

GUSTAVO DANIEL CORTEZ

Brugge, Belgium | gdcg0021@outlook.com
linkedin.com/in/gdaniel-cortez | github.com/danfromdablock | dcortez.vercel.app

SUMMARY

Hands-on engineer across AI systems, cloud infrastructure, and security. Currently building secure digital solutions at Cor4 Digital: a production on-premise computer-vision safety system that cut false-positive detections from 64 to 1 while raising true detections 7%, running fully offline on client hardware, and an AI-driven WhatsApp/Telegram restaurant reservation platform with a React/TypeScript owner dashboard. Prior production experience provisioning cloudspaces and VMs on commercial IaaS, deploying and securing on-premise LLMs on dedicated GPU infrastructure, and building end-to-end n8n workflows with prompt-injection hardening. Cybersecurity background covers full-scope penetration testing, ELK-based threat monitoring, and vulnerability assessment. Comfortable moving between secure architecture, automation delivery and the operational context a solution has to fit.

EXPERIENCE

Cor4 Digital

Cybersecurity & Digital Solutions Specialist

Bolivia

July 2026 – Present

- Delivered a production computer-vision safety system on 8 plant cameras (26 Python modules, an 11-table SQLite store, 3 n8n workflows), covering frame capture through RF-DETR detection, ByteTrack tracking, zone rules and automated Telegram/PDF reporting.
- Cut false positives 98% (64 to 1 over 70 frames) and raised true detections 7% (771 to 828) by benchmarking four model sizes, fixing inference resolution and switching the DVR off its substream, with no new hardware.
- Designed for zero internet egress and no facial recognition, deriving person IDs from spatiotemporal continuity instead of biometrics, then reverse-engineered a DVR's proprietary DVRIP/Sofia protocol to unblock a client whose unit exposed no RTSP endpoint.
- Turned the single-site build into a repeatable product: one-step install via network auto-discovery and offline installers validated across 7 camera source types, and raised alert delivery to 100% under concurrent violations by re-keying deduplication to per-person identity.
- Built the front end and owner dashboard for Cor4 Digital's second product: an AI agent that books restaurant tables over WhatsApp and Telegram, in React 19, TypeScript and Tailwind CSS v4, with n8n-backed auth and Google Sheets as the data layer.
- Gave the AI agent a live floor to check instead of a static calendar: staff mark tables occupied, create/edit/cancel bookings and free tables from a month calendar and day view, with a 7-second undo on destructive actions.
- Shipped it bilingual (English/Spanish) with light and dark themes, auditing every color pairing with a canvas-based contrast checker.
- Built Cor4 Digital's bilingual company website in React 19, TypeScript and Vite: app catalogue, consulting, team and contact pages, light and dark themes, and security built in: hash-based Content Security Policy, HSTS and hardened headers, consent-gated storage and a rate-limited n8n contact form.
- Designed and built a 17-page Spanish/English website for Yorservi S.R.L., an oilfield-services client, with GSAP ScrollTrigger and Lenis scroll choreography, prerendered to static HTML with no server-side form, so the site collects no personal data.

whitesky.cloud

AI Automation and Cloud Operations Intern

Belgium

February 2026 – May 2026

- Cut an estimated 40% of manual L1 support workload by building a production AI ticketing workflow in n8n connecting Zammad, Rocket.Chat, PostgreSQL and Qdrant, using RAG retrieval with Ollama embeddings and recursive character text splitting, on-premise LLM drafting, and confidence-score routing.
- Eliminated manual console work from infrastructure provisioning by writing Python automation against the whitesky.cloud API to create cloudspaces, spin up VMs, add users and manage resources.
- Kept customer ticket data inside the company network by deploying Qwen 3 30B on GPUStack on a dedicated GPU VM air-gapped from the public internet, so all inference runs internally.
- Hardened the ticketing agent against prompt injection by enforcing strict JSON output schemas and prompt-level rules, then verifying with adversarial payloads (jailbreaks, instruction overrides, payloads hidden in ticket bodies and image attachments) plus magic-byte validation on file attachments.
- Built a Python prompt-injection test framework covering tool abuse, reasoning-chain hijack, confidence manipulation and SQL injection, with an input sanitizer module and JSON report output.
- Restricted backend services to VPN-only reachability by configuring an OPNsense first-match LAN ruleset with whitelist-based isolation and WireGuard with per-user /32 tunnel IPs.
- Automated infrastructure health triage with a second n8n workflow polling the Meneja API every 5 hours, running each failed healthcheck through an AI agent against a GitLab knowledge base and posting severity-sorted reports to Rocket.Chat.
- Kept a fleet of Docker containers (n8n, Ollama, Qdrant, PostgreSQL, pgAdmin) healthy on Linux VMs through health checks, log inspection and restart procedures, and documented architecture and troubleshooting playbooks.

