europass

# Pablo Gutierrez Bueno

**Date of birth:** 29/12/2001 | **Nationality:** Spanish | **Phone number:** (+34) 695506828 (Mobile) |

**Email address:** pabloinfosec@gmail.com | **Website:** https://www.pabloinfosec.com/ | **LinkedIn:**

https://www.linkedin.com/in/pablo-gutiérrez-bueno-852272144/ |

**Address:** Barcelona, Spain (Home)

## ABOUT ME

I am a cybersecurity professional with an engineering background, driven by a strong interest in understanding how complex systems fail and how they can be secured against real-world threats. My motivation to work in cybersecurity comes from a genuine curiosity about technology, infrastructure and human behaviour, and from a constant need to analyse, document and improve the systems I work with.
Throughout my academic and professional journey, I have naturally gravitated towards hands-on technical work, combining security engineering, automation and offensive security practice. I enjoy environments where careful analysis, attention to detail and structured methodologies are valued, and where security decisions must be both technically sound and operationally realistic.
I am particularly interested in offensive security and Red Team activities, as they bring together deep technical knowledge, strategic thinking and creativity. At the same time, my engineering mindset leads me to design tools, automations and workflows that improve efficiency, reliability and security over time.
Comfortable working in multidisciplinary and international environments, I value clear communication, documentation and collaboration, and I am motivated by contributing to organisations where security plays a critical role in protecting data, services and people.
I want to compromise your systems before others do.

## WORK EXPERIENCE

**CYBERSECURITY ANALYST – INDRA** – 10/2025 – Current – BARCELONA, SPAIN

Full-time job (40 hours per week)
Key Responsabilities:

- Managing user lifecycle and access control (account provisioning, deprovisioning and permissions governance) across critical systems.
- Developing Python/SQL automations using the Databricks SCIM API for programmatic role and group assignments.
- Automating access documentation into Confluence and designing a Neo4j + PyVis graph model to visualize and analyze permission relationships.
- Ensuring compliance with ENS, ISO 27001 and GDPR through stakeholder reviews and least-privilege validation.
- Daily use of Azure IAM, participation in AWS onboarding, and creation of internal scripts in Python, PowerShell and Bash to streamline security operations.

**QUALITY ASSURANCE COORDINATOR – BERTRANDT S.A.** – 01/2025 – 10/2025 – CASTELLVI DE ROSANES, SPAIN

Leading the QA team in mobile and architecture car validation for SEAT & CUPRA applications, while balancing technical and managerial responsibilities.

- Coordinating daily activities and distributing tasks among team members.
- Acting as a point of contact for client communication and feedback loops.
- Delivering weekly and monthly project tracking reports and presentations.
- Continued executing technical validations alongside organizational duties.

**QUALITY ASSURANCE ENGINEER – BERTRANDT S.A.** – 08/2023 – 12/2024 – CASTELLVI DE ROSANES, SPAIN

Full-time job (40 hours per week)
Key Responsabilities:

- Performed comprehensive validation and testing for automotive applications and vehicle architecture for SEAT & CUPRA brands.
- Mobile app validator for SEAT & CUPRA brands

- Vehicle architecture validator for SEAT & CUPRA
- Creation of Test Plans and Test Cases
- Log reading for applications, back-end, and vehicles
- Use of tools such as Wireshark, dataloggers, Datadog, Kibana, Figma, Zeplin, and Jira, among others
- Automation of mobile applications with XCode, Python, Appium and Selenium

## EDUCATION AND TRAINING

10/2024 – 10/2025

### SPECIALIST IN ARTIFICIAL INTELLIGENCE - RACKS ACADEMY IUNIT - Centro Universitario

Specialisation in integrate AI to Cybersecurity and Automate processes:
- Development of LLMs to analyse responses from cybersecurity tools to ensure a short path to finding vulnerabilities
- Machine Learning, Deep Learning and LLM-based systems applied to automation and data analysis.
- Development of AI-driven SaaS tools and workflow optimization solutions.
- Integration of AI models to support intelligent decision-making across different industries.

**Thesis**: Design and Implementation of an AI-Based Automated System for Job Offer Management and Prioritization

Designed and implemented an AI-powered workflow that ingests job offer emails, extracts structured data with LLMs, scores relevance against my profile and centralises all opportunities in a single tracking system.

**Level in EQF** EQF level 7 |

**Thesis** Design and Implementation of an AI-Based Automated System for Job Offer Management and Prioritization

03/2024 – 04/2025

### MASTER'S IN CYBERSECURITY - DELOITTE IMF Smart Education

Specialisation in Ethical Hacking:
- Ethical hacking, technical security audits and malware analysis.
- Digital forensics and security incident management.
- Secure development practices and penetration testing of systems and networks.
- SIEM monitoring, event correlation and attack mitigation.
- Security frameworks: ENS, ISO 27001, GDPR.

**Thesis**: Building and Breaking an Active Directory Environment

Designed and deployed a full Active Directory environment to practice real-world attack chains, including enumeration, credential extraction, lateral movement and privilege escalation to Domain Admin. Fully documented the architecture, attack paths and defensive mitigations.

