Oscar David Olarte Forero - Cloud & AI Security Engineer

+57 3209219438 | *oscardavidolarteforero@gmail.com* *https://www.linkedin.com/in/oscardavidolarteforero/* | *https://github.com/osdaolfonabaco-beep* | https://osdaolfonabaco-beep.github.io/ Bogotá, Colombia (Open to Remote - LATAM/Global)

Professional Summary : Highly motivated (C1 English) Cloud & AI Security Engineer with a unique background in Business Administration and experience in highly regulated **US banking environments**. Proven ability to architect, build, and deploy production-grade security solutions from the ground up.Specialized in **Generative AI Security** (PII redaction, prompt injection defense), automated **DevSecOps** pipelines (GitHub Actions, AI code review), and cloud-native threat detection on **AWS** (Lambda, S3, Terraform). Eager to apply a blend of deep technical skill and business risk acumen to a challenging remote role

Technical Skills

- **Cloud:** AWS (S3, Lambda, EC2, IAM, CloudWatch, SQS)
- **DevOps & IaC:** Docker, Terraform (Infrastructure as Code), GitHub Actions (CI/CD)
- **Security & AI:** GenAI Security, Prompt Injection Detection, PII Redaction (Presidio), Threat Intelligence, Log Analysis, Security Data Pipelines, NIST Frameworks, MITRE ATT&CK, OWASP Top 10
- **Languages & Frameworks:** Python (Proficient), FastAPI, SQL (PostgreSQL, SQLite), Streamlit
- **Data & Observability:** Grafana, Prometheus, NLP, RAG, Knowledge Graphs, ETL Pipelines

Security Engineering Experience (Portfolio)

AI Security Gateway (Lead Developer & Architect) | *GenAI Security Portfolio*

- Engineered and containerized (Docker, FastAPI) a production-grade security proxy to protect enterprise LLM usage (GPT, Claude), mitigating critical data loss and compliance risks.
- Implemented a multi-layered defense chain to scan all ingress/egress traffic: detecting **prompt injection** attacks and automatically redacting sensitive **PII** (Presidio) to prevent data leaks.

DevSecOps AI Reviewer (Lead Developer) | *DevSecOps Portfolio*

- Built and configured a complete DevSecOps pipeline in **GitHub Actions** to serve as an AI-powered security reviewer on developer Pull Requests, fully automating the "shift-left" security model.
- Trained the AI (Claude 3) to scan **Python/Flask** code for vulnerabilities (e.g., SQL Injection) and **Terraform** (IaC) files for misconfigurations (e.g., public S3 buckets), posting actionable reports directly in the PR.

Cortex: AI Threat Intelligence Platform (Lead Developer) | *Threat Intel Portfolio*

- Architected a complete ETL pipeline to automate the ingestion, correlation, and analysis of unstructured, multi-source threat intelligence (blogs, reports) from text into an interactive knowledge graph.
- Transformed manual text-based analysis into a dynamic, queryable visual interface, enabling rapid identification of relationships between malware, IPs, and APT groups.

Previous Business Experience : Sales & Client Support Agent (on behalf of Capital One) | *Sutherland Global Services 2021 – 2025*

- Managed sensitive client portfolios for **Capital One (US-based)** within a highly regulated banking environment, ensuring strict compliance and ethical handling of confidential data.
- Conducted all client negotiations and complex communications fluently in **English (C1 Level)**, consistently exceeding performance targets.
- Provided technical context and client-facing support, skills directly transferable to pre-sales and GRC (Governance, Risk, Compliance) roles in technology.

Education & Languages

Bachelor of Business Administration | *Corporación Universitaria Minuto de Dios 2019 – 2023 -*

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