Student Pair Delivers Cybersecurity Posture Monitoring Tools to Fairfax County-Based Defense Contractor

A Professional Readiness Experiential Program (PREP) Project Effort

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

Raheem Zikria is a senior at George Mason University pursuing a Bachelor of Science in Information Technology with a concentration in Cybersecurity. Over the past three years, he has contributed to the missions of more than ten organizations across multiple fields in full-time, part-time, and internship capacities, including with the Defense Information Systems Agency (DISA), Department of Homeland Security (DHS), United States Attorney's Office for the District of Columbia (USAO-DC), Red River, and Omni Federal, among others. He also holds numerous industry certifications, including CompTIA CySA+, CompTIA Security+, CompTIA Network+, CompTIA A+, and AWS Certified Cloud Practitioner. His professional interests include cybersecurity engineering, cybersecurity policy, system administration, and cloud infrastructure engineering, and he looks forward to cultivating his skills in said fields through his graduation in May of 2026.

Abdirahman Mohamed is a Junior at George Mason University majoring in Information Technology with concentrations in Cybersecurity and Cloud Computing, expecting to graduate in 2027. I'm passionate about security engineering, cloud technologies, and building automated solutions that improve threat detection and incident response. I've gained hands-on experience through my internship at KPMG as an Embark Scholar, where I worked across technology risk, IT audit, and identity and access management testing, as well as through my role as a Service Desk Engineer Intern at Capital Techies, where I supported end users and troubleshot system and security issues. I'm currently expanding my skills in Network+, Security+, AWS Cloud, Linux, and scripting while building projects to strengthen my technical foundation. Looking ahead, I'm interested in pursuing cybersecurity roles focused on cloud security, detection engineering, and automated security operations.

----- ***Industry Participant / Mentor*** -----	----- ***Faculty Member*** -----
William Ogus Solutions Architect Mobius Consulting	**Brian K. Ngac, PhD** FWI Corporate Partner Faculty Fellow Instructional Faculty & Dean's Teaching Fellow George Mason University's Costello College of Business
Interested in being an Industry Participant and or PREP Sponsor? Please reach out to bngac@gmu.edu, Thanks!	

Introduction

Mobius Consulting has experienced significant growth in its headcount and revenue over the past few years, and the complexity of Mobius' IT environment has grown along with it. However, due to the prioritization of more pressing matters, such as obtaining CMMC compliance and day-to-day user support, its cybersecurity apparatus has lagged. The Mobius IT team recognized this need for a more mature approach to security. This is where the PREP student team comes in.

Business Challenge

The Mobius IT team lacked a central authority for user security information within its operating environment. When in need of security-related information, IT team members would be required to amalgamate data from numerous disconnected sources and compile them together. This process was inefficient, cumbersome, inconsistent, and in some cases, would result in incomplete or overexaggerated data.

To combat these issues, Raheem and Abdi were tasked with leveraging Kusto Query Language (KQL) and Microsoft's Power BI tool to develop dashboards within Microsoft Sentinel to improve Mobius' threat detection and visibility capabilities.

Activities Done to Address the Business Challenge

Raheem and Abdi launched efforts on multiple fronts to bolster Mobius' defensive cybersecurity capabilities. The pair began by creating numerous real-time workbooks within Microsoft Sentinel tailored specifically to Mobius' IT team's requirements. Notable examples include:

1. **International Authentication Attempt & Successful Sign-ins**: This interactive Power BI dashboard and its corresponding Sentinel workbook illustrate all authentication attempts from international IP addresses as well as successful sign-in.

