Student Team Elevates Security Posture for Small Business Across Critical Areas

A Professional Readiness Experiential Program (PREP) Project Effort

----- ***Authors / Student Project Team Members*** -----

Taylor Le is a student at George Mason University graduating with a bachelor's degree in Information Technology with a concentration in Cybersecurity.

Quan Vo is a student at George Mason University graduating with a bachelor's degree in Information Technology with a concentration in Cybersecurity.

John Pham is a student at George Mason University graduating with a bachelor's degree in Information Technology with a concentration in Cybersecurity.

Angelo Pilande is a student at George Mason University graduating with a bachelor's degree in Information Technology with a concentration in Cybersecurity.

Brandon Nguyen is a student at George Mason University graduating with a bachelor's degree in Computational Data Sciences.

----- ***Industry Participant / Mentor*** -----

Wills Ogus
Technology Solutions Architect (Technology and Cybersecurity Programs)
Mobius

Lashdeep Singh
Director of Operations
Mobius

----- ***Faculty Member*** -----

Brian K. Ngac, PhD
Instructional Faculty & Dean's Teaching Fellow
George Mason University's Costello College of Business
bngac@gmu.edu

Interested in being an Industry Participant and or PREP Sponsor? Please reach out to bngac@gmu.edu, Thanks!

Introduction

Mobius is an award-winning, SBA HUBZone-certified, Woman-Owned Small Business specializing in government contracting and commercial work. We provide solutions in cybersecurity, systems engineering, modeling and simulation, and intelligence analysis. Our cybersecurity efforts focus on developing mission-critical solutions that mitigate vulnerabilities, combat advanced threats, and ensure compliance with industry security standards. We joined Mobius' cybersecurity team through an extensive interview process, where we demonstrated our technical knowledge, problem-solving skills, and ability to thrive in a collaborative environment. The program provided us with a unique opportunity to tackle real-world security challenges while contributing to the organization's efforts to strengthen its security posture across multiple critical vectors.

Business Challenge

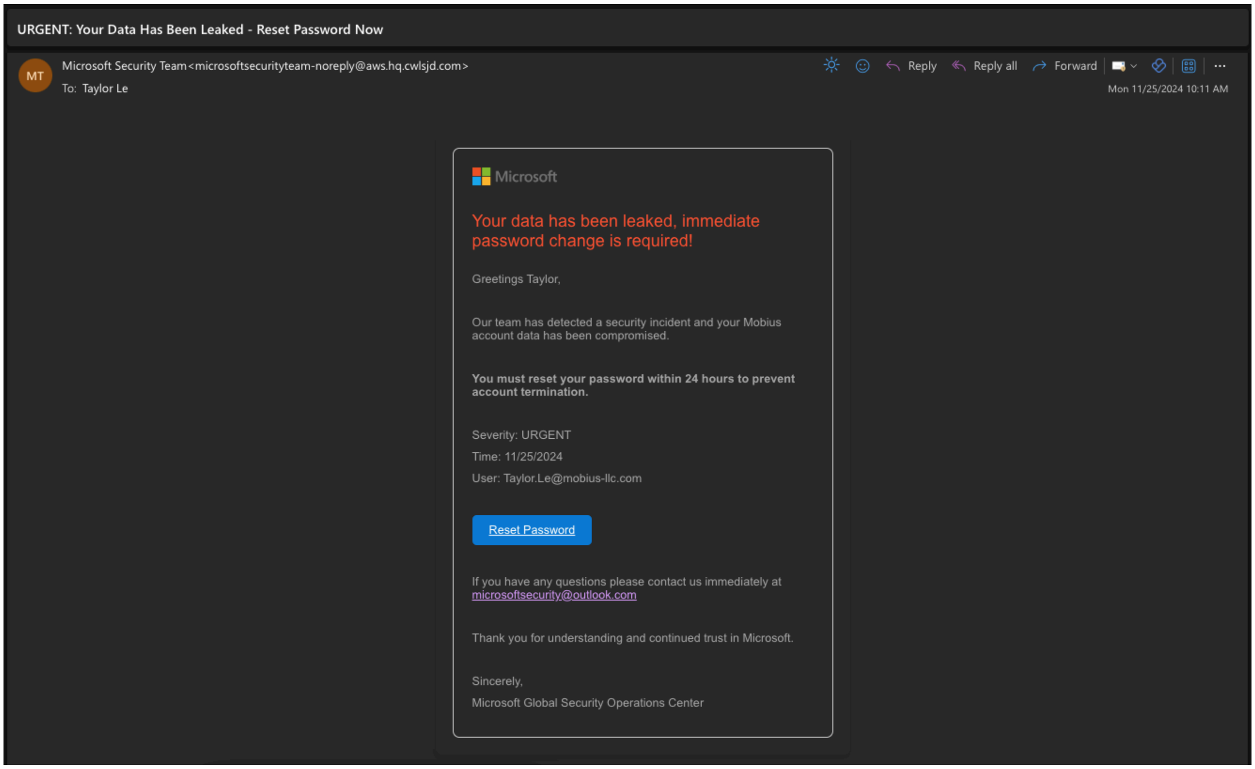
Mobius places a strong emphasis on security and is committed to the continuous improvement of its security infrastructure and operational efficiency. A poor security posture can expose an organization to increased threats, damage its reputation, disrupt business continuity, and result in penalties and costly downtime. During our cybersecurity internship program, we worked on four key projects that targeted areas of growth, strengthened existing systems, and introduced innovative solutions. These projects addressed phishing vulnerabilities, underutilized security policies, and the lack of auditing capabilities within Mobius.

