

# MICHELLE DUELL

Virginia Beach, VA • michelle.m.duell@gmail.com • (409) 543-3900  
• [linkedin.com/in/michelle-duell](https://www.linkedin.com/in/michelle-duell) • [github.com/aeronique](https://github.com/aeronique) • [medium.com/@aeronique](https://medium.com/@aeronique)

## Professional Summary

Intelligence professional and U.S. Army Reservist with active TS/SCI clearance, transitioning to cybersecurity with strong interest in blue team operations, threat intelligence, and reverse engineering. Self-taught practitioner with demonstrated strong aptitude, proven through SANS Cyber Academy Scholar designation and exceptional competitive performance including 2nd place in the 2025 Target Cyber Defense Challenge and 5th place in the SANS Holiday Hack Challenge. Experienced in analytical workflows, pattern recognition, and structured problem-solving that directly translate to threat hunting, security operations center environments, and incident response. Seeking entry-level cybersecurity analyst positions in blue team operations, threat intelligence, SOC environments, or OSINT analysis to leverage intelligence background, analytical expertise, and self-developed technical skillset.

## Technical Skills

**Defensive Security:** Security monitoring, log analysis, SIEM deployment (Wazuh), IDS/IPS configuration (Suricata), vulnerability assessment (Nessus), network traffic analysis, threat hunting

**Threat Intelligence & OSINT:** Adversary TTP identification, honeypot deployment and analysis (T-Pot), IOC correlation, threat landscape research, open-source intelligence gathering

**Reverse Engineering (basic):** Binary analysis, malware behavior analysis, assembly interpretation, DNS exfiltration techniques

**Infrastructure & Tools:** Proxmox, VMware, Docker, Active Directory, MITRE Caldera, Metasploit, Ghidra, Python scripting (basic), bash

**Operating Systems:** Windows 10/11, Linux (Kali, Ubuntu)

## Certifications & Training

- **SANS Cyber Academy Scholar** | GIAC Certified Incident Handler (GCIH) in progress, expected March 2026
- **GIAC Security Essentials (GSEC)** | December 2025
- **GIAC Foundational Cybersecurity Technologies (GFACT)** | October 2025
- **ISC<sup>2</sup> Certified in Cybersecurity (CC)** | June 2025
- **Google Professional Certificates** (Cybersecurity, IT Support, AI Essentials) | 2025

## Professional Experience

**Geospatial Intelligence Analyst | U.S. Army Reserve** Norfolk, VA | June 2018 to Present | TS/SCI Clearance

- Serve as Joint Intelligence Targeting Staff (J2T) member conducting strategic and operational-level targeting for combatant command operations
- Lead Joint Targeting Team of 9 personnel, coordinating cross-functional intelligence production and delivering targeting packages to operational commanders
- Author detailed intelligence reports and briefings for senior leadership requiring clear technical writing and complex information synthesis
- Analyze satellite and aerial imagery using pattern recognition and anomaly detection techniques directly applicable to network traffic analysis and threat hunting
- Apply intelligence cycle methodologies (collection, analysis, dissemination) mirroring threat intelligence lifecycle, including IOC identification and adversary TTP mapping
- Conduct multi-source data correlation and research using analytical techniques similar to SIEM log correlation and security event analysis

**Advanced Mapper (Volunteer) | National Geospatial-Intelligence Agency** GEMINI Program | May 2020 to Present

- Maintain and enhance open-source intelligence maps using research approaches aligned with cyber threat intelligence collection and OSINT reconnaissance

## Cybersecurity Projects & Achievements

### Competitive Achievements

- **2nd Place Overall** | 2025 WiCyS x Target Cyber Defense Challenge
- **5th Place** | 2025 SANS Holiday Hack Challenge
- **Top 5%** | 2025 DoD Cyber Sentinel Challenge (116/2155)

### Technical Projects

- **Security Operations Homelab** | Self-designed Proxmox infrastructure with Wazuh SIEM, Active Directory, vulnerable systems (Metasploitable, DVWA), and MITRE Caldera for purple team operations
- **Network Security Lab** | Configured network segmentation with VLANs and Suricata IDS/IPS for defensive monitoring
- **Cloud Threat Intelligence** | Deployed T-Pot honeypot on GCP to capture live attack traffic and analyze adversary TTPs

### Speaking Engagements

- **"Reverse Engineering with Ghidra for DNS Exfiltration", WiCyS 2026 Conference** | Co-presenting 45-minute technical session covering novice to professional reverse engineering methodologies, Washington, DC

### Technical Writing & Publications

- Author technical reports and analysis documenting CTF challenge solutions, honeypot deployment findings, blockchain security research, and homelab infrastructure. Published 6 articles at [medium.com/@aeronique](https://medium.com/@aeronique)

## Education

**Undergraduate Certificate, Computers and Networking** | American Military University (GPA: 4.0) | 2022

**Associate of Applied Science, Intelligence Operations** | Cochise College | 2019

**Master of Music Education** | Lamar University | 2010

**Bachelor of Music Performance** | Lamar University | 2007

### Professional Affiliations

GIAC Advisory Board • Military Cyber Professionals Association • Women in CyberSecurity (WiCyS) • VetSec • Military Intelligence Corps Association

### Other Work Experience

**Assistant Band Director | Nederland Independent School District** Nederland, TX | 2010 to 2015

- Led highly successful band program of approximately 500 students, earning multiple regional and state recognitions for performance excellence
- Developed curriculum, managed student performances, and coordinated community outreach programs
- Demonstrated strong leadership, organizational skills, and cross-functional collaboration with administrators, parents, and community stakeholders