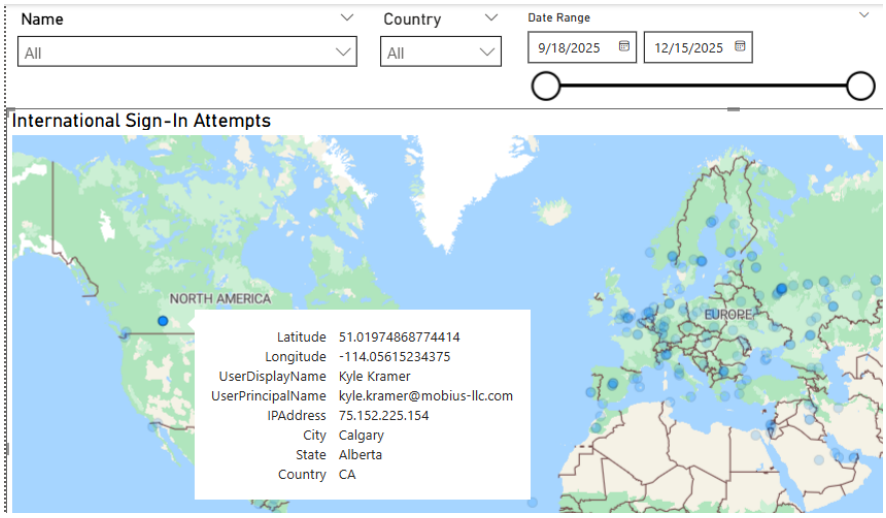

Figure 1: International sign-in attempts Power BI dashboard.

All international authentication attempts:

Country	UserPrincipalName	UserDisplayName	IPAddress	TimeAndDate	City	State	Longitude
KH	john.holmes@mobius-llc.com	John Holmes	110.235.255.191	2025-12-15 22:51:57	Tuol Tumpung Ti Pir	Phnum Penh	104.912803649902
CN	kyle.kramer@mobius-llc.com	Kyle Kramer	112.25.205.74	2025-12-15 19:48:40	Nanjing	Jiangsu	118.78417205810
SG	kyle.kramer@mobius-llc.com	Kyle Kramer	58.182.111.162	2025-12-15 19:48:17	Singapore	Central Singapore	103.8517837524

Figure 2: International sign-in attempts Sentinel workbook.

Authentication attempts from questionable nations (Russia, China, North Korea, Iran, Cuba, Yemen):

RedFlag	UserPrincipalName	UserDisplayName	IPAddress	TimeAndDate	City	State
CN	kyle.kramer@mobius-llc.com	Kyle Kramer	112.25.205.74	2025-12-15 19:48:40	Nanjing	Jiangsu
CN	kyle.kramer@mobius-llc.com	Kyle Kramer	111.62.42.70	2025-12-15 19:47:30	Shijiazhuang	Hebei

Figure 3: International sign-in attempts from red-flag nations Sentinel Workbook.

2. **Phishing and Brute Force Detection:** These Power BI dashboards visualize volume of failed sign-ins over time, with the x-axis representing hours and the y-axis representing days.

Failed Sign-In Heat Map (Brute Force Indicators)

Day	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	To
2025-11-19									1		1	1	12	11	23	24	33	23	12	21	2	11	7	6	1
2025-11-20		5			3							1	1	5	14	10	7	5	5	1	5	3	7	4	
2025-11-21	1			1							5	2	24		22	15	19	19	6	20	7	12	5	9	1
2025-11-22	3	1	1	8			1						8			1		7	1		1			3	
2025-11-23		7			2	6	2	1		2	1		3		6		1	3	3		4	10	6	7	
2025-11-24	1		29	3	9				1		2	10	20	13	33	22		20	6	6	10	14	23	11	2
2025-11-25	20	8	7	12	3	6	3		1	1		2	7	19	9	16	5	18	10	8	1	23	8	5	1
2025-11-26	3	9	2	10	2	1	7	3	1	1	1	10	5	14	10	21	19	8	11	7	6	5	7	13	1
2025-11-27	3	3		7	12		2	2	1	2		3		6	4	2	7	1	1		2	1	7		
2025-11-28	4	1	1	4	2		1		1		1	2	12	9	9	14	16	8	19	9	8	4	10	2	1
2025-11-29	2	1		1	5		1		1					7	2	2	9	2	3		16	14	15	1	
Total	**114**	**124**	**105**	**128**	**124**	**75**	**42**	**41**	**19**	**32**	**55**	**96**	**168**	**351**	**390**	**379**	**342**	**281**	**286**	**291**	**249**	**270**	**229**	**170**	**43**

Figure 4: Failed authentication attempts heat map sorted by date and time.

