

## CONTACT

San Diego, CA

720-318-3311

[linkedin.com/in/celine-tannous-34a44a1a7/](https://linkedin.com/in/celine-tannous-34a44a1a7/)

[github.com/ObsidianNull](https://github.com/ObsidianNull)

[www.celinetannous.com](http://www.celinetannous.com)

## CLEARANCE

TS/SCI — ACTIVE

## CERTIFICATIONS

CompTIA Security+

## SKILLS

### SECURITY

Network Security  
Vulnerability Analysis  
Incident Response  
Threat Modeling

### SYSTEMS

Linux / Windows  
Virtualization  
SIEM Concepts

### CODE

Python  
C

# CELINE TANNOUS

CYBERSECURITY PROFESSIONAL // FORMER U.S. NAVY OFFICER

## PROFILE

Cyber-focused Surface Warfare Officer with experience as a shipboard Cyber Officer and a technical foundation in cyber operations from a CAE-CO accredited program. Operated in high-risk, high-reliability environments securing mission-critical systems and leading technical teams under pressure. Transitioning into cybersecurity roles with interests in adversary emulation, detection evasion, and defensive countermeasures.

## EXPERIENCE

**United States Navy** — Surface Warfare Officer / Nuclear Officer (LT)  
*2021 – Present*

### Cyber Officer — USS HARPERS FERRY (LSD-49)

- Owned shipboard cybersecurity posture, risk assessments, and compliance for operational networks.
- Identified configuration weaknesses impacting mission assurance.
- Coordinated remediation efforts with command leadership and cyber organizations.
- Delivered cybersecurity training to technical and non-technical personnel.

### Reactor Electrical Division Officer — USS CARL VINSON (CVN-70)

- Led 20+ sailors responsible for nuclear propulsion electrical systems.
- Managed fault isolation, redundancy, and casualty response in time-critical environments.
- Executed training programs increasing qualification rates and system reliability.

## EARLY TECHNICAL EXPERIENCE

**General Electric Aviation** — Cyber Analyst Intern

- Performed indicator of compromise (IOC) research to support identification of malicious activity and emerging threats.
- Analyzed emails for indication of phishing, malware, or compromise, and escalated confirmed threats.

**Johns Hopkins University Applied Physics Laboratory (JHUAPL)** —

Cyber / Research Intern

- Supported applied research projects related to cybersecurity and national security systems.
- Assisted with technical analysis, scripting, and documentation in a mission-focused research environment.

## PROJECTS

### Offensive / Defensive Security Lab

- Built virtualized lab using Kali Linux and vulnerable targets.
- Practiced reconnaissance, exploitation, and detection techniques.
- Documented attack paths and mitigations.

### Python Security Automation

- Developed scripts for log parsing, reconnaissance, and data analysis.