Ethan Couch Tampa, FL • (813) 997-3109 • ethanccouch@gmail.com • GitHub • LinkedIn • Website

EDUCATION & CREDENTIALS

University of South Florida, *Honors College* - **3.91 GPA;** *Summa Cum Laude* B.S. in Cybersecurity - **Graduated 2023**
CompTIA Certified **- Security+, CySA+ (CSAP)** **Active** from September 2022 - 2025

Awards

USF Dean's List (2020, 2022, 2023) • USF Director's Award • USF Scholars Award • USF Business Ethics Scholarship
Herbert & Elaine Gimelstob Scholarship • Computing Partners Program Scholarship • Florida Academic Scholar

Security Clearance

DoD **Secret** Clearance (**Active** as of August 2023) • **DHS--EOD** Granted (**Active** as of August 2023)

PROFESSIONAL EXPERIENCE

The MITRE Corporation, McLean Virginia ***Cyber Operations Intern*** (May 2023 - Current)

- Developed and optimized **detection analytics** aligned with the MITRE **ATT&CK** framework and MITRE's internal analytics repository in **Sigma** and **Splunk** formats.
- Served as a consultant to a **DoD** agency, providing advancements in areas of network traffic capture, encrypted traffic analysis, **threat detection**, and incident response protocols. Provided templated threat reporting guidance derived from CISA incident response protocols and the **MITRE D3FEND** matrix.
- Gained expertise in **embedded systems** design and **C** programming via MITRE's eCTF competition, performing firmware extraction and **hardware exploitation**.

Key Achievement:
Enhanced government threat hunting initiatives by developing 30+ **threat intelligence playbooks** that offer guidance across cyber operations of **threat detection** and **emulation**, incident response, and network artifact collection. All playbook deliverables were dynamically rendered in a **Node.js** tech stack with a **REACT** front-end & **Express** back-end**.**

ReliaQuest, Tampa Florida ***Incident Response Intern*** (March 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 Falcon XDR, 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%)**.

SKILLS

Analytical Skills
- Technical Writing (CTI)
- Memory Forensics
- Traffic Analysis
- System Administration
- OSINT
- Threat Detection
- Security Monitoring
- Sandboxing

Technologies/Environments
- **SIEMs:** Splunk, QRadar, LogRhythm, Exabeam
- ServiceNow, MySQL, AWS, VMware VSphere
- **EDR:** SentinelOne, Falcon Insight XDR, Microsoft ATP, CarbonBlack
- Kali Linux
- Windows Active Directory
- Cisco CLI
- Azure Active Directory

InfoSecTools
- Burpsuite & OWASP ZAP
- Metasploit
- Nmap & Nessus
- Wireshark
- Volatility Framework
- Cisco Packet Tracer
- MITRE ATT&CK

Programming Languages
- Python
- HTML + CSS
- JavaScript - React, Node.js
- PowerShell
- C, Embedded C
- Java, C#
- Sigma Rules
- YAML

PROJECTS

Cybersecurity Home Lab, *Personal*

- Built a **home lab** consisting 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*.

FourFlyer, USF

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

SkyScraper, *Personal*

- Developed SkyScraper-- an 8-week collaborative project developed in a sprint by a team of four. SkyScraper encompassed the development of a **Python-based** web scraper, **UML** diagram utilization, **API** integration, and simplistic UI. The end product is a dynamic tool for comparing airline ticket prices based on *user input.*

TryHackMe, *Top 7%*

- I have completed several learning paths and cybersecurity rooms across the **TryHackMe** platform, netting me a placement among the **top 7%** of users on the platform.

INVOLVEMENTS

Whitehatters Computer Security Club, USF ***Secretary*** (December 2021 - December 2022)

- Fostered knowledge on utilizing the Volatility memory forensics 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 cybersecurity knowledge, while also having established a lasting *funding partnership* for the club.

Protocol Security, *Tampa FL* ***Co-Founder*** (December 2022 - Present)

- Established an independent cybersecurity community focused on sharing knowledge related to information security and SWE, as well as competing in national and local CTFs.
- Held various meetings focusing on **Hack The Box,** web application penetration testing, and active directory exploitation challenges. Attended various *BSides* security conferences to compete in accompanying CTFs.

USF Judy Genshaft Honors College, *USF*

- Conducted undergraduate thesis research examining artificial intelligence, human interaction, and ethical dilemmas that arise from their synergy (*Artificial Intelligence - The Hybrid of Humanity and Technology)*. Received various scholarships, derived from the completion of **2** theses and graduation with honors distinction.

CAE-NCX Cyber Competition, *NSA/CAE*

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

Saint Leo University CTF, *Saint Leo University*

- **Placed 2nd** out of six teams in a local collegiate competition that challenged participants in fields of memory forensics, web application penetration testing, and cryptographic algorithm exploitation.

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 across 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.

Mentor Collective, *USF*

- Served as a dedicated mentor for undergraduate students, providing guidance in various computer science and engineering-adjacent disciplines, including SQL databases, conceptual physics, precalculus, and virtualization.