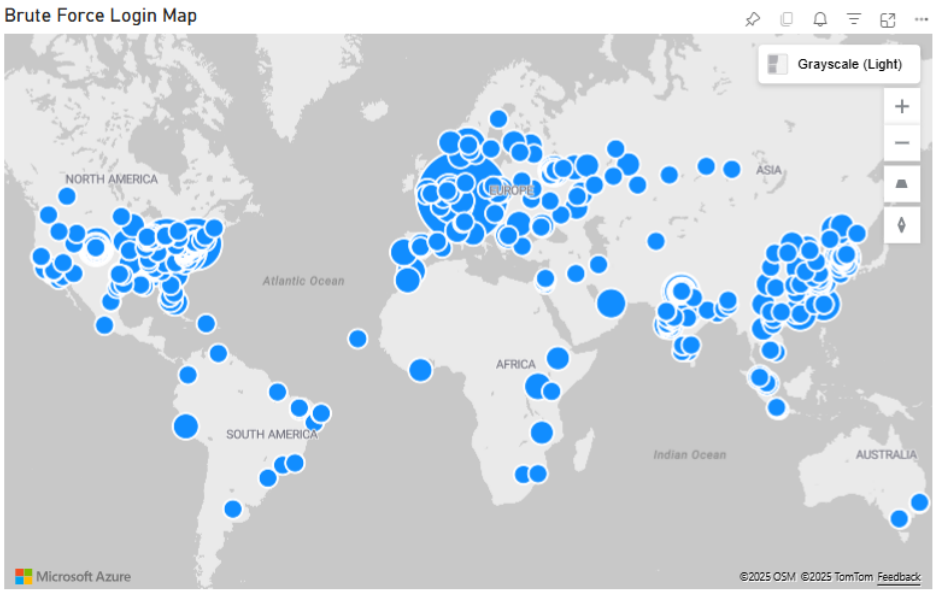

Figure 5: Power BI dashboard showcasing brute force attempts by geographical region. The greater the volume of attempts by region, the larger the map marker.

3. **User Security Sentinel workbook** highlighting inactive accounts, recent password resets, password reset frequency over the past month, users with the greatest sign-in volume, failed authentication attempts with corresponding error codes, weekend log-ons, and accounts lacking multi-factor authentication.

Accounts inactive for >30 days:

UserPrincipalName	UserDisplayName	LastLogin	DaysSinceLastLogin
christy.mote@mobius-llc.com	Christy Mote	12/24/2024, 10:38:50.112 AM	360
barry.grant@mobius-llc.com	Barry Grant	12/27/2024, 7:40:27.418 AM	357
ben.weller@missiondrivenresearch.com	Ben Weller - Mission Driven Research	1/1/2025, 6:20:03.066 PM	352
karen.ferrantelli@mobius-llc.com	Karen Ferrantelli	1/2/2025, 7:51:10.460 AM	351
kathryn.muenstermann@mobius-llc.com	Kathryn Muenstermann	1/7/2025, 11:27:44.977 AM	346
user_946c5fccb38948e1a3adb68f8a46005a@enablingtec...	eGroup Enabling Technologies technician	1/7/2025, 2:03:58.289 PM	346
thomas.blume@mobius-llc.com	Thomas Blume	1/9/2025, 12:23:49.700 PM	344
melanie.wells@mobius-llc.com	Melanie Wells	1/10/2025, 4:31:14.999 PM	343
brandon.nguyen@mobius-llc.com	Brandon Nguyen	1/13/2025, 11:38:02.020 AM	340
braden.thacker@mobius-llc.com	Braden Thacker	1/14/2025, 12:01:13.563 PM	339
will.cook@qed-analytics.com	William Cook	1/20/2025, 7:50:13.874 PM	332

Figure 6: Sentinel workbook highlighting accounts that have not been used in more than 30 days.

