Ethan Couch

Tampa, FL • (813) 997-3109 • couch1@usf.edu • [GitHub](#) • [LinkedIn](#) • [Personal Website](#)

EDUCATION & CREDENTIALS

University of South Florida - **3.9 GPA**   B.S. in Cybersecurity - 2023
CompTIA Certified **- Security+**   September 2022 - 2025
Awards
USF Dean's List (2020, 2022) • USF Director's Award • USF Scholars Award • USF Business Ethics Scholarship
Herbert & Elaine Gimelstob Scholarship • Computing Partners Program Scholarship • Florida Academic Scholar

SKILLS

Analytical Skills
- Reporting & Technical Writing
- Memory Forensics
- Network Traffic Analysis (Wireshark)
- OSINT & Sandboxing

Technologies/Environments
- Splunk, QRadar, LogRhythm
- ServiceNow
- SentinelOne, CrowdStrike, Microsoft ATP, CarbonBlack
- MySQL, AWS
- Windows and Linux System Administration

Pentesting Tools
- Burpsuite & ZAP
- Metasploit
- Nmap
- Nessus
- Kali Linux
- FFuF

Programming Languages
- Python
- HTML + JavaScript
- PowerShell
- C & C#
- Java

RELEVANT EXPERIENCE

ReliaQuest, Tampa - Florida   ***Security Analyst Intern*** (June 2022 - August 2022)
- Utilized Splunk, QRadar, LogRhythm, and Exabeam to analyze outlying activity within the application/authentication logs of **10** customer environments.
- Collaborated with **~10 customers** to *triage* and *prevent* incidents using *EDR* tools such as Crowdstrike, SentinelOne, and CarbonBlack.
- Employed skills in **sandboxing** (ANY.RUN), **OSINT** (VirusTotal, Cisco Talos), and automated playbooks to run remediating campaigns against prevalent customer threats.

Key Achievement:
Built **_SIEM queries_** using Splunk, SentinelOne, and Exabeam search syntaxes to *evaluate* true positive IOCs **(~20%)**.

Whitehatters Computer Security Club, USF   ***Secretary*** (December 2021 - December 2022)
- Fostered knowledge on utilizing the Volatility framework for memory analysis/incident response challenges following **6 Chapters** of *The Art of Memory Forensics.*
- Orchestrated a custom CTF teaching high school students foundational technical skills within cybersecurity in Florida districts **(50+ high school students taught).**
- Led **3** educational meetings on *system hardening & scripting* (Powershell), system administration, and virtualization.

Key Achievement:
As a leader of the Whitehatter's Public Relations committee, I led the expansion of our club in terms of member count **(5 to 100+)** and knowledge base, and have established a lasting *funding partnership* (**$16,000/yr**) for our club.

PROJECTS & ACTIVITIES

CAE-NCX Cyber Competition, *NSA*
- Participated in a 4-day long cybersecurity competition which challenged skills of software development, packet analysis, cryptography, computer forensics, and active cyber offense/defense. Our team **placed 2nd in the nation**.

Cyberforce Competition, *Department of Energy*
- **Placed 35th nationally** in the Fall 2021 Cyberforce Competition. *Team captain* of the Fall 2022 Cyberforce Competition. Competition trained system hardening skills of multiple AWS-governed virtual machines.

Hivestorm Cyber Defense Competition, *Remote*
- **Placed 33rd/300** in the 2021 Hivestorm competition; placed 50th/300 in the 2022 Hivestorm competition.

Home Lab Maintainer, *Personal*
- Built a **home lab** comprised of a server, server rack, and switch. Currently using Proxmox to *administrate* many virtual machines, of which are responsible for a *DNS sinkhole*, a *log collector*, and a *virtualized honeypot*.

Project Lead, USF
- Led a 6-week project in building a robotic deliverable implementing Arduino code and sensor-based navigation.