

JAVIER NAPOLES

Stamford, CT | [LinkedIn](#) | [jnapfx.github.io](#) | [github.com/jnapfx](#) | [jnapfx@gmail.com](#) | English & Spanish

ABOUT ME

Cybersecurity professional in training specializing in SOC operations, threat detection, and vulnerability management. Experienced in building simulated SOC environments integrating SIEM, IDS, and threat intelligence. Transitioning from a 10-year design career to cybersecurity to pursue new challenges, expand my skills, and continue growing both personally and professionally.

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,

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 & Website Support – Malcan Physical Therapy (2024 – Present)**
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) — Currently preparing**
(expected January 2026)