Michael Simmons msimmo94@students.kennesaw.edu **(912) 441-1991**
LinkedIn: https://www.linkedin.com/in/michael-simmons-2669a5266/

- A rising Information Security student with 3+ years educational experience in Security Research. I am seeking an opportunity to support Cisco's security portfolio by utilizing my education and work experience to detect vulnerabilities and analyze risk in advance.

SAP USA Virtual Cybersecurity Internship Program
Certificate of Completion, October 2021:
https://insidesherpa.s3.amazonaws.com/completion-certificates/SAP/5L6aBHz9ZYCs4eibk_SAP_DgFtzkq4BPsTowkpE_1633640325187_completion_certificate.pdf

- Created a home lab – Windows 10 virtual machine.
- Installed Windows Server 2019 for administration of Active Directory, server hardening and Group Policies.
- Audited Active Directory identities to determine compliance with NIST 800-63B standards. Identify weak passwords, non-compliance flaws and password false positives for the client's most sensitive accounts.
- Identified indicators and mitigated phishing attempts for clients. Reviewed emails and identified false positives.
- Provided final impact analysis and recommended remediations for the client's identity systems.

NSA 2021 Codebreaker Challenge - Hackathon
Performed security research engineering to Investigate a suspicious IP address communicating with a network of US Defense companies. The NSA believed it to be a listening post linked to foreign cyber actors and these companies may be compromised.

- Created a home lab – Kali Linux virtual machine.
- Inspected pcap files using Wireshark to identify any IP addresses talking to the C2 controller server.
- Performed log analysis of the compromised proxy server and domain controller to identify the user logon ID.
- Analyzed the MD5 header of the phishing email opened by the user. The email contained a PDF with obfuscated PowerShell code.
- Performed Windows registry analysis of EXE files using RegEx and Docker analysis to find other infected systems.
- Reverse engineered the C++ malware code using Ghidra.

Education
Bachelor of Science in Information Technology (Cybersecurity Concentration)
Kennesaw State University – Kennesaw, GA **Expected Graduation: Fall 2023**
Courses Completed:

- Intro to Software Engineering
- Programming Principles (Python)
- Web and Mobile App Security
- Infrastructure Defense
- OPS Concepts & Administration (Linux OS, ELF)
- Programming & Prob. Solving II (C#)
- Database Systems (SQL)
- Web Development (JavaScript, Azure Cloud)
- Data Communication & Networking
- Digital Forensics
- Ethical Hacking Defense
- Hardware & Software Concepts

Security Research Experience

- **Wireshark Lab** – Researched common network protocols used in the packet analysis tool Wireshark. Inspect the packet captures to distinguish normal vs anomalous behaviors and propose solutions. **Protocols reviewed**: DNS, HTTP/TLS, PPPoED, PPP LCP, ICMPv6, TCP, EAP, UDP.
  https://github.com/MikedaMachine/Wirehark-Research-Lab

- **Snort Custom Rules Lab –** Created and configured custom alerts based on the Snort rules language. This allowed alerts to be generated on host and network based intrusions in the Security Onion IDS.
  https://github.com/MikedaMachine/Snort-Custom-Rules-Lab

- **Blockchain Research Paper** – Discussion of the impact Blockchain has on securing infrastructure to defend against future cyber-attacks. Topics include cryptography, incident response, zero-trust, and intrusion detection.
  https://github.com/MikedaMachine/Blockchain-Impact-on-Securing-Infrastructure/blob/main/Blockchain's-Impact-on-Securing-Infrastructure.pdf

- **IAAS Research Paper** – Discussion of Infrastructure as a Service https://github.com/MikedaMachine/Infrastructure-as-a-Service-IAAS-/blob/main/Research%20Paper_IaaS.pdf

- **Cross-Site Scripting Paper** – Discussion of a real-life incident where cross-site scripting was used and offers preventative solutions to the vulnerability. https://github.com/MikedaMachine/OWASP-Vulnerability-Cross-Site-Scripting/blob/main/Cross-Site%20Scripting.pdf

- **Web Anonymity Lab** - Demonstrated how Tor browser anonymizes web browsing. Used Wireshark to observe network data packets masked by Tor Routing Technology. https://github.com/MikedaMachine/WEB-ANONYMITY-LAB--USING-WIRESHARK-TO-OBSERVE-TOR-DATA-PACKETS

- **Enumerating SMB Lab** - This lab addressed the vulnerabilities of NetBIOS, Samba SMB server and how to exploit them. Ethical hacking practices were conducted using various tools to perform the following tasks:
    1. Enumerating the Samba Server with enum4linux
    2. Cracking Samba User passwords with xHydra (brute-force tool).

  https://github.com/MikedaMachine/Enumerating-SMB

Work Experience

October 2014 – present

Material Control Specialist III / **Gulfstream Aerospace (General Dynamics)**

- Conduct risk analysis on vendor documentation to identify potential delays and meet compliance requirements.
- Utilize the SAP ticketing system to create and support supply chain action requests.
- Support the production manufacturing schedule of G650 & G700 aircraft by coordinating delivery of materials shipments to meet planned and unplanned demand.
- Communicate weekly status of material backlogs to senior managers and stakeholders. I also prioritize and delegate action items to team members. This allows me to drive successful outcomes to support the initial phase completion payment of $10 million.
- Lead the materials department on training initiatives to certify an average of 3-5 team members yearly. They go on to accept job roles as planners, analysts, material leads, and mechanics.
- I am a Certified Receiving Inspector and Quality Control stamp holder (FAA approved)
- Use SAP Global ERP system to perform all receiving functions for purchase orders, non-stock parts, loans/DMT, and internal stock transfers. Uphold FAA and ITAR government regulations for aircraft manufacturing.