Enhancing the Critical Security Operations with Mobius Consulting

A Professional Readiness Experiential Program (PREP) Project Effort

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

Jose Miguel Frondoso is a student at George Mason University graduating with a bachelor's degree in Management Information Systems.

Franco Lagdameo is a student at George Mason University graduating with a bachelor's degree in Management Information Systems.

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

Wills Ogus
Director, Information Technology & Security
Mobius Consulting

----- ***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 Consulting LLC is an award-winning, SBA HUBZone-certified, Woman-Owned Small Business (WOSB) specializing in missile defense, analytics, and strategy expertise for government and commercial customers. Recognized for their work in space and missile defense systems, Mobius delivers innovative technology solutions emphasizing modeling and simulation, weapons system integration, and acquisition management. Mobius is also a trusted partner of the Missile Defense Agency (MDA), contributing to innovative defense strategies through cybersecurity and organizational strategy. Their outstanding customer ratings and proven past performance ensure the highest operational excellence standard, as they drive the future of defense engineering and program management.

Business Challenge

In the growing landscape of IT, utilizing advanced technological solutions to streamline operations and enhance security measures is essential. At Mobius Consulting, the challenge was strengthening the efficacy of contract management processes and improving cybersecurity protocols to protect sensitive data. We addressed these security needs during our experimental learning program.

Our business challenge centered around optimizing the data management system for contract proposals using Microsoft Dynamics 365. This initiative was crucial in maintaining the integrity and confidentiality of contractual information, which is important for the sustained success and trustworthiness of Mobius. We also aimed to enhance organizational security posture in response to increasing threats of data breaches. This involved not just responding quickly, but preventative measures such as employee knowledge on cybersecurity threats like phishing, and the implementation of robust security protocols using Microsoft Sentinel.

Through these focused efforts, we sought to create a more resilient operational framework, aligning with Mobius's strategic goals while ensuring the highest data security and operational excellence standards.

While addressing the business challenges faced by Mobius, we recognized the potential of utilizing Microsoft Office 365 tools to overcome these hurdles and improve our operational framework. The goal was clear: to harness the versatile capabilities of Microsoft's cloud-based suite to enhance our contract management processes and enhance cybersecurity measures, ensuring the integrity of sensitive data.

Activities Done to Address the Business Challenge

To start, we aimed to optimize our contract management system by leveraging Microsoft Dynamics 365's advanced data management and workflow capabilities. This integration of Dynamics 365 with other Office 365 applications facilitated the automatic collection, analysis, and storage of contractual data, providing our team with real-time insights and simplifying proposal generation. With centralized access to key documents, our contract management became more efficient and secure, ensuring that critical information was consistently up-to-date and readily accessible to authorized personnel.

Enhancing Security Operations with Microsoft Sentinel, Custom KQL Codes, and Power BI Visualizations

Deploying Microsoft Sentinel enhanced Mobius' Security Information and Event Management (SIEM) capabilities. This cloud-native SIEM platform, equipped with AI-driven analytics, offered real-time monitoring and threat detection across our network infrastructure. However, to tailor to the intricacies of Mobius' security vulnerabilities we incorporated additional Kusto Query Language (KQL) codes. These customized queries expanded Sentinel's analytical depth, enabling our team to detect anomalies and patterns indicative of potential security incidents.

Utilizing specialized KQL codes, we utilized Sentinel's monitoring of our unique environment, filtering logs for unusual login attempts, unauthorized file transfers, and other red flags. These enhanced queries also improved our ability to identify emerging threats by cross-referencing internal data with Microsoft's comprehensive threat intelligence feeds. This approach allowed our security team to receive alerts, which reduced response times and ensured that threats were mitigated before causing damage.

Complementing this setup, we leveraged Microsoft Power BI to visualize data generated from Microsoft Sentinel. With its powerful data visualization capabilities, Power BI provided our team with dynamic dashboards that consolidated security insights into easily comprehensible formats. Through these dashboards, our analysts could quickly assess the state of our network security and track key performance indicators, such as the number of incidents detected and patterns in attacks. These visualizations also helped non-technical stakeholders understand security trends, fostering informed decision-making at all organizational levels.

The deployment of Microsoft Sentinel, the implementation of custom KQL codes, and integration with Power BI created a comprehensive security management ecosystem for Mobius. This empowered Mobius Consulting to maintain a security posture, ensuring the safety of our data systems while continuing to meet our strategic objectives.

Results & The Positive Impact

In summary, Mobius Consulting LLC faced the challenge of optimizing contract management and enhancing cybersecurity protocols to safeguard sensitive data. Through our strategic goal of utilizing Microsoft Office 365 tools, we aimed to boost their operations and strengthen the security posture against emerging threats.

By leveraging Microsoft Dynamics 365's data management and workflow capabilities, our contract management processes became more efficient, transparent, and secure, ensuring contractual information remained accurate, up-to-date, and accessible. This integration enhanced the integrity of our proposal system, bolstering trust and reliability in our services.

Furthermore, deploying Microsoft Sentinel significantly improved our Security Information and Event Management (SIEM) capabilities. Customized Kusto Query Language (KQL) codes enabled us to tailor Sentinel's monitoring and provide actionable alerts, helping us swiftly respond to potential threats. Power BI visualizations allowed us to interpret these insights with clarity,

providing dynamic dashboards that enabled technical and non-technical stakeholders to visualize potential vulnerabilities.

Conclusion

In conclusion, our combined efforts created a comprehensive security management ecosystem, reinforcing Mobius Consulting's robust and adaptive security. By leveraging Microsoft's advanced cloud-based tools, we strengthened the defense of our data systems, resulting in greater operational efficiency and safeguarding the sensitive information of both government and commercial clients. This transformation aligned perfectly with our strategic objectives, enabling us to deliver exceptional consulting services with the highest standards of data security and operational excellence.

PREP Student Reflection