For instance, I could be handling a phishing campaign one day and assisting in a digital forensics investigation the next. Although it's ideal for no security incidents to occur, it's exciting when a problem needs to be solved.

Discouraging Aspects

Although the internship was primarily a positive experience, there were some discouraging aspects, especially during the early stages. The most significant challenge was the initial learning curve. In the first few weeks, I was overwhelmed with all the unfamiliar terminology, tools, procedures, and technical concepts. It was initially tough to adjust to the professional setting and respond to alerts with confidence. There were moments when I doubted my ability to meet the expectations or make a meaningful contribution to the team. There are real consequences that impact users and systems, so there was definitely some anxiety about causing an error or misidentifying a threat.

Another drawback of the internship was that it was unpaid. While I am grateful for the opportunity and I understand the value of this experience, it was a challenge to balance an unpaid internship alongside my academic responsibilities and personal costs. A paid internship would provide support for students eager to gain experience while also getting financial compensation. It would have been ideal to get paid, but I like to think of this internship as a means of putting in unpaid work for a better chance at a great-paying job. Nevertheless, I remained motivated by the knowledge and guidance I was receiving.

Most Challenging Aspects

One of the challenging aspects that came early in my internship was gaining the confidence and accuracy needed to investigate real-world security incidents. Each alert or risky user posed a potential threat to the city's network or data, which added significant responsibility to every task. From this, I learned that cybersecurity requires attention to detail and critical thinking when analyzing risky sign-ins or potentially malicious emails. I overcame this doubt by relying on my skill set and continuously asking my superiors questions.

Another major challenge was developing an investigative mindset to complete my daily tasks effectively. Investigating risky user logins, phishing emails, and suspicious activity required me to think critically and approach each task as if piecing together a puzzle. I needed to learn to collect relevant evidence and analyze technical data to draw informed conclusions. Investigations took more than following a set of procedures. Every incident is unique, and it is essential to understand the underlying reasons behind certain behaviors. Developing this mindset is like exercising a muscle; it takes time, repetition, and consistency to strengthen my analytical thinking.

Lastly, juggling the demands of the internship with my academic responsibilities posed an extra challenge. Completing coursework, exams, internship assignments, and studying simultaneously required a great deal of time management skills. Several times during the semester, I wrestled with my different responsibilities. Nevertheless, overcoming these challenges helped me learn how to prioritize my time and efforts.

Recommendations for Future Interns

Based on my experience, I have some advice for future interns. It's best to develop a foundation of cybersecurity knowledge before starting the internship. Having a fundamental understanding of networking, authentication techniques, and cyberattacks can go a long way. Also, research the career path you want to pursue in cybersecurity; let your interests guide the direction you take. For instance, I was more interested in the technical aspects of cybersecurity rather than the policy side, so I chose to intern with the SOC team over the GRC team. Furthermore, take notes and ask questions. The SOC side demands attention to detail and critical thinking. You can't remember everything at once, so it's smart to keep a notebook of notes, which could include important terms, tools, and processes. Another important recommendation is not to hesitate to ask for help. The cybersecurity team is very knowledgeable and supportive; asking questions will show your initiative and eagerness to learn.

Expect to be overwhelmed at first. You may not feel fully prepared, but take the internship one step at a time. Concentrate on learning and rely on the team. While the learning curve may be tough, it is achievable with consistency and effort. It's important to remember that communication is key. Whether you're working on a case together, confirming an alert, or seeking feedback, openly communicate with your team or manager. Additionally, if you have downtime, consider exploring the different tools or studying on your own. This initiative will

help build your skill set and show your interest in cybersecurity to Bob and the team. Lastly, it's important to be adaptable. Given that cybersecurity threats are constantly evolving, adaptability will prepare you for when an unfamiliar threat arises.

Conclusion

My internship with the City of Virginia Beach Department of Information Technology has been valuable to my academic and career path. It enabled me to apply cybersecurity principles in a real-world environment, collaborate with experienced professionals, and contribute to securing the city's critical systems and data. A key takeaway I gained from this internship is the importance of being adaptable and continuously learning. Whether addressing security alerts or analyzing phishing attempts, every incident is unique and requires a calculated approach. I also learned that being proactive about growth and asking questions can lead to valuable connections and new opportunities.

Undoubtedly, this experience will influence how I spend the remainder of my time at Old Dominion University. I am more motivated to expand my cybersecurity knowledge, especially in incident response and threat analysis. It gave more insight into certifications and skills I should focus on next. Looking forward, I now feel more equipped to pursue a career in cybersecurity. This internship helped me gain confidence in my skills and provided valuable insight into the daily operations of a Security Operations Center. After graduation, I plan to pursue an entry-level cybersecurity analyst position with the IT department. As for my future, it remains to be determined, but I will continue to expand my cybersecurity experience.