Freelance Security Assessments

Belgium

Security Assessor (two-person engagements)

Client details confidential

- Internal network vulnerability assessment for a residential care organisation: asset discovery, authenticated scanning, manual verification and perimeter checks, reported with CVSS/CWE scoring and prioritised remediation.
- Workstation exposure scan and OSINT review for a pharmacy, with plain-language remediation for non-technical staff.

PROJECTS

Full-Scope Penetration Test: NDL Vulnerability Assessment

Academic Project

- Identified 5 Critical, 4 High and 4 Medium vulnerabilities by running a full-scope penetration test across VPN, DMZ and internal lab segments.
- Reached SYSTEM-level access by exploiting XML-RPC deserialization RCE, Elasticsearch MVEL script RCE, Pass-the-Hash, SNMPv1 misconfiguration and RDP credential interception.
- Performed lateral movement and subnet pivoting with Metasploit, Impacket and credential harvesting, and delivered an audit report with CVSS scoring, CWE references, topology maps and a remediation roadmap.

Web Security Monitoring and Honeypot Analysis

Academic Project

- Reduced mean time to detection ~30% by triaging 2,000+ ModSecurity alerts by attack type (SQL injection, XSS, RCE) and tightening WAF rules against the top patterns.
- Captured 500+ brute-force attempts and SQLMap scans by deploying a Cowrie SSH honeypot wired to Elasticsearch and Kibana for live threat dashboards.

Advanced Nmap Scanner (Python CLI Tool)

Personal Project

- Made scan results consumable by downstream tooling by wrapping Nmap in a Python CLI with OS fingerprinting, custom NSE scripts, decoy scanning and normalized JSON/XML/grepable output.

EncryptedChatBackEnd (Python, Flask-SocketIO)

Personal Project

- Supported 100 concurrent users on a real-time encrypted messaging backend using AES-256, async I/O and environment-based secret management.

ProductionPetrolForecast (Python, Flask)

Personal Project

- Turned decline-curve analysis into a self-serve tool by implementing Exponential, Hyperbolic and Harmonic petroleum production forecasting models behind a Flask interface with dataset upload and Excel report generation.

TECHNICAL SKILLS

AI & Computer Vision: RF-DETR object detection, ByteTrack multi-object tracking, OpenCV, PyTorch (CPU inference), zone/geofence logic, model benchmarking and false-positive analysis, on-premise LLM deployment (GPUStack, Ollama, Qwen 3 30B), RAG pipelines, Qdrant vector database, prompt engineering, AI agent security testing, adversarial payload frameworks

Automation & Integration: n8n workflow automation (production flows, templating, webhooks), REST API integration, Telegram Bot API, SQLite (WAL), PostgreSQL, automated PDF reporting, structured/schema-validated LLM output

Frontend & Web: React 19, TypeScript, Vite, Tailwind CSS v4, react-router, GSAP (ScrollTrigger), Lenis smooth scroll, static prerendering, WCAG AA accessibility auditing, i18n (multi-language UI), light/dark theming

Video & Camera Systems: DVRIP/Sofia protocol (port 34567, XM / Night Owl), RTSP (Hikvision, Dahua, Reolink, Axis), ONVIF discovery, multi-channel NVR, MJPEG over HTTP, USB capture, stream/substream configuration

DevOps & Cloud: Docker, Linux (Ubuntu, Kali), VMware, OPNsense, WireGuard VPN, CI/CD, Bash scripting, Infrastructure as Code, IaaS provisioning (whitesky.cloud); AWS familiarity (academic / project level)

Kubernetes: Multi-node cluster setup and operations (Talos Linux, 3-node cluster), kubectl, deployments, services (NodePort, ClusterIP), MetalLB, Kubernetes Dashboard, Metrics Server, Horizontal Pod Autoscaling, resource requests and limits, YAML manifests, failure recovery testing

Security Engineering: Secure SDLC (SSDLC), security-by-design architecture, threat modelling, firewall rule design, network segmentation, VPN administration, Metasploit, Nmap, Burp Suite, OWASP ZAP, Wireshark, Pass-the-Hash, ARP spoofing, RCE exploitation

Monitoring & Detection: Elasticsearch (ELK Stack), Kibana, Filebeat, ModSecurity log analysis, honeypot deployment (Cowrie)

Digital Forensics: Autopsy / The Sleuth Kit, disk and file-system analysis, evidence timeline reconstruction, artifact recovery

Programming: Python, JavaScript, Bash, SQL, Flask, Flask-SocketIO, Java, PHP; C# (.NET) with full-stack experience including frontend development and Supabase PostgreSQL backend integration

AI Tools: Claude (daily use for coding, debugging, problem-solving), GitHub Copilot in VS Code and JetBrains IDEs

EDUCATION

Howest University of Applied Sciences

Brugge, Belgium

Bachelor of Applied Computer Science, Cybersecurity Professional

British School Quito

Quito, Ecuador

High School Diploma

LANGUAGES

English (Proficient) · Spanish (Proficient)