**Address** Building and Breaking an Active Directory Environment | **Level in EQF** EQF level 7

09/2019 – 02/2024 Cerdanyola del Vallès , Spain

### BACHELOR'S DEGREE IN ELECTRONIC TELECOMMUNICATIONS ENGINEERING Universitat Autónoma de Barcelona

Specialisation in Electronics:
- Electronics, telecommunications, networking and digital systems.
- Design, implementation and validation of technical engineering projects.
- Technical analysis, measurement, calculation and report writing.
- Problem-solving, applied programming and multidisciplinary teamwork.

**Thesis:** Neuronal Network for Random Number Generation

Designed and trained a neural network using analog transistor-based signal inputs to generate high-entropy random numbers without traditional seeding mechanisms. Explored signal processing, noise modelling and neural behavior for cryptographic-grade randomness.

**Level in EQF** EQF level 6 | **Thesis** Neuronal Network for Random Number Generation

## LANGUAGE SKILLS

Mother tongue(s): **SPANISH** | **CATALAN**

Other language(s):

| | UNDERSTANDING | | SPEAKING | | WRITING |
|---|---|---|---|---|---|
| | Listening | Reading | Spoken production | Spoken interaction | |
| **ENGLISH** | B2 | B2 | B2 | B2 | B2 |

*Levels: A1 and A2: Basic user; B1 and B2: Independent user; C1 and C2: Proficient user*

## PROJECTS

06/2025 – CURRENT

### HTB Writeups Portfolio

Hands-on practice across Windows, Linux, AD, privilege escalation, web exploitation and network attacks using realworld Hack The Box machines. Focused on developing offensive techniques aligned with OSCP-level methodology.

10/2025 – 11/2025

### Databricks IAM Automation System

Developed a Python and SQL automation framework using the Databricks SCIM API to manage user provisioning, role assignments and access governance. Built a Neo4j + PyVis graph model to visualize permissions and detect excessive privilege relationships.

### Security Automation Toolkit

Created internal scripts to automate security operations tasks such as permission audits, documentation updates, user lifecycle workflows and compliance checks across Azure and Databricks environments.

## ACTIVE TRAINING & PROFESSIONAL DEVELOPMENT

04/2025 – CURRENT

### Offensive Security Training Path

My current professional objective is to obtain the Offensive Security Certified Professional (OSCP) certification within the next year, as a natural progression towards advanced offensive security and Red Team roles.
As part of this journey, I am actively preparing for and planning to sit the CJCA (Certified Junior Cybersecurity Analyst) and CPTS (Certified Penetration Testing Specialist) certifications from Hack The Box. These intermediate certifications are intentionally chosen to continuously assess and validate my practical skill level during the OSCP preparation process.
Given my ongoing hands-on practice solving real-world Hack The Box CTFs, I consider HTB's training paths and certifications the most accurate and relevant benchmarks to objectively measure my offensive security capabilities before attempting OSCP.
This approach allows me to maintain a structured, skills-driven progression focused on real exploitation techniques, Active Directory attacks, privilege escalation and operational security.

## SKILLS

### Offensive Security

Hands-on experience in offensive security through continuous resolution of real-world Hack The Box CTFs, working primarily from Kali Linux. Proficient with core offensive tooling such as Nmap, Metasploit, Burp Suite, John the Ripper, Nessus, Maltego, and extensive use of Impacket-based tools (smbclient, smbmap, CrackMapExec, WinRM).
Strong focus on Active Directory attacks, including user enumeration, NTLM hash extraction, and advanced techniques such as Silver Ticket and Golden Ticket attacks. Solid understanding of lateral movement and privilege escalation, supported by tools like BloodHound, Neo4j, LinPEAS, and manual analysis.
Web security experience includes directory traversal, RCE, SQL injection, XSS, LFI, SSTI and buffer overflow fundamentals, using tools such as OWASP ZAP, Nikto, WPScan, Gobuster and SQLMap. Currently operating at an intermediate level, prioritizing deep analysis and methodology over speed, with the ability to solve machines without external writeups.

### Security Engineering, IAM & Data Governance

Security engineer role focused on Identity and Access Management (IAM) and data governance within a large-scale government enterprise data platform. Responsible for user lifecycle management, permissions governance and access control across Databricks, ensuring compliance with ENS and GDPR.

Daily work includes securing secrets, tokens and credentials across Azure, Databricks, AWS and data visualization platforms such as Power BI, following least-privilege and segregation-of-duties principles.
Designed and implemented advanced security automations, including:

- A Neo4j-based access graph built in Python using PyVis, querying the Databricks SCIM API every 30 minutes to visualize relationships between users, groups, service principals and data assets, enabling permission path analysis and access impact validation.
- Automated environment provisioning using structured Python-based permission and group templates, reducing a full day of manual IAM configuration to minutes through repeatable, auditable deployments.

## Cloud Platforms & Infrastructure

Administrator-level experience in Microsoft Azure, managing users, identities, machines and access controls to prevent unauthorized data exposure.
Early-stage involvement in AWS environment deployments, contributing to the initial setup and security configuration.
Experience deploying and maintaining personal and professional projects on Railway and Vercel, with solid understanding of API integrations, credential management, web security fundamentals and data storage architectures.

## Programming & Security Automation