References

Core service areas. (n.d.). City of Virginia Beach. https://it.virginiabeach.gov/core-service-areas

Information technology. (n.d.). City of Virginia Beach. https://it.virginiabeach.gov/

Images from:

Garrodonnell. (n.d.). Investigate risk with Azure Active Directory B2C Identity Protection. Microsoft Learn. https://learn.microsoft.com/en-us/azure/active-directory-b2c/identity-protection-investigate-risk?pivots=b2c-user-flow

Sonne, M. M., & Sonne, M. M. (2024, April 3). Defender for Office 365 – Hunting and responding to QR code-based phishing attacks – Blog - Sonne´s Cloud. Blog - Sonne´s Cloud – Michael Morten Sonne | Microsoft MVP. https://blog.sonnes.cloud/defender-for-office-365-hunting-and-responding-to-qr-code-based-phishing-attacks/

Sruthy. (2025, January 20). Reporting suspicious messages in M365 shared and delegated mailboxes. AdminDroid Blog. https://blog.admindroid.com/reporting-suspicious-messages-in-m365-shared-and-delegated-mailboxes/

Appendix

Figure 1

This screenshot shows correspondence between me and a user flagged for suspicious login attempts. With the users' names redacted, this email chain is part of the verification process to confirm whether the flagged activity is malicious. The login attempts are verified, and I can proceed to dismiss user risk.

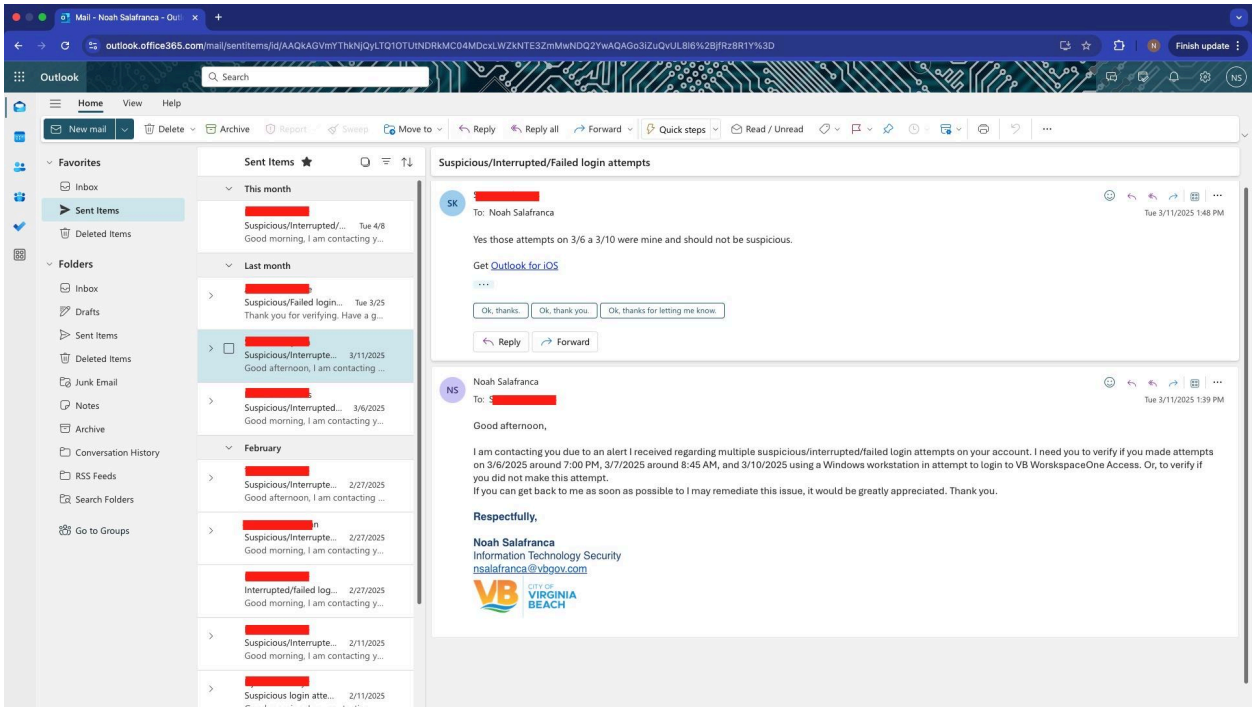

Figure 2

To maintain confidentiality, screenshots of real security incidents won't be included. This image is from Learn Microsoft and displays risky user alerts in Azure. The flagged users are displayed, along with their corresponding risk levels. The "Recent Risky Sign-ins" tab displays metadata, including the time, date, location, and IP address of the login attempt. The "Detections not linked to a sign-in" tab displays any anomalous tokens detected, along with their corresponding time and date. The buttons outlined in red are the classifications and actions to resolve an incident after investigation.

