# WYATT W. TAUBER – me@wyatttauber.com

(218) 536-1570 · Backus, MN · wyatttauber.com · blog.wyatttauber.com · github.com/wwt9829

## Professional Summary

Fifth-year honors BS/MS Computing Security student making technology more secure and accessible for everyone.

- Professional-level security practitioner and analyst certifications (DoD 8140/CNSS 4011)
- Specializations in network security, vulnerability analysis, threat hunting, and development
- Recipient of national entrepreneurship, scholarship, and service awards
- Member of national defense, security, robotics, and STEM education organizations

## Skills and Qualifications

**Certifications:** GIAC GSEC, GCIH, CompTIA CASP+, CySA+, PenTest+, Cisco CCCOA, CCNA (Security, Devices)
**Languages:** Assembly (MIPS, x86), Bash, C, Java, MATLAB, P4, PowerShell, Python, SQL
**Technologies:** ANB, Autopsy, Cuckoo, Docker, , FTK, IDA, Kali, Jupyter, SIFT, Snort, Volatility
**Communication:** Agile, Curriculum Development, Metacognition, Public Speaking, Technical Writing

## Education

**BS/MS Computing Security,** Rochester Institute of Technology, Rochester, NY *(December 2022)*
GPA 3.68/4.0, Math Minor, Accelerated Dual Degree, CyberCorps Scholarship for Service

## Experience

***Operations Development Program**, United States Government, Washington, DC (December 2022)*

**Cooperative Education Development Program,** United States Federal Government, Washington, DC

Offensive Operations Tour; April – August 2022

- Emulated an advanced persistent threat to evaluate defenses of customer networks
- Conducted recon, gained access, and maintained persistence to meet customer objectives
- Evaluated customer detection capabilities to determine if defenses alert on the activity
- Hunted for indicators of compromise in customer networks during the evaluation

Research & Development Tour; January – March 2022

- Leveraged generative ML (GML) training sets and evolutionary properties across capabilities
- Investigated GML applications in the malware analysis domain with academic partners
- Explored methods to analyze network defense data in cyber GML-based capabilities
- Employed GML algorithms and generated data to produce and evaluate efficient ML models

Defensive Operations Tour; May – August 2021

- Toured with the threat identification & characterization (TIC) team
- Assigned to attribute unidentified suspicious or malicious digital network activities
- Worked with other government partners to define TTPs for two threat actor campaigns
- Assisted with producing 13 activity reports, one selected for organization director briefing

Enterprise Architecture Tour; August – December 2020

- Toured with the learning management system (LMS) team
- Tasked with implementing QA and security monitoring solutions for the LMS
- Oversaw the deployment of performance monitoring on three LMS platforms
- Decreased the team's recurring error and downtime rates by 25% over 5 months

**Network Technology & Security Intern**, The MITRE Corporation, Bedford, MA
May – July 2020; National Security Engineering Center (NSEC)

**Computer Security Engineer Intern,** Parsons Corporation, Centreville, VA
June – August 2019; Cyber Operations, Parsons Government Services

## Featured Project

**CryptoRhythm PayPal Scam Takedown**, December 2020, *https://link.wyatttauber.com/cryptorhythm*
Leveraged an unencrypted administrator portal and a PHP RCE vulnerability on a fake PayPal site to disrupt the scam and delete victim information. Recovered IDs and PII sent to PayPal to alert customers.