Andrew Frank

Delray Beach, Florida ▪ andr3wfrank@protonmail.com ▪ (561) 809-1578

EDUCATION

B.S. Cybersecurity | University of South Florida, Tampa, FL
Major GPA: 4.0 | **Overall GPA:** 3.61 | **Graduated with Honors Cumlaude** *May 2024*

SKILLS

Programming: PowerShell, Bash, Python, C, XML, MySQL, Microsoft SQL, Regex
SIEM Tooling & Data Analysis: Splunk, Zeek, Graylog, Elastic, YARA & Sigma Rules, Carbon Black
SOC Operations: Windows Event Log Analysis, Threat Hunting, Triage Investigation, SPL Queries, KQL Queries, Sysmon Log Configuration, Malware Analysis in IDA, Rapid Triage, Sandboxing
Networking & Infrastructure: OPNSense Firewall, Docker, Active Directory, VMWare
Networking Tools: Wireshark, Tcpdump, Nmap, Traceroute, Nslookup, Netcat, SSH

EXPERIENCE

Mentor/Competition Team | Whitehatters Computer Security Club, Tampa FL
October 2021 – May 2024

- Engaged in Cybersecurity Competitions to perform System Hardening for Windows/Linux OS + remediating infected machines.
- Practiced Red-Team topics ranging from Binary Exploitation, Breaching Windows Active Directory, and Web Penetration testing on OSCP practice boxes to enhance understanding of offensive security techniques and tactics.

SOC Labs Analyst | ReliaQuest, Tampa FL
March 2023 – April 2023

- Authored a comprehensive post-incident report detailing findings, attack vectors, and impacted systems that was later delivered to non-technical stakeholders.
- Utilized XDR detection tools to analyze log information, threat hunt events, & created alerts to enhance threat detection & response capabilities using enterprise security tools.
- Collaborated with four SOC team members via Slack channels to streamline incident response processes, share critical updates, and ensure timely task resolution.

Student | Hack The Box Academy, Remote
June 2024 – Present

- Simulating a SOC environment where I used the Elastic Stack to perform real-time threat detection, log analysis, designing incident timelines, correlating logs from different sources, and designing YARA/Sigma rules to identify malicious activities within an enterprise network.
- Working through various incident response scenarios, including investigating compromised systems, analyzing malicious binaries such as the PowerSploit exploitation framework, and escalation performed in Active Directory, preparing detailed reports for remediation efforts at the end of investigations.
- Building a custom SIEM dashboard to aggregate logs from various sources(Suricata, Zeek, Sysmon, http streams), set alerts, create detection rules, and perform threat analysis.

CERTIFICATIONS

CompTIA Security+ *September 1st 2024*

KEY PROJECTS

CapyClub *January 2024 – April 2024*

- Built a Docker multiplayer game that runs on Godot4 with a NodeJS API that utilized network ports & services connected by virtual containers. The game was accessible via browser through Godot’s application.