# FRANCISCO JOSÉ ALPUENTE SANTOS

Valencia | Phone: +34 673 30 48 08 | Email: franalpu86@hotmail.com
LinkedIn: linkedin.com/in/francisco-jose-alpuente-santos-/
Portfolio: fran-alpuente.vercel.app

Professional transitioning to Cybersecurity (Blue Team), currently preparing for CompTIA Security+ and certified in Fortinet NSE 1, 2, and 3. I combine a solid technical foundation in networking, infrastructure, and defensive analysis with experience in highly demanding industrial environments, ensuring ISO 9001/14001 and Lean Manufacturing standards. I bring strong analytical skills, incident resolution capabilities, and a continuous improvement mindset, aiming to join a defensive cybersecurity team.

## PROFESSIONAL EXPERIENCE 08/2006 - 04/2025 FORMICA S.A PRODUCTION WORKER AND SECTION MANAGER

- Comprehensive management of production lines and operation of industrial machinery, assuming responsibilities for planning and material supervision under quality regulations.
- Performed autonomous quality controls, proactive incident reporting, and daily operational data entry in SAP.

## EDUCATION, CERTIFICATIONS, AND OTHER DETAILS

- **Specialized Bootcamp (In progress):** The Bridge | 550 hours | Scholarship awarded through X Talento Digital (Start: May 2026).
- **Certifications:** Fortinet Network Security Expert (NSE) 1, 2, and 3 | CompTIA Security+ (In preparation).
- **Courses and Specializations:**
  - Fundamentals of Governance, Risk and Compliance (GRC) - Alison (May 2026).
  - Architecture and Identity: CyberArk Privilege Cloud, Privileged Access Management (PAM), and Identity Security.
  - Cloud Deployment: CyberArk PAMonCloud Image Building Process on AWS and Azure.
- **Academic Background:** High School Diploma (IES Sanchis Guarner, 2006).
- **Languages:** Spanish and Valencian (Native) | English (A2).
- **Other Details:** Driving license and own vehicle | Disability certificate: 35%.

## RELEVANT CYBERSECURITY PROJECTS AND PERSONAL LAB

*(Note: Detailed architectures and complete documentation are available on my Portfolio: fran-alpuente.vercel.app)*

**OpenSentry: Open Source SOAR & DevSecOps Architecture (In development)**

- **Stack:** Python, Flask, Wazuh (EDR/SIEM), FortiGate (NGFW), SQLite, YAML, APIs (VirusTotal).
- End-to-end development of an asynchronous SOAR platform to automate the DFIR lifecycle, governed by a dynamic and modular playbook engine in plain text (YAML).
- Implemented *Active Defense* strategies (Honeytokens on Windows Server) with autonomous containment, alert interception and execution of host isolation in Wazuh or perimeter blocking in FortiGate within milliseconds.
- Created an automated Anti-Phishing pipeline via background daemons that monitor IMAP mailboxes, extract IOCs (RegEx), and enrich case intelligence by querying external APIs (OSINT/VirusTotal).

**Security Coach: Enterprise EDR (Browser Extension) & SOC Integration**

- **Stack:** Python (FastAPI), JavaScript (Manifest V3), Windows Server 2022 (AD, GPO, IIS), Wazuh SIEM, SQLite.
- Full-stack development of a corporate EDR sensor in the form of a browser extension, designed to monitor web telemetry and enforce security policies directly on the endpoint.
- Orchestrated a massive unattended deployment in a Windows domain environment using GPO (Active Directory) policies and an internal IIS server to bypass network restrictions.
- Implemented locally-operating DLP (Data Loss Prevention) and anti-fraud engines, blocked bank cards using the Luhn algorithm, prevented Typosquatting (Levenshtein algorithm), and forwarded structured telemetry (JSON) to Wazuh for Threat Hunting.

**Enterprise SOC & Threat Hunting Lab (Hybrid Infrastructure & Zero Trust)**

- **Stack:** VMware, FortiGate, Windows Server 2022 (AD DS), Wazuh XDR, LAPS, AppLocker.
- Designed a micro-segmented network architecture using FortiGate NGFW, logically isolating the corporate network from the SOC management network to ensure forensic traceability.
- Deployed a hybrid identity environment with *Zero Trust* policies, implementing Microsoft LAPS for credential rotation and kernel-level AppLocker to prevent the execution of unsigned binaries.
- Detection engineering based on the MITRE ATT&CK framework: created custom decoders and XML rules in Wazuh to correlate network events, simulating and detecting real-world adversary tactics (SMB brute force, Pass-the-Hash).