Enhancing Cybersecurity at Mobius: Strengthening Insider Risk Management and Compliance through AI and Automation

A Professional Readiness Experiential Program (PREP) Project Effort

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

Cameron Portis

Steven Ly

----- ***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

Throughout the 12-week internship, Cameron and Steven worked in various aspects of information security at Mobius Consulting LLC. Their tasks included monitoring and investigating alerts from the Security Information and Event Management System (SIEM), handling IT helpdesk duties, and deploying a phishing attack simulation to improve employee awareness. The primary goal of the internship was to enhance security policy adherence and maintain compliance with government and company standards related to data loss prevention and insider risk management. Given Mobius' role as a government contracting firm handling sensitive data, their work played a critical role in safeguarding national security. While both interns worked on security-related projects, Cameron focused on improving insider risk management with AI threat monitoring, whereas Steven worked on ensuring compliance with NIST standards and developing security automation tools.

Business Challenge

During the first project (strengthening Insider Risk Management), Cameron was tasked with enhancing Mobius' insider risk management policies by implementing advanced monitoring tools. Although a system was already in place, it lacked specificity in detecting certain high-risk activities. The challenges identified included Monitoring and preventing risky website browsing (e.g., phishing, malware, gambling, and explicit content); Identifying and mitigating data leaks from volatile employees based on behavioral indicators (e.g., excessive profanity in messages, stressor events); and Implementing adaptive protection using AI to dynamically assess user activity and assign risk scores for automated security responses.

During the second project (NIST Compliance and Security Automation), Steven worked on two key challenges: 1 – NIST Compliance: Ensuring that Mobius' Microsoft Azure cloud and associated devices met the NIST 800-172 security standards, which are crucial for protecting controlled unclassified information; and 2 – Security Automation: Developing an automation system to enhance the security team's efficiency by streamlining workflows, onboarding processes, and visitor access requests.

Activities Done to Address the Business Challenge

For the first project, Cameron Implemented an AI-driven adaptive protection system that assigns risk scores to user activities; Monitored high-risk browsing behavior and enforced policy violations; and Created automated security controls like mandatory two-factor authentication, password resets, and policy acknowledgment requirements for at-risk users.

For the second project, Steven Conducted an initial assessment of Mobius' cloud infrastructure to evaluate compliance gaps; Researched NIST 800-172 standards and implemented necessary security controls, improving the compliance score from 65% to 91%; and Designed and developed an automation system for the security team using Microsoft Dynamics 365, integrating key security processes like onboarding and visitor access management.

Results & The Positive Impact

Cameron's and Steven's work resulted in three major positive impacts for Mobius:

- Improved Security Compliance: Mobius' adherence to NIST 800-172 standards significantly improved, enhancing data protection and ensuring continued government contract eligibility.
- Enhanced Insider Risk Management: The AI-driven monitoring system provided real-time risk assessments, reducing potential data leaks and improving response times.
- Increased Operational Efficiency: The automation tools developed for the security team streamlined workflows, reducing manual tasks and improving data tracking.

Conclusion

The internship provided Cameron and Steven with valuable hands-on experience in cybersecurity. Their contributions had a lasting impact on Mobius, improving security compliance, insider risk management, and operational efficiency. Their work not only strengthened Mobius' security framework but also provided them with critical industry skills for future careers in cybersecurity and IT.

PREP Student Reflection

Cameron found the internship to be an invaluable learning experience, emphasizing the importance of teamwork and continuous learning in cybersecurity. He gained firsthand experience with industry tools and strategies, reinforcing his ability to adapt and find solutions to emerging security challenges.

Steven reflected on the long-term impact of his work at Mobius, recognizing the importance of compliance and automation in cybersecurity. He appreciated the opportunity to develop technical skills in Sentinel, Azure, and automation while working closely with his supervisor and IT team.