ANDRÉS DUARTE ORNELAS

Chihuahua, MX · Open to relocation | Linkedin | andres@doarte.net

SUMMARY

Cybersecurity professional fully available for full-time roles. Completed UTSA in-person residency May 2026; currently finishing Tecnológico de Monterrey's cybersecurity master's part-time/online (expected Dec 2026), which does not require full-time student status. Background in network security architecture, vulnerability assessment, and incident response, with hands-on experience in network simulation and fault diagnosis. Seeking SOC Analyst, Network Security, or IT Support roles.

EDUCATION

University of Texas at San Antonio (UTSA) San Antonio, TX
Master of Science in Information Technology, *August 2025 – May 2026*
Cybersecurity Concentration – Full-time, in-person

- U.S. residency year (2025–2026) of the dual UTSA–Tecnológico de Monterrey Master's in Cybersecurity
- Coursework: Security Risk Analysis, Strategic Management of IT, Data Mining, Cyber Warfare, plus jointly-advised Independent Study research paper

Monterrey Institute of Technology (ITESM) Monterrey, MX
Master's in Cybersecurity – Online, part-time *September 2024 – Expected: December 2026*
Bachelor of Science in Electronics Engineering, Specialization in Cybersecurity *August 2020 – June 2024*

CERTIFICATIONS

Cisco CyberOps Associate Certification November 2023
Cisco Networking Academy

- Demonstrated comprehensive understanding of Security Operations including intrusion detection, analysis, and network monitoring
- Completed 52 hands-on labs (30+ hours) using Security Onion, ELK Stack, and Cisco Packet Tracer

AWS Certified AI Practitioner July 2026
Amazon Web Services (AWS)

- Validated foundational knowledge of AI, ML, and generative AI concepts, including model types, use case selection, and responsible AI practices
- Demonstrated proficiency with AWS AI/ML services (Amazon Bedrock, SageMaker, Amazon Q) and prompt engineering techniques for foundation models

PROFESSIONAL EXPERIENCE

Cybersecurity Trainee August 2024 – December 2024
Dipole Digital, Monterrey, MX & Hermosillo, MX (Hybrid)

- Evaluated risks in production environments and developed tailored mitigation solutions
- Designed and implemented segmented office network using VLANs with DMZ for internet-facing services
- Configured traffic rules to control inter-segment communication and enhance network security
- Performed web vulnerability scanning using Zed Attack Proxy (ZAP) to identify and remediate threats
- Assisted in creating and implementing company-wide cybersecurity policy framework
- Gained hands-on experience in security incident management and response

Cybersecurity Engineering Intern March 2024 – June 2024
Dipole Digital, Monterrey, MX (Remote)

- Conducted comprehensive vulnerability assessments and implemented system hardening strategies
- Documented security findings and provided actionable recommendations to enhance cybersecurity posture

RELEVANT ACADEMIC PROJECTS

Empirical Characterization of a Commercial Coding Agent for CLI-Based OSPF Fault Diagnosis January 2026 – May 2026

- Conducted the first empirical evaluation of a general-purpose coding agent (Claude Code) performing autonomous OSPF fault diagnosis in a traditional, non-SDN CLI environment, addressing a gap in existing LLM network operations research
- Designed a 50-session quantitative experiment using a three-router GNS3/VyOS topology modeled after CCNA 11.6.3, with six simultaneously active faults per session and automated pre/post verification via Netmiko snapshots
- Achieved an effective fault resolution rate of ~97% and a perfect-run rate of ~78% at a mean cost of $0.81/session; zero sessions introduced a configuration regression
- Publicly released experimental materials, router configurations, and analysis scripts at github.com/Doarte45/LLMnetopsLab

Cloud as a Service Commercial and Operative Design August 2023 – October 2023

- Designed multi-cloud service architecture using AWS, Azure, and Google Cloud for company Quanti
- Developed commercial strategy for service delivery and operational framework

Digital Forensic Investigation: "Posthumous Digital Note" Case Analysis August 2025

- Collaborated on comprehensive digital forensic analysis of suspicious death case using industry-standard tools (Autopsy/Sleuth Kit, Volatility, Registry Explorer)
- Analyzed disk images, RAM dumps, and Windows event logs to reconstruct timeline and establish evidence of third-party involvement
- Documented complete chain of custody following ISO/IEC 27037 and NIST SP 800-86 standards

TECHNICAL SKILLS

Cybersecurity: Network security architecture, vulnerability assessment, incident response, security policy development, VLAN segmentation, DMZ configuration

Security Tools: Security Onion, ELK Stack, Zed Attack Proxy (ZAP), Cisco Packet Tracer, Nessus (Basic)

Forensic Tools: Autopsy/Sleuth Kit, Volatility

Networking Technologies: Fortinet, TP-Link, Mikrotik, Cisco, VyOS, GNS3

Programming & Scripting: Python (Basic), C (Basic), MATLAB (Intermediate)

Operating Systems: Linux (Intermediate), Windows

Software & Tools: MS Office (Intermediate), Google Suite (Intermediate), Git

LANGUAGES

Spanish (Native) | **English** (Advanced)