Enrique Cano Carballar

VP OF SECURITY, IT AND COMPLIANCE

EnriqueCano12@gmail.com | 0795 0102 438 | https://www.linkedin.com/in/enrique-cano/ | UK

PROFILE

Hands-on security leader who built Fresha's security function from the first dedicated hire into a 24×7 security operation defending the world's largest beauty and wellness marketplace — 140,000+ businesses under sustained DDoS, credential stuffing, fraud and phishing. Stood up the SOC, the WAF and anti-abuse defences, threat modelling across every engineering team and the vulnerability management programme, then re-platformed security operations for the AI era: the Security Hub and the agentic security assistant my team runs on are code I wrote. Backed by the governance a board expects — ISO 27001 and HIPAA certified, PCI DSS underway, enterprise risk and private-equity diligence. Nearly 30 years in engineering and security, including 13 at General Electric (GE) securing mission-critical software for electricity and telecom utilities.

EXPERIENCE

Fresha

Since June 2021

Global beauty & wellness booking marketplace and payments platform, HQ London. 140,000+ partner businesses across 120+ countries; 35m+ appointments a month, ~$1.4bn monthly marketplace value. Engineering distributed across the UK, Poland and Kosovo.

Vice President of Security, IT and Compliance

Since 2024

Accountable for cyber security across the group — engineering, 24×7 operations, platform and anti-abuse defence — plus privacy, compliance and corporate IT. Own strategy, roadmap, budget, headcount and vendors.

Security Hub. Designed and built the platform the SOC now runs on: a web UI and an MCP server aggregating threat intelligence, operational metrics (security incidents, detections, response times) and operational controls in one place — so analysts and AI tools such as Claude Code operate the SOC through the same controls, permissions and audit trail.

Agentic security assistant (production). A Slack-native LLM agent with a tool and playbook architecture, authorisation layer, guardrails and observability, giving analysts and customer-facing teams governed access to investigation and response actions that previously needed an engineer.

AI-based detection. LLM and vision-model pipelines for phishing-campaign and malicious-content detection, benchmarked across providers and deployed into the live campaign approval path.

Supply chain security and AI governance. GitHub Actions hardening, dependency firewall rollout, and the organisation-wide response and executive briefing after a GitHub-borne worm event. Own the group AI usage policy and AI spend governance across engineering.

Board, investor and customer assurance. Present risk posture, incident performance and roadmap to the board and C-suite. Led the security, privacy and compliance workstream of a major private-equity diligence process, producing the evidence pack and fronting the investor sessions. Own enterprise customer security questionnaires and the cyber insurance programme.

Risk management. Built the enterprise risk framework — register, scoring, quantification, treatment plans and a standing review forum with the executive team — and the third-party risk programme, including vendor tiering, assessment and contractual security requirements across the supplier estate.

Certification and assurance. Led Fresha's first ISO 27001 certification end to end — scope, gap analysis, the full policy set, control implementation, auditor selection, Stage 1 and Stage 2 — then carried it through surveillance audit and recertification. Extended the same machinery to HIPAA, and now leading the PCI DSS programme. Selected and implemented a GRC platform (Sprinto, see https://sprinto.com/customers/fresha/) that automates evidence collection across critical systems such as AWS, GitHub and Datadog, replacing a manual spreadsheet process.

Privacy and regulatory. Ran GDPR operations through rapid international growth: data subject access requests including law-enforcement and overseas regulator requests, ICO submissions and cookie compliance, intra-group data transfer agreements, and a group-wide data retention framework.

Corporate IT as a product. Took ownership of IT in 2025 and rebuilt it around automation: joiner/mover/leaver provisioning, device management, access provisioning and SaaS governance, all driven by the IT Hub, the Security Hub's counterpart, which I built. Hands-on delivered the HRIS (Deel → HiBob) and ATS (Lever → TeamTailor) migrations.

Team and succession. Grew and led a distributed team across security engineering, security operations, GRC and IT. Ran hiring end to end, developed engineers into senior and lead positions, and opened and recruited a Head of Compliance beneath me to carry the function forward.

Head of Security

2022 — 2024

Built the operational security capability — detection, response, anti-abuse and vulnerability management — for a platform under continuous attack.

Stood up the SOC. Cloud SIEM, alerting, runbooks, an on-call and 24×7 cover model, the incident response plan, tabletop exercises and a blameless post-mortem discipline. Recruited and developed the analysts who run it.

SOC Shell. Built the bespoke Python toolkit the SOC ran on — one interface over observability data, WAF and CDN logs, production data and threat intelligence — the forerunner of today's Security Hub.

Platform defence at scale. Designed and deployed the WAF estate as code — AWS WAF and Shield Advanced across every CloudFront distribution, plus automated IP/CIDR blocking driven by traffic analysis and OSINT feeds, rate limiting, a maintenance-page capability for use under attack, and reCAPTCHA and adaptive 2FA across partner and marketplace authentication.

Held the line against sustained abuse. Led response to volumetric DDoS, distributed scraping, credential stuffing, account enumeration, BIN testing, SMS pumping, payout fraud and repeated phishing campaigns impersonating the brand — in a marketplace where attacker economics are favourable and downtime is revenue.

