

# Alonso Veliz Garcia

Computer Science & BBA Graduate — Cybersecurity & Network Analyst

📍 Valencia, Spain   ✉ [avelgar@outlook.com](mailto:avelgar@outlook.com)   ☎ +34 640 26 89 72   [in](#) Alonso Veliz Garcia   [🔗](#) [alonsoveliz1](#) [🔗](#)

## About Me

---

Recent **Computer Science & Business Administration** graduate with hands-on experience in threat detection and network security. Developed an **IDS achieving 98% accuracy** in malicious traffic detection using **Machine Learning** (Bachelor's Thesis - Honors). Strong foundation in **TCP/IP**, packet analysis, and security monitoring. Proficient in **Python** and **Rust** for security tooling. My business background complements my technical skills with structured problem-solving and clear documentation. Eager to contribute to a SOC or security team in a collaborative, learning-focused environment.

## Technical Skills

---

**Security & Monitoring:** IDS/IPS, Network Traffic Analysis, Log Analysis, Wireshark, TCP/IP, SIEM fundamentals.

**Programming:** Python (scripting, automation), Rust, Bash, SQL.

**ML for Security:** Scikit-learn, Pandas, ONNX Runtime, Anomaly Detection, Threat Classification.

**Systems & Tools:** Linux (CLI, administration), Docker, Git, Windows.

## Education

---

**Double Degree in Computer Science and Business Administration**

*Sept 2019 – Dec 2025*

*Universitat Politècnica de València (UPV)*

- **Bachelor's Thesis:** Layton - Network Intrusion Detection System – **Honors (10/10)**.
- **Relevant Coursework:** Computer Networks, Operating Systems, Distributed Systems.

## Projects

---

**Layton – Network Intrusion Detection System (IDS)**

[github/Layton](#) [🔗](#)

- Built real-time threat detection system achieving **98% accuracy** in identifying malicious TCP flows.
- Integrated ML models via **ONNX Runtime** for async inference and threat classification.
- Implemented log analysis and alerting dashboard for real-time security monitoring.
- **Stack:** Rust, Tauri, ONNX Runtime, Wireshark, Docker, React, TypeScript.

**ML Pipeline for Cyberattack Detection**

[Layton-models](#) [🔗](#)

- Developed classification models (Random Forest, XGBoost) for network anomaly detection.
- Optimized for **high recall** to minimize false negatives – critical for security operations.
- Processed CICIDS network dataset: feature engineering, cleaning, and analysis.
- **Stack:** Python, Scikit-learn, XGBoost, Pandas, Optuna.

## Languages

---

**English:** B2/C1 (Cambridge FCE – Grade A)   **Spanish:** Native   **Catalan:** Native   **French:** A2