Alex Lopez

alexmlopez7823@gmail.com • 626-879-5565
https://linkedin.com/in/alexmlopez7823 • https://alexmlopez-tech.com

Professional Summary

Cybersecurity-focused IT professional and U.S. Army Apache pilot with 7+ years of experience operating and securing mission-critical systems under high-stakes conditions. Holds CompTIA A+, Network+, Security+, and CySA+ certifications with hands-on academic exposure to threat analysis, incident response, vulnerability assessment, GRC, and cloud security. Currently pursuing a B.S. in Information Technology at Georgia Southern University. Seeking a cybersecurity position where military discipline, a strong certification foundation, and practical lab experience can contribute to real-world security operations and risk management.

Education & Certifications

B.S. Information Technology | Georgia Southern University | Projected Date of Graduation: **May 2027**
A.A. General Studies | American Military University | Graduated: **May 2020**
Certifications: **CompTIA A+, Network+, Security+, CySA+, CIOS, CSIS, CSAP**

Technical Skills & Proficiencies

- SIEM & Log Analysis
- Incident Response
- Threat Analysis & Hunting
- Risk Management & GRC
- Firewalls & IDS/IPS
- Vulnerability Assessment
- Malware Analysis
- Security Monitoring
- Behavioral Analytics
- Cloud Security (AWS/Azure)
- Access Control & IAM
- Active Directory
- Security Documentation
- System Hardening
- Security Compliance
- Information Security
- Risk Mitigation
- Scripting (Python/JS)
- Security Compliance
- Incident Response

Professional & Military History

Apache Pilot & Mechanic: U.S. Army March 2018 – Present

- Operate and navigate AH-64 Apache helicopters in mission environments, maintaining crew safety and mission success.
- Diagnose and remediate mechanical, electrical, and computer system failures under high-pressure conditions — directly analogous to identifying and resolving technical vulnerabilities in critical systems.
- Execute system upgrades and preventive maintenance programs to sustain operational readiness — mirroring proactive security posture management and patch management practices.
- Inspect aircraft systems to detect anomalies and implement corrective measures before mission impact — applying a threat-detection mindset to mission-critical infrastructure.
- Train and mentor soldiers on technical procedures, safety protocols, and system operations — experience directly transferable to security awareness training delivery.
- Handle and safeguard sensitive mission data, classified communications, and restricted operational information in compliance with military security protocols.

Awards: *Army Commendation Medal with "C" Device, Army Achievement Medal, Army Good Conduct Medal, National Defense Service Medal, Global War on Terrorism Service Medal, Afghanistan Campaign Medal with Campaign Star, NCO Professional Development Ribbon, Army Service Ribbon, Overseas Service Ribbon, NATO Medal, Combat Action Badge, Basic Aviation Badge, Inherent Resolve Campaign Medal with Campaign Star*

Projects and Coursework

The following reflects lab-based and coursework experience developed through academic study in IT and cybersecurity:

- Conducted threat analysis and vulnerability assessments using industry-standard security tools, identifying and remediating risks across simulated enterprise environments.
- Participated in incident response exercises following NIST SP 800-61, including threat hunting, containment, eradication, and post-incident reporting.
- Deployed and configured security monitoring tools including Snort IDS, Windows Event Viewer, rsyslog, and Tripwire for real-time detection and log analysis.
- Performed attack simulations (XSS, SQLi, Meterpreter, DDoS, SET phishing) and practiced corresponding defense, containment, and mitigation strategies.

- Conducted system hardening exercises including patching, access control configuration, and security baseline implementation to reduce attack surface.
- Configured AWS and Azure cloud environments including IAM policies, network security groups, CloudTrail logging, and cloud-native security services.
- Developed and maintained security documentation including lab reports, assessment findings, and procedural write-ups aligned with GRC frameworks.
- Assessed third-party risk exposure through vendor security evaluation exercises, applying risk scoring methodologies and mitigation recommendations.