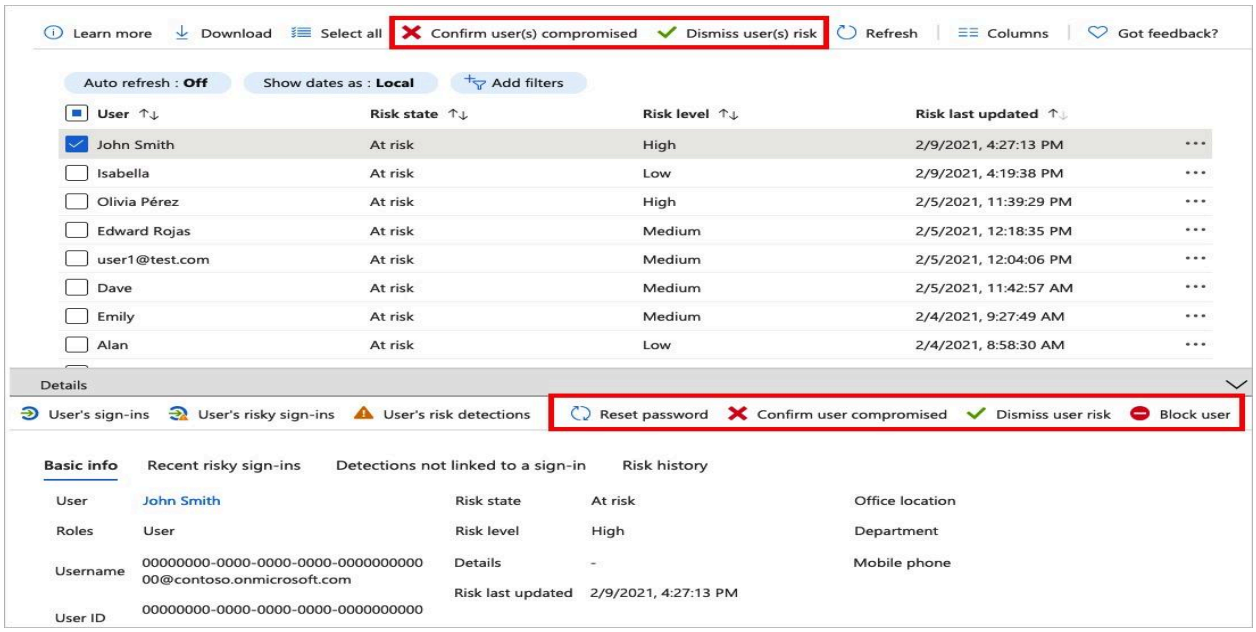

Figure 3

This image is from a Microsoft 365 community blog and displays email submissions in Defender to maintain confidentiality. Each submission will display its reported reason, sender address, recipient address, and subject line. The "Mark as and notify" button drops down to display the categories into which email submissions can be classified: phishing, spam, or no threats found. The user is then notified of the classification.

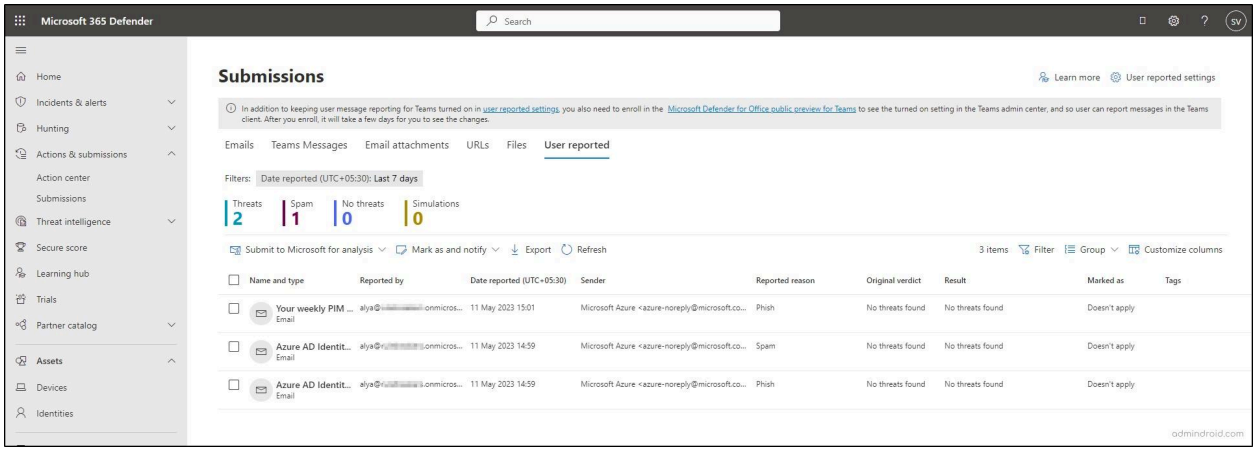

Figure 4

To maintain confidentiality, the following images are from a Defender blog rather than real security incidents within the city network. These images display the metadata collected during the investigation of a phishing email, including the sender's IP address and email address. The marked "Open email entity" leads to additional information for further analysis, including email preview, domain, attachments, and URLs.