Activities Done to Address the Business Challenge

Our internship program was structured to provide a collaborative experience, offering us the opportunity to develop expertise in various aspects of cybersecurity. Each intern was assigned to lead their own project, taking responsibility for its overall direction and deliverables, focusing on phishing awareness, policy optimization, and streamlining compliance processes. All interns actively contributed to each other's projects, resulting in well-rounded solutions built through collaboration and ensuring everyone gained hands-on experience in different areas, expanding their skill sets. To facilitate progress and learning, we held weekly meetings to discuss project updates, address challenges, and refine our strategies.

Attack Simulation & Security Training *(Quan Vo)*

Every quarter, the security team at Mobius launches a mock cyberattack on the company to test the awareness and reactions of its employees. For this quarter, we worked as a team to develop a phishing email posing as the Microsoft Security team, stating that the employee's data had been leaked and requiring them to click on our suspicious "Reset Password" link to reset their password. In this email, we ensured the inclusion of common aspects of a phishing email, such as a sense of urgency, a suspicious sender's domain, and typos within the sender’s email address. Furthermore, only 4 (2.5%) employees clicked on our link, while the rest reported the email within 25 seconds of its release. Though only 2.5% of our employees clicked on the link, we are working towards an environment where everyone is aware of these common attacks and knows how to handle them. As a result, once an individual clicks on the “Reset Password” link, they are directed to a cybersecurity training site that highlights the typical methods used in phishing attacks.



URGENT: Your Data Has Been Leaked - Reset Password Now

Microsoft Security Team<microsoftsecurityteam-noreply@aws.hq.cwlsjd.com>
To: Taylor Le

Mon 11/25/2024 10:11 AM

Your data has been leaked, immediate password change is required!

Greetings Taylor,

Our team has detected a security incident and your Mobius account data has been compromised.

You must reset your password within 24 hours to prevent account termination.

Severity: URGENT
Time: 11/25/2024
User: Taylor.Le@mobius-llc.com

Reset Password

If you have any questions please contact us immediately at microsoftsecurity@outlook.com

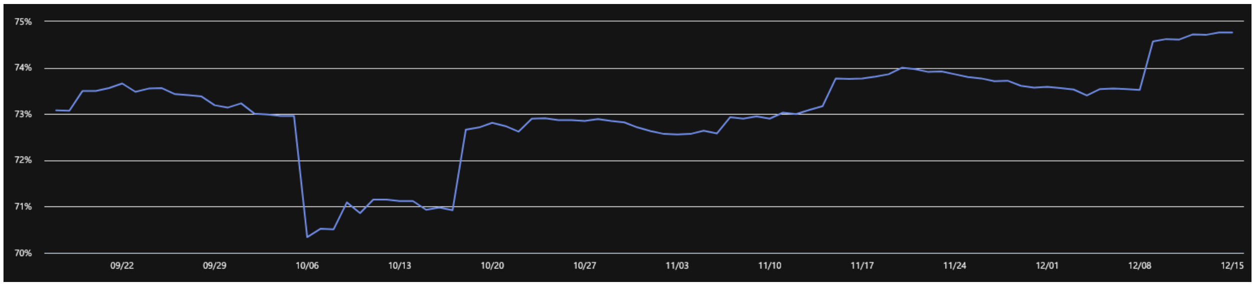
Thank you for understanding and continued trust in Microsoft.

Sincerely,
Microsoft Global Security Operations Center

Caption: This is our attack simulation phishing email that was sent out to all users in our organization.

