Strengthening Cybersecurity through Data Protection, Access Management, and Automation with Mobius

A Professional Readiness Experiential Program (PREP) Project Effort

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

Joseph Yeboah

Kamran Ahmadjan

Brandon Lee

Jameel Abed

Adnan Shoukat

----- ***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

The Mobius Cybersecurity Internship provided an immersive learning experience where interns tackled real-world security challenges. Over the course of the program, the interns worked on data loss prevention (DLP), access management, security automation, and cybersecurity compliance. Their tasks involved implementing NIST guidelines, enhancing security policies, and using Microsoft security tools like Sentinel and Intune to protect company assets. This internship not only expanded their technical expertise but also provided insight into cybersecurity careers.

Business Challenge

One of the key challenges was ensuring the protection of sensitive company data, personal identifiable information (PII), and financial records. The interns were responsible for implementing and enforcing DLP policies that complied with U.S. state laws, HIPAA regulations, and cybersecurity best practices.

Another challenge was onboarding new subcontractors into Mobius' system while maintaining strict security access controls. This involved Implementing Microsoft 300-level security modules, Creating access packages to ensure users had the correct permissions, Streamlining Identity and Access Management (IAM), and Enhancing automation with Microsoft Dynamics to reduce manual security processes

Activities Done to Address the Business Challenge

For the first project of Data Loss Prevention and Compliance, the interns first developed and implemented DLP policies in Azure to safeguard PII, financial data, and proprietary information. They then configured automated alerts to detect and flag potential security risks. They utilized Microsoft Endpoint Manager to track and manage devices, ensuring compliance. And finally, they created security classifiers to identify sensitive data in emails and documents, preventing unauthorized data leaks.

For the second project of Access Management and Security Automation, the interns first had to complete the Microsoft 300-level modules to understand security frameworks. They then developed and tested access packages to minimize the risk of unauthorized access. They implemented SSO and multi-factor authentication (MFA) to enhance system security. They automated cybersecurity processes with Microsoft Dynamics and Sentinel, improving security monitoring and response efficiency. And finally, they deployed applications using Microsoft Intune to manage software installations securely across company devices.

Results & The Positive Impact

The work resulted in four major positive impacts for Mobius:

- Stronger Data Protection: Improved detection and prevention of unauthorized data leaks, increasing compliance with HIPAA, U.S. State Breach Laws, and the U.S. Patriot Act.
- More Efficient Access Management: New security frameworks minimized the risk of unauthorized access while improving the onboarding process for subcontractors.

- Automation and Operational Efficiency: Security teams benefited from reduced manual work and improved security response times due to automation.
- Hands-On Learning and Career Readiness: Interns gained valuable experience working with enterprise-level cybersecurity tools and frameworks, preparing them for careers in the field.

Conclusion

This internship provided hands-on experience in data security, access control, and cybersecurity automation. Interns successfully implemented DLP policies, security automation, and IAM best practices, enhancing Mobius' security posture. The experience also helped interns refine their technical and teamwork skills while gaining insight into potential cybersecurity career paths.

PREP Student Reflection

In their final presentation to Mobius, the interns reflected on their experiences as follows:

- Gaining Real-World Security Experience: Interns appreciated the opportunity to apply classroom knowledge to real cybersecurity challenges.
- Exploring Career Paths: The exposure to different security domains (policy creation, compliance, automation, and security monitoring) helped them identify areas of interest within cybersecurity.
- Building a Stronger Team Environment: They emphasized the importance of effective collaboration and communication in a professional IT setting.
- Learning from Mistakes: Encountering technical hurdles and troubleshooting challenges reinforced problem-solving skills and adaptability.