

ABEL MALDONADO REQUENA

(415) 637-3691 ■ abelabmaldonado@gmail.com ■ [LinkedIn](#) ■ [GitHub](#) ■ San Jose, California

PROFESSIONAL SUMMARY

OSCP-certified security engineer specializing in offensive security, AI security, cloud infrastructure/IAM, and DevSecOps. Owns security programs end-to-end and builds the tooling behind them, from cloud posture hardening to autonomous offensive-security systems.

PROFESSIONAL EXPERIENCE

Platform Security Engineer

Stealth Startup

Mar. 2026 - Present
Santa Clara, California

- Built an autonomous offensive-security engine on GKE and GLM-5.3 using a Pydantic agent with 54 ATT&CK-mapped techniques, gVisor-sandboxed exploit execution, and a hybrid RAG stack (BGE-M3/Qdrant) over a 228k-document corpus.
- Led Wiz rollout and a cloud posture audit across 15 exposure classes; hardened estate via least-privilege IAM, VPC Service Controls, and Pod Security, driving CIS benchmark compliance from 66% to 93%.
- Ran internal and external penetration tests and infra security-controls assessments, inventoried internet-exposed VMs and clusters across the cloud estate, and modeled exploitable attack paths in a Neo4j security graph.
- Hardened self-hosted vLLM-serving infrastructure with zero-egress perimeter, per-client API-key RBAC, Linkerd mesh authorization, seccomp; secured the model supply chain by blocking a trojaned Guardrails AI release and isolating MCP tool servers.
- Authored an agentic vulnerability triage engine that enriches DefectDojo findings with NVD, EPSS, CISA KEV, GHSA, KSV, and GTI data, scoring exploitability against an IaC compensating-control graph and auto-managing Jira triage, priority, and SLAs across thousands of findings.

Security Analyst & Administrator

Colegio San Juan Bautista

Dec. 2020 - Aug. 2024
Catacaos, Piura, Peru

- Managed IT infrastructure and administrative operations, overseeing data organization, system access, and user enrollment for the organization.
- Deployed Splunk Cloud for centralized threat monitoring and detection, significantly expanding network visibility and accelerating incident response times.

TECHNICAL SKILLS & CERTIFICATES

Offensive Security: Attack-Path Analysis & Attack Chaining, Web/Database/Cloud/Docker/Active Directory/Kubernetes-Based Penetration Testing (Internal & External), MITRE ATT&CK & ATLAS, External Attack Surface Management, Exploit Development

Cloud Security: CNAPP/CSPM, Cloud-Posture Auditing & Hardening, Exposure-Class Analysis, Custom & Least-Privilege IAM Roles, Workload Identity Federation, Scoped/Zero-Role Service Accounts, VPC Service Controls, Deny-by-Default Egress, Bucket Hardening (UBLA), IAP, VPC Flow & Cloud Audit Logs, Prowler, GCP, AWS, Azure, Secure Infrastructure Engineering

AI Security & Engineering: Self-Hosted vLLM Serving Hardening, CUDA Graphs, FP8 Quantization, Qdrant, Prompt Injection Defense, Pydantic, LangGraph, Deepagents, Langchain, Structured/Guided Decoding, Hybrid RAG, Retrieval-Grounded Eval, Bifrost, Guardrails AI, LLM Red Teaming, Model Guard, Securing Open-Weights Models

Programming & Data: Rust, Golang, Python, PowerShell, Bash, PHP, SQL, MongoDB, Neo4j/Cypher, Kafka, JavaScript, Redis, Valkey, ClickHouse, Elasticsearch, Terraform, Helm, n8n

DevSecOps & Enterprise Security: Docker, Pod Security, NetworkPolicy, Trivy, Linux System Administration & Hardening, Detection Engineering, Elastic SIEM, Firewall Configuration, Incident Response, C4 Architecture

Frameworks & Compliance: NIST CSF, NIST RMF, NIST 800-53, ISO 27001, SSDF, CIS, STRIDE

Certificates: OSCP, CompTIA Security+, AZ-900, Splunk Search Expert

EDUCATION

Master of Science in Cybersecurity

Boston University | GPA 3.94/4.00 | Sep. 2024 - Jan. 2026

Achievements: NCAE CyberGames Team Captain, 2025 East Overflow Regional Winner, Voted Most Valuable Teammate (Invitational & Regional), President, BU MET CyberSec Club