Fraud partnership. Worked with Payments, Data Science and Trust to build partner risk scoring, phishing-campaign detection in the marketing approval path, and account-takeover containment; led the investigations behind material fraud losses and the control changes that followed.

Vulnerability management. Wrote the policy, scoring model and SLAs; automated dependency-alert triage into per-team Jira tickets with reporting by team; ran the external penetration testing programme and the vulnerability disclosure and bug bounty intake.

Engineering hygiene at organisation scale. Drove org-wide runtime upgrades (Elixir, Node.js), rootless containers across the Kubernetes estate, branch protection strategy, secrets detection and rotation, and per-service security tiering — the unglamorous work that removes whole classes of risk.

Principal Security Engineer

2021 — 2022

First dedicated security hire. Everything below started from nothing.

Made security a team sport. Created the "Jedi" security champions network — a champion embedded in every engineering team, a governing council, and a bot that automated training compliance and chased it.

Embedded threat modelling across every engineering team and into the SDLC, from the first session in 2021 through to sign-in flows, marketplace and website-builder features years later.

Established data protection foundations. Built the personal data inventory and classification scheme for GDPR, then designed and implemented the production data obfuscation pipeline — with a CI check that forces a decision on every new field — so non-production environments stopped carrying real customer data.

Cleared the inherited security debt. Worked through the full penetration test backlog and hands-on rebuilt authentication weaknesses — password reset, login attempt handling, abuse protection — in Elixir and Ruby.

EXPERIENCE (CONTINUED)

General Electric

2008 — 2021

Grid Software Solutions — 60+ commercial products sold to electricity, telecom and utility companies, including Energy and Distribution Management Systems classed as mission critical and operated under heavy regulation.

Cyber Security Architect

2018 — 2021

Cyber security authority for hundreds of software engineers across the Grid Software Solutions portfolio — the closest analogue in a large enterprise to the role I have run at Fresha.

Led architecture and hands-on development of the shared security platform underpinning the next generation of products: OAuth2 authentication, role and permission-based authorisation, an API gateway handling routing and session management, and automated certificate management with PKI integration over EST and OCSP. Microservices with RESTful APIs, delivered as containers onto highly available Kubernetes clusters through CI/CD.

Owned the Secure Development Life Cycle: threat modelling before development, security and design reviews throughout, static and dynamic code analysis, third-party component vulnerability analysis, and the security test plan and final report for each release.

Embedded Privacy by Design into the development life cycle for GDPR, and analysed penetration test reports and resulting security defects across the portfolio.

GENERAL ELECTRIC (CONTINUED)

Technical Lead / Senior Staff / Staff Software Engineer — 2012 – 2018

Technical lead and architect for microservices and web applications on Predix, GE's Industrial IoT platform — Node.js and JavaScript services with a Postgres backend on Cloud Foundry, and web apps built as web components, delivered TDD/BDD in a CI/CD environment with the team owning operational support (DevOps).

Volunteered as site security lead for the Cambridge office, covering around 30 Smallworld products: threat models, security defect analysis and external penetration testing.

Earlier: technical leadership and development across Smallworld GIS web and desktop products (Network Viewer, Network Inventory Gateway, Electric Office, GIS Adapter). Recognised with a Gold Award for technical leadership; co-inventor on a filed patent.

EARLIER CAREER

British Telecommunications — Database Administrator. 850GB Smallworld GIS estate, 3,000 registered and 1,000+ concurrent users; performance tuning, disaster recovery and confidence-test procedures. **2004 – 2008**

Centro Rural de Comercio y Actividades — Software Developer. .NET point-of-sale system (C#, SQL Server) for a family-run retail business. **2002 – 2003**

Implemental Systems — Project Manager, then Services Consultant. Network inventory solutions for telecom operators across Spain. **1999 – 2002**

Sainco — Software Developer. Smallworld GIS desktop applications and data modelling. **1997 – 1999**

EXPERTISE

LEADERSHIP

Security strategy and roadmap · Board and investor reporting · Budget and headcount · Hiring and succession · Distributed multi-country teams · Vendor negotiation

GOVERNANCE

ISO 27001 · HIPAA · PCI DSS (in progress) · GDPR and ICO · Enterprise and third-party risk · Policy and audit · GRC automation

SECURITY ENGINEERING

Threat modelling · Secure SDLC · AppSec and OWASP Top 10 · Vulnerability management · Anti-abuse, bot and fraud defence · Incident response · Supply chain security

PLATFORM & AI

AWS (WAF, Shield, CloudFront, Bedrock, IAM) · Kubernetes · Terraform · Datadog Cloud SIEM · Python, JavaScript · LLM agents, MCP, Claude Code · CI/CD

EDUCATION & RECOGNITION

Master's Degree in Software Engineering
University of Seville, Spain · 1991 — 1998

GE RISE Programme — graduate
One of 120 employees selected across Europe for a year-long programme developing candidates for senior positions · 2015

Web App Penetration Testing & Ethical Hacking
SANS Institute · 2017

Patent co-inventor
Filed patent for work on the Smallworld GIS Adapter (see https://patents.justia.com/inventor/enrique-cano-carballar and https://patents.justia.com/patent/20140358492).