Matthew Schramm

6910 N Loop 1604 W, TX 78249 • matthewmschramm1@gmail.com • 708-270-3004
Matthew Schramm | LinkedIn

OBJECTIVE

Ambitious Computer Science student with a strong foundation in Cybersecurity, seeking an internship position focused on blue teaming and SOC operations. Eager to apply and expand skills in protecting and optimizing critical infrastructure through proactive defense strategies and real-time threat monitoring.

EDUCATION

Bachelor of Science, Major in Computer Science; Concentration in Cyber Operations **San Antonio, TX**
Minor in Foreign Language (Japanese) **2022-2026**
The University of Texas at San Antonio, GPA: 3.81

CERTIFICATIONS

- **HTB Certified Defensive Security Analyst (CDSA)**
- **CompTIA Cybersecurity Analyst+ (CySA+)** **Expires: Jan 2027**
- **CompTIA Security+** **Expires: Jan 2027**

PROJECTS

Active Directory & SIEM Homelab **May 2024-Present**

- Implemented an Active Directory (AD) environment to simulate enterprise network conditions. Configured multiple domain controllers, organizational units (OUs), group policies objects (GPOs), and user accounts.
- Integrated AD logs with both Splunk & Elastic Stack and created custom alerts and dashboards for analyzing and monitoring various AD-related attacks involving authentication events, group changes, etc.
- Performed various AD enumeration and attacks such as Pass-the-Hash (PtH), Pass-the-Ticket (PtT), Kerberoasting, DCSync, and more using tools like Mimikatz, Rubeus, and the Impacket Toolkit to identify and remediate vulnerabilities and security misconfigurations within the AD environment

Malware Analysis & Reverse Engineering Lab **July 2024-Present**

- In-depth static and dynamic analysis of malware samples using FlareVM for Windows and REMnux for Linux.
- Analyzed network traffic through Wireshark and Zeek to identify Command & Control communication patterns and data exfiltration channels stemming from Cobalt Strike beaconing activity and other malicious C2 DNS and HTTP communication channels.
- Disassembled malware using tools like IDA Pro and x64dbg to analyze its code structure and used YARA to create custom rules for detecting unique malware strings and patterns.

EXPERIENCE

DOE CyberForce Competition Team **Aug 2024-Present**

- Leading Windows Threat Hunting operations using Sysmon, Event Viewer, and SIEM platforms to proactively detect, analyze, and mitigate security incidents ahead of the Department of Energy's CyberForce competition.
- Configured and deployed MITRE's CALDERA to simulate adversarial tactics, techniques, and procedures (TTPs) used by advanced persistent threats (APTs), reinforcing incident response strategies.

ADDITIONAL INFORMATION

- **Technical Skills:** Splunk, ELK, Sigma, Suricata, Snort, Autopsy, FTK, Velociratpor, Volatility, IDA
- **Programming Languages:** C, Java, Python, Bash, x86 Assembly, SQL, Swift
- **CTFs:** NCL - Spring 2024 Individual Game (Placed 80 / 7406)