

JAVIER NAPOLES

Stamford, CT | (929)-202-6220 | github.com/jnapafx | jnapafx@gmail.com | English & Spanish

ABOUT ME

Cybersecurity professional in training specializing in SOC operations, threat detection, and vulnerability management. I have hands-on experience building and managing simulated SOC environments that integrate SIEM tools, IDS/IPS, log correlation, and threat intelligence workflows—closely mirroring real-world security operations.

With a 10-year background in design and post-production, I bring strong problem-solving skills, attention to detail, and the ability to communicate complex ideas clearly and visually. Now transitioning into cybersecurity, I'm driven by the challenge of protecting systems, learning advanced defensive techniques, and growing into a well-rounded security professional committed to continuous improvement and real-world impact.

TECHNICAL SKILLS

SIEM & Monitoring: Wazuh, Splunk, ELK Stack, Grafana

Threat Intelligence: OTX, MISP, AbuseIPDB

Attack & Assessment: Nmap, Hydra, Metasploit, OpenVAS, Nessus

Firewalls & Segmentation: iptables, UFW, Windows Firewall

Incident Response: Rule tuning, triage, IOC analysis, remediation

Systems & Virtualization: UTM, Parrot OS, Kali Linux, Windows, MacOS

Programming & Productivity: Python (basic), HTML/CSS, GitHub, Notion, Terminal

Design Tools: Adobe Creative Suite (Photoshop, Illustrator, InDesign, Premiere Pro, After Effects), Figma.

TECHNICAL PROJECTS

Divide & Defend: SOC Lab Project with Micro-Segmentation & Real-Time Monitoring 2025 – Capstone Lab Project

- Built a home-based SOC lab with multiple VMs simulating attacker, victim, and SIEM nodes
 - Deployed Wazuh as the primary SIEM, with custom detection rules for brute-force, privilege escalation, and unauthorized access
 - Simulated attacks using Nmap and Hydra; captured logs from Windows and Linux agents
 - Implemented micro-segmentation with UFW, iptables, and Windows Firewall for traffic isolation
 - Conducted incident triage and threat hunting with OTX, MISP, and AbuseIPDB
 - Performed vulnerability scans using Nmap and OpenVAS
 - Integrated Grafana dashboards with Wazuh to visualize real-time SOC metrics and detection trends
 - Configured alerting workflows in Grafana to send notifications directly to Discord channels for faster incident response
 - Delivered a professional report with IOC analysis, detection dashboards, and remediation plans
-

PROFESSIONAL EXPERIENCE

IT Support (Freelance / Contract)

Malcan Physical Therapy (2023-2024)

Redesigned and manage the clinic website, SEO, UI, and security settings. Provide IT support including DNS, email setup, Cloudflare security, hosting management, and troubleshooting. Improve staff workflows and brand consistency.

Photographer & Graphic Designer

SSNUS, Norwalk, CT | 2020 – Present

Lead product photography and visual content for marketing. Manage multiple deadlines and projects simultaneously. Strong organization, documentation, and communication—directly applicable to SOC workflows.

Post-Production Editor

Aventura TV, Venezuela | 2015 – 2017

Edited broadcast content under tight deadlines. Developed precision, consistency, and process discipline.

CERTIFICATIONS & EDUCATION

Faculty of Architecture and Design – La Universidad del Zulia

B.A. in Graphic Design

2015 | Maracaibo, Venezuela

Google Cybersecurity Certificate – Coursera

2024 | Stamford, CT

DAE Cybersecurity Program – SOC Analyst Track

2025 | Stamford, CT

CompTIA Security+ (SY0-701)

February 2026

Microsoft Certified: Security Operations Analyst Associate (SC-200)

In Progress