OSCAR DAVID OLARTE FORERO

AI & Cybersecurity Specialist

+57 320 921 9438

osdaolfonabaco@gmail.com

https://osdaolfonabaco-beep.github.io

https://linkedin.com/in/oscar-david-olarte-forero-110292382

Bogota, Colombia

PROJECT EXPERIENCE

"Superhuman" AI Security Gateway

Independent Portfolio

- Designed and containerized a "defense-in-depth" security proxy (FastAPI, Docker) to sit between users and any LLM (e.g., GPT, Claude).
- Implemented ingress controls to scan and block Prompt Injection attacks using ML-based detection.
- Engineered egress controls to scan LLM responses, automatically detecting and redacting sensitive PII (DLP) and blocking toxic content, solving a critical enterprise adoption risk.

PROFESSIONAL SUMMARY

A highly motivated professional pivoting from a 4-year career in the US financial sector (Capital One) to **AI & Cybersecurity**. My background in business administration and C1 English proficiency allows me to bridge complex business goals with deep technical execution.

I am now fully focused on a technical career, with a proven portfolio of building, automating, and securing enterprise-grade systems using AWS, Terraform, Docker, and AI.

TECHNICAL SKILLS

Cloud & DevOps:
AWS (Lambda, S3, Boto3, CloudTrail), Terraform (IaC), Docker, Serverless Architecture, GitHub Actions

AI & Data Engineering:
Python (FastAPI, Pandas), AI Security, LLM Integration (LangChain), Data Pipelines, SQL (SQLite)

Cybersecurity:
Security Automation, Log Analysis, Threat Intelligence, Offensive AI Security, Data Loss Prevention (DLP)

Autonomous SOC Analyst Agent

Independent Portfolio

- Automated the complete Level 1 SOC Analyst workflow, ingesting AWS CloudTrail logs to detect login anomalies (e.g., suspicious IPs).
- Orchestrated an autonomous investigation pipeline, enriching anomalous IPs with external threat intelligence from VirusTotal and Geo-location APIs.
- Utilized LangChain and Anthropic Claude 3 to generate executive-ready incident reports, dramatically reducing alert fatigue and human triage time.

AWS Serverless Log Analyzer

Independent Portfolio

- Engineered and deployed a 100% serverless security analysis pipeline on AWS using **Terraform (IaC)** for repeatable, consistent infrastructure.
- Configured S3 event triggers to invoke an AWS Lambda function (packaged as a Docker container) for real-time log processing.
- Automated the analysis of high-volume log files to identify and report suspicious IP frequencies to Amazon CloudWatch.

LogSentinel Cloud Security Data Pipeline

Independent Portfolio

- Built an end-to-end security data pipeline to transform raw logs into actionable intelligence.
- Architected a flow to ingest data from AWS S3, enrich it via threat intel APIs (AbuseIPDB), and persist findings in an SQL database for historical analysis.
- Demonstrated data engineering mastery by generating realistic, large-scale (1M+ lines) datasets with Pandas for robust testing.

PROFESSIONAL EXPERIENCE

PROFESSIONAL & LANGUAGE SKILLS

Language:
English (C1 Certified), Spanish (Native)

Business Acumen:
Business Administration, Process Improvement, Stakeholder Communication

Soft Skills:
Client Relations, Negotiation, Problem-Solving in Regulated Environments

Collections Agent (US Market) *May 2022 – Sep 2025*

Capital One | Bogota, Colombia

- Managed a high-volume portfolio of US-based customer accounts, ensuring compliance with US financial regulations (FDCPA, UDAAP).
- Negotiated complex payment solutions and settlements, consistently meeting or exceeding monthly recovery targets.
- Acted as a primary point of contact for sensitive client data and financial information, maintaining strict confidentiality and data integrity.

EDUCATION

Bachelor of Business Administration (B.B.A.) *Feb 2019 – Feb 2023*

Minuto de Dios University Corporation (UNIMINUTO) | Bogota, Colombia