Researching and Delivering AI and Hyperautomation Defense Recommendations to the U.S. Cyber Command

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 of Science in Information Technology with a concentration in Cybersecurity. Taylor applied hands-on experience in security automation, cloud infrastructure, and government compliance to research how APT groups operate across the cyber kill chain and identify where AI and hyperautomation can close detection gaps.

Jeffrey Sterns is a student at James Madison University graduating with a Bachelor's degree in Computer Information Systems, with a concentration in Information and Cybersecurity Management. He applied his knowledge of cybersecurity and risk assessment to research advanced persistent threats (APTs) and analyze them using the cyber kill chain framework. Additionally, he leveraged his understanding of security techniques to develop potential solutions that align with both business objectives and client needs, particularly in strengthening defenses with the use of AI and hyperautomation against these evolving threats.

Samantha Whetzler is a student at George Mason University graduating with a bachelor's degree in Business with dual concentrations in Finance and Business Analytics. She used her research and critical analysis skills to provide a structured approach to collecting information. She also used her understanding of business consulting to provide a product aligned to both the business challenge and client's needs.

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

Anonymous
US Cyber Command

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

Brian K. Ngac, PhD
FWI Corporate Partner Faculty Fellow
Assistant Dean, Centers of Excellence
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

Advanced Persistent Threats (APTs) represent a critical national security challenge requiring immediate strategic intervention. State-sponsored actors maintain undetected presence within government and critical infrastructure networks for extended periods while conducting espionage and data exfiltration. This research addresses a central operational question: how can defenders close the APT detection gap by applying AI and hyperautomation across the cyber kill chain at the same speed and scale that adversaries already use against them? This paper, prepared for publication in the Communications of the ACM and submission to United States Cyber Command, identifies specific automation opportunities across the complete attack lifecycle.

Business Challenge

The US Cyber Command has identified APTs as always evolving becoming stronger and now have started to weaponize the use of AI and hyperautomation to attack critical infrastructures. With many security processes such as threat detection, incident response, and risk analysis still having manual intervention this leads to longer decision making with potential inconsistencies. The US Cyber Command wanted the team to dive into researching how hyper-automation could be used in cyber operational processes that would be able to save critical decision making time.

Activities Done to Address the Business Challenge

Our team began by gathering the requirements necessary from US Cyber Command stakeholders through structured weekly discussions where these sessions strengthened our defined objectives for the engagement. We determined that a comprehensive, high-level research paper analyzing the Lockheed Martin Cyber Kill Chain would provide the greatest foundation and benefit for identifying hyperautomation opportunities to leverage. We proceeded by generating a threat assessment analysis of real-world APT activities, including threat actors such as Salt Typhoon, Lazarus Group, Charming Kitten, and Cozy Bear. For each stage of the kill chain, we documented how modern adversaries weaponize AI and hyperautomation, then developed corresponding defensive strategies that apply equivalent technologies to improve threat detection, response, and decision-making. Our team's approach to research enabled us to translate threat actor operational capabilities into specific, actionable automation recommendations for cyber operations that can directly address the US Cyber Command's defensive abilities against next-gen adversaries.

Results & The Positive Impact

Our team produced a high level research paper prepared for delivery to the U.S. Cyber Command. The paper maps the full Lockheed Martin Cyber Kill Chain against named state sponsored APT groups, including Salt Typhoon, Lazarus Group, Charcoal Typhoon, SweetSpectre, WageMole, Charming Kitten, Fancy Bear, Crimson Sandstorm, APT31, APT10, APT28, APT41, and Cozy Bear. For every stage of the kill chain, we documented how these adversaries are actively weaponizing AI and hyperautomation, then translated each offensive capability into a corresponding defensive recommendation grounded in the same technologies.

The positive impact of this work is twofold. First, the paper gives U.S. Cyber Command a single consolidated reference that connects real threat actor behavior to specific, actionable automation opportunities across reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. Recommendations include AI driven attack surface management, automated dark web credential monitoring, semantic email analysis, identity verification workflows, automated patch deployment, behavioral analytics for fileless persistence, anomaly detection for encrypted C2 traffic, and AI driven exfiltration prevention. Second, the paper reframes the role of the human analyst as a critical decision maker working alongside AI and hyperautomation rather than being replaced by them, giving stakeholders a defensible position on how to scale defenses without losing human judgment.

By aligning defensive strategy directly to adversary tradecraft, our work supports U.S. Cyber Command's ability to prioritize investment, accelerate detection, and shift the operational advantage back toward defenders before the gap widens further.

Conclusion

Over the course of this PREP engagement, our team was able to address the research question that was given to the team at the start of this process. By developing a high level research paper analyzing the cyber kill chain and real-world APT activity, we were able to explore how modern adversaries are leveraging AI and hyperautomation to increase the speed, scale, and effectiveness of their operations. In response, we identified and proposed defensive strategies that apply the same technologies to improve detection, response, and decision-making across each stage of the kill chain. We hope that our collaboration with U.S. Cyber Command provides valuable insight into the mindset of modern threat actors, the methods they use to target critical infrastructure, and how emerging technologies such as hyperautomation can be leveraged defensively to shift the advantage away from attackers and strengthen our collective ability to prevent and respond to cyber threats.

PREP Student Reflection

This PREP project gave our team the opportunity to move beyond surface-level cybersecurity concepts and deeply analyze how APTs operate in real-world environments. Through our research for U.S. Cyber Command, we broke down each stage of the cyber kill chain and examined how modern threat actors execute attacks with precision, persistence, and increasing reliance on AI-driven techniques. By incorporating real-world APT examples, we strengthened our ability to connect theoretical frameworks to actual adversary behavior, giving us a clearer understanding of how these threats evolve over time. We developed recommendations such as behavioral analytics, automated threat intelligence pipelines, and AI-driven decision support systems to improve detection, response time, and overall operational efficiency. This opportunity provided us with the ability to conduct technical research, synthesize complex threat intelligence, and present structured, actionable insights. Working with the U.S. Cyber Command was highly beneficial, as it provided real-world context and insight into current cyber defense challenges, allowing us to align our research and solutions with the needs of a mission-focused organization operating at the forefront of national cybersecurity.