Antonio Monje
Cell Phone: (951) 805-9388 | Email: amonje@alumni.usc.edu
Clearance Level: Secret

EDUCATION
• Master of Science in Cyber Security Engineering, University of Southern California
• Bachelor of Science in Computer Science, California State University San Marcos

TECHNICAL SKILLS
Programming Languages: C++, Python, C#, Go, Rust, Java
Technologies & Tools: Linux, Unix, Windows, Visual Studio, Emacs, Jira, Wireshark, Qualys, Metasploit, Nmap, OSSEC (HIDS), Rapid7, Nexpose, Wifite, Hashcat, Azure, Virtual Machines, VMware, DevSecOps, SIEM, Wazuh, ELK Stack, Docker, Kubernetes, OpenShift, RHEL, Tekton, Artifactory, ZAP, Coverity, Grafana, Prometheus, OIDC, OAuth2.0, ForgeRock, Terraform, AWS, Ansible, SAST, DAST
Certifications: Security+ (2023)

PATENTS & RESEARCH
• Patent: "Complete Data Exfiltration Profile and Model (CODAEX)" (Navy Case 113598, Awarded 2023)
• Patent Application: A Distributed Quantum Evaluation Network (Navy Case 212170)
• Patent Disclosures: Blockchain security applications (Navy Case 212084)
• Publication: "Being a Bad Influence on the Kids: Malware Generation in Less than Five Minutes Using ChatGPT" (Lead Author)

Professional Experience

Scientist
Naval Information Warfare Center Pacific (NIWC Pacific)
August 2019 – Present

- Spearhead advanced cybersecurity research in SCADA systems, driving innovative initiatives in computer network defense and ensuring system integrity in complex, high-stakes environments.
- Direct comprehensive DevSecOps operations for Matrix Chat, orchestrating secure application deployments across a fleet of more than 40 U.S. Navy vessels.
- Demonstrate exceptional expertise in troubleshooting OpenShift, optimizing Kubernetes performance, and integrating sophisticated OIDC authentication protocols.
- Enhance security measures by incorporating tools such as ZAP, Coverity, Artifactory X-Ray, Grafana, and Prometheus to fortify Kubernetes environments.
- Engineer and implement Tekton pipelines that automate security scanning, thereby ensuring continuous improvement in security posture.
- Deploy and manage AWS instances for IL4 and IL6 testing through Terraform and Ansible, maintaining rigorous security standards on air-gapped and hardened networks.
- Translate complex cybersecurity concepts into actionable insights for Navy leadership, thereby driving consensus among diverse internal and external stakeholders.
- Oversee VR/AR cybersecurity training tool development, including a Wireshark prototype in C#, to elevate training efficacy.

- Serve as principal investigator for multiple DARPA, ONR, and NISE projects, including DARPA OPS-5G, DAISEY, VEGA, DPRIVE, DECEPTI_SCADA, and MADMen.
- Led the ONR program MADmen that utilized MITRE's Caldera and MITRE ATT&CK framework to model attacks on a micro-grid testbed and on a condensed digital twin of the MIT ghost micro-grid model
- Lead an internal research project for a MITRE ATT&CK-trained LLM to enhance security threat filtering capabilities.
- Mentor junior professionals and interns in penetration testing, cybersecurity methodologies, and advanced system diagnostics.
- Develop simulation tools such as a vehicle hacking simulator to educate personnel on CAN bus vulnerabilities, effectively bridging theoretical concepts with practical applications.
- Strengthen encryption protocols and security measures for autonomous unmanned systems within FDAS programs.
- Establish and manage HIDS (Wazuh) and SIEM solutions (Sumo Logic) to ensure proactive cybersecurity monitoring and rapid response to incidents.

Cyber Security Analyst
RSI Security
January 2019 – July 2019

- Conducted comprehensive penetration tests and vulnerability assessments utilizing tools including Rapid7, Qualys, Metasploit, Wireshark, and Hashcat.
- Executed forensic investigations employing Cyber Triage, EnCase, and FTK Imager to support legal and compliance efforts.
- Ensured adherence to HIPAA, PCI, and NIST standards for multiple clients through meticulous security monitoring and compliance verification.
- Managed SIEM, FIM, IDS, and IPS tools, reinforcing the cybersecurity posture of client systems.

System Engineer Intern
ATX Networks
June 2018 – December 2018

- Performed multi-layer network troubleshooting and packet analysis to diagnose and resolve complex system issues.
- Developed and executed rigorous system verification test plans based on R&D specifications.
- Led a comprehensive regression test initiative for a high-profile product, ensuring quality and reliability.

Software Engineer Intern
StratumPoint
January 2018 – May 2018

- Developed an innovative web application for cyber and physical risk intelligence utilizing PHP, JavaScript, and Drupal 7.
- Integrated Google Maps API and coordinated management across multiple databases, ensuring robust data handling and user experience.

Personal Projects

- **Merkle Tree Implementation:** Developed an advanced Python implementation to verify inclusion and consistency, reinforcing data integrity.
- **Secure Data System:** Engineered an AES-encrypted data storage system with RSA-protected keys, showcasing expertise in cryptography.
- **Decentralized Audit System:** Created a secure, blockchain-based audit system with integrated privacy and identity management features.
- **NFT Art Generator:** Designed a Python-based NFT art generator that mints digital assets on the Cardano blockchain.
- **Network Classification Project:** Led a machine learning project in Go and Python to classify network properties, differentiating between decoy and operational machines.
- **AI-Generated Malware Feasibility Study:** Conducted research and successfully developed a ransomware prototype using components generated by large language models, later published on ResearchGate.