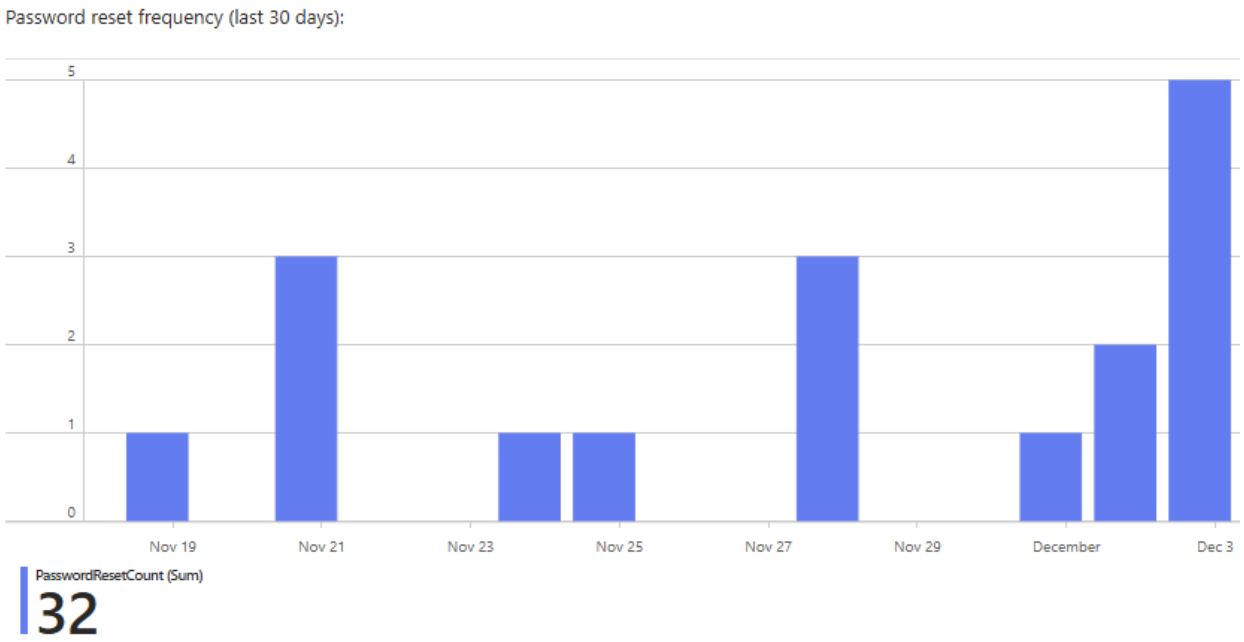

Figure 7: Workbook visualizing password reset frequency by day.

Top sign-in volume (last day):

UserPrincipalName	UserDisplayName	SignInCount
franco.lagdameo@mobius-llc.com	Franco Lagdameo	79
zachariah.allen@mobius-llc.com	Zachariah Allen	75
randy.salvagno@mobius-llc.com	Randy Salvagno	43
jonathan.williams@mobius-llc.com	Jonathan Williams	16
lashdeep.singh@mobius-llc.com	Lashdeep Singh	15
joseph.yeboah@mobius-llc.com	Joseph Yeboah	14
brian.stone@mobius-llc.com	Brian Stone	13
delia.hill@mobius-llc.com	Delia Hill	13
james.weinberger@mobius-llc.com	James Weinberger	12
kristen.brown@mobius-llc.com	Kristen Brown	8
robel.mengesha@mobius-llc.com	Robel Mengesha	8

Figure 8: Workbook showcasing accounts with the greatest number of successful access attempts over the last day.