Identity & Data Security *(John Pham, Brandon Nguyen)*

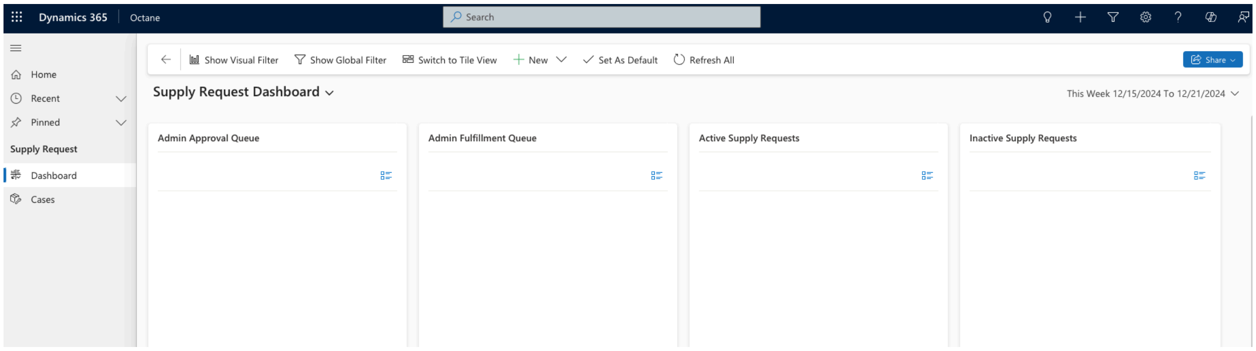
We focused on improving Mobius’ identity and data security scores to enhance its overall Microsoft Defender security score, which initially stood at 70%. The Microsoft Defender dashboard provided actionable recommendations, and we concentrated on areas with the greatest impact within the identity and data categories. Key actions included enabling multi-factor authentication, tightening access controls, ensuring mobile device encryption, and quarantining messages from impersonated domains. Our team worked collaboratively to evaluate each recommendation’s feasibility, implementation process, and impact on business operations. We prioritized measures that addressed vulnerabilities and strengthened compliance with security standards. Through these efforts, we resolved key security gaps and elevated Mobius’ defense capabilities, showcasing the value of teamwork in achieving significant security improvements.



Caption: This is a graph of our organization's Microsoft Defender security score. A steady increase is observed from the start of our internship (mid-October) to the present.

Security Process Management System *(Taylor Le)*

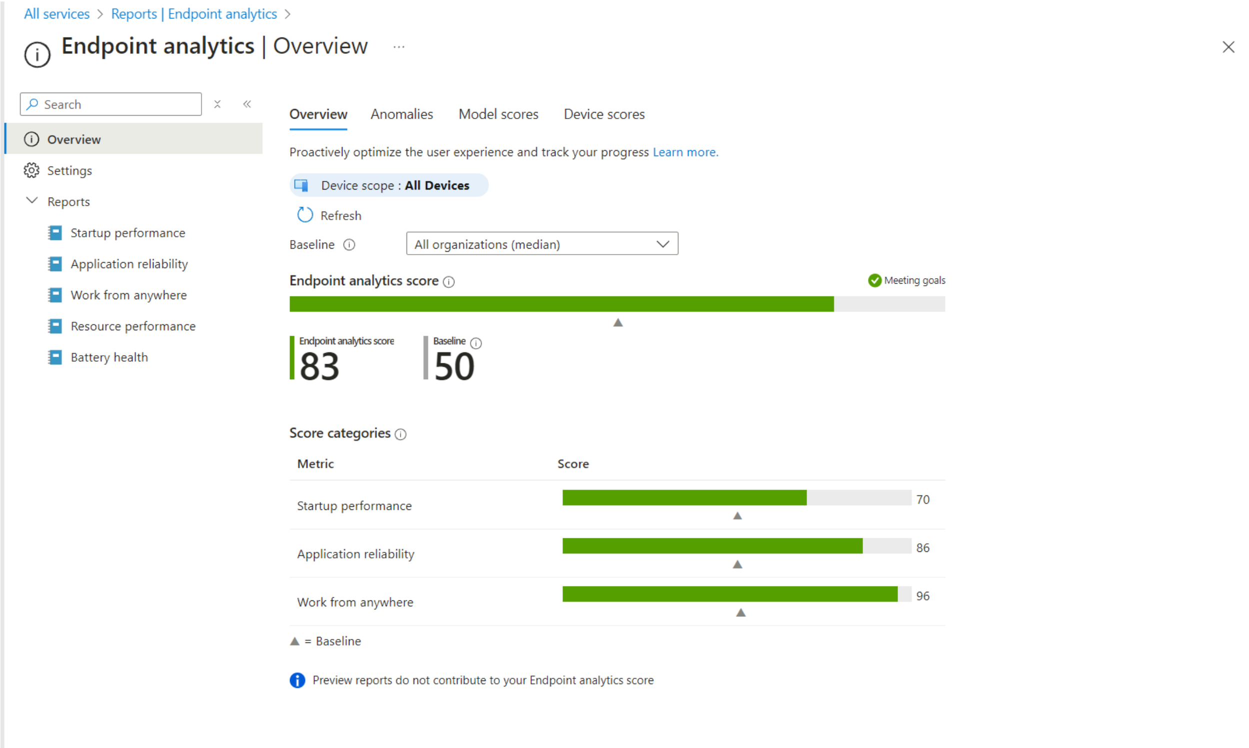
We expanded the existing contract management system to support security-oriented entitlement package processing for visit authorization, onboarding, and equipment requests. Leveraging Dynamics 365, Power Apps, and Entra ID, we improved process efficiency and enhanced compliance and auditing capabilities through detailed logging. Throughout the project, we collaborated closely with the security department to ensure the solution met both security and operational needs. Areas of collaboration included researching and deploying the solution onto a model-driven app in Dynamics 365.



Caption: This is the admin dashboard for our supply requests, part of a larger system that manages various security and facility processes.

Device Security & Compliance *(Angelo Pilande, Brandon Nguyen)*

Mobius utilizes various applications and devices that previously operated under different policies, which led to inconsistent security controls and compliance challenges. A key factor to consider was the potentially significant impact an action could have on improving the secure score, weighed against the associated costs. With the help of Microsoft Intune, we were able to focus on standardizing device management practices and application delivery across the organization. Working together with the IT security and operations team, we were able to optimize compliance policies using the monitoring tools provided by Intune and Defender. These measures effectively strengthened security posture and streamlined application deployment and updates. Using Defender, Intune, and Sentinel, we were able to gather the data provided by these software tools to efficiently carry out these changes.



Endpoint analytics | Overview

Proactively optimize the user experience and track your progress Learn more.

Device scope : **All Devices**

Baseline: All organizations (median)

Endpoint analytics score

Endpoint analytics score	Baseline
83	50

Score categories

Metric	Score
Startup performance	70
Application reliability	86
Work from anywhere	96

▲ = Baseline

Preview reports do not contribute to your Endpoint analytics score

Caption: This is a report generated by Intune, displaying the most recent report of Mobius' endpoint analytics including: "Application Reliability" and "Work from Anywhere" compliance.

Results & The Positive Impact

Each project during the internship addressed various pain points within Mobius, enhancing the organization's security posture and operational efficiency. The phishing simulation resulted in a 100% decrease in compromise rate and a 13% decrease in message link click rate compared to previous tests. This successfully demonstrated improved employee awareness and the effectiveness of the security training initiative. The security process management system automated security workflows, reducing processing time and the need for administrator intervention. The system also increased compliance and auditing capabilities through detailed logging. Our efforts to improve identity and data security were successful, achieving a 4.43% increase in Microsoft Defender's overall security score. We also significantly improved the health of endpoint security across the organization. These projects not only allowed us to diversify our skill sets but also gave us a sense of fulfillment in making positive and meaningful impacts on the organization's security infrastructure.

Conclusion

Our cybersecurity internship at Mobius provided us with a unique and enriching opportunity to address real-world security challenges. As a team, we successfully tackled phishing vulnerabilities, enhanced security policies, and bridged the gap between identity and data protection. We accomplished this through the projects and tasks assigned to us. Key projects, such as our phishing simulation, process automation, and security score optimization, provided us with valuable experience that led to a 4.43% increase in Mobius' Microsoft Defender security score. The collaboration between Mobius and the student team was essential in driving innovation and success. Our contributions laid the groundwork for sustainable security improvements while also resolving critical security vulnerabilities. This partnership highlights the value of combining theoretical knowledge and technical expertise to tackle complex real-world cybersecurity challenges.

PREP Student Reflection

Through our participation in the PREP program, our time at Mobius was fulfilling as we were exposed to many different industry-standard tools and techniques, enhancing our capacity to navigate complex projects and quickly adapt to emerging technologies. In addition, we improved our communication and teamwork skills, as we had to address various challenges and resolve roadblocks within a collaborative environment. Gaining practical, hands-on experience in cybersecurity projects not only deepened our technical understanding but also made us more competitive candidates in the job market. Our experiences at Mobius fostered both personal and professional growth, equipping us with the tools and mindset needed to excel in future careers.