Failed sign-in attempts and corresponding error codes:

UserPrincipalName	UserDisplayName	ResultType	ResultDescription	Date
thomas.lee@mobius-llc.com	Thomas Lee	50097	Device authentication is required.	12/19/2025, 12:53:37.273 PM
richard.moore@mobius-llc.com	Richard Moore	50076	Due to a configuration change made by your administrat...	12/19/2025, 12:48:28.651 PM
delia.hill@mobius-llc.com	Delia Hill	50097	Device authentication is required.	12/19/2025, 12:47:08.228 PM
frank.privitera@mobius-llc.com	Frank Privitera	50053	Sign-in was blocked because it came from an IP address ...	12/19/2025, 12:21:28.895 PM
bud.moeller@mobius-llc.com	Bud Moeller	50097	Device authentication is required.	12/19/2025, 12:18:07.625 PM
lashondia.davis@mobius-llc.com	Lashondia Davis	50125	Sign-in was interrupted due to a password reset or passw...	12/19/2025, 11:55:14.601 AM

Figure 9: Workbook highlighting failed sign-in attempts and their corresponding error codes and descriptions.

Successful weekend log-ons (Eastern time):

UserPrincipalName	UserDisplayName	TimeGenerated
lyn.raabe@mobius-llc.com	Lyn Raabe	12/14/2025, 11:38:46.742 PM
lyn.raabe@mobius-llc.com	Lyn Raabe	12/14/2025, 11:38:26.146 PM
lyn.raabe@mobius-llc.com	Lyn Raabe	12/14/2025, 11:38:16.124 PM
franco.lagdameo@mobius-llc.com	Franco Lagdameo	12/14/2025, 11:11:18.498 PM
mariekirlou.sare@mobius-llc.com	Mariekirlou Sare	12/14/2025, 10:42:12.158 PM
franco.lagdameo@mobius-llc.com	Franco Lagdameo	12/14/2025, 10:01:59.732 PM

Figure 10: Workbook showcasing successful weekend authentication attempts.

Additional projects undertaken include assisting in the development of a more than 100-page incident response plan, along with corresponding documentation templates; drafting a 40-page system security plan; and assisting the PREP team responsible for CMMC Level II compliance through Sentinel visualizations.

Results & The Positive Impact

The dashboards developed by Raheem and Abdi had a transformative effect on Mobius Consulting's cybersecurity posture. By centralizing security information into a single, accessible platform, the IT team no longer had to waste valuable time piecing together data from disparate sources. This streamlined approach improved both efficiency and accuracy, allowing the team to detect threats more quickly and respond with confidence. Real-time visibility into international authentication attempts, phishing activity, and inactive accounts provided actionable intelligence that strengthened Mobius' defenses against evolving cyber threats. Beyond operational improvements, the dashboards also supported compliance readiness by aligning with CMMC requirements, which enhanced Mobius' credibility with clients and auditors. Ultimately, the project not only improved technical capabilities but also fostered a stronger security culture within the organization.

Conclusion

The PREP student team's contributions marked a significant step forward in Mobius Consulting's journey toward cybersecurity maturity. By leveraging Kusto Query Language and Microsoft Sentinel, Raheem and Abdi transformed fragmented, inconsistent data into meaningful insights that empowered the IT team to act decisively. Their work addressed a critical gap in Mobius' security apparatus, providing scalable solutions that will continue to support the company's growth. The project demonstrated the value of combining technical expertise with business awareness, showing how targeted student-led initiatives can deliver lasting impact.

PREP Student Reflection

For Raheem and Abdi, the project was both a technical and professional learning experience. They gained hands-on expertise in KQL, Power BI, and Microsoft Sentinel, deepening their understanding of how these tools can be applied to real-world cybersecurity challenges. Working closely with Mobius' IT team taught them the importance of clear communication, adaptability, and aligning technical solutions with organizational needs. Delivering dashboards that directly improved Mobius' security posture gave them confidence in their ability to contribute meaningfully in professional environments. Most importantly, they came away with the realization that cybersecurity is not just about technology; it is about empowering people with the right information at the right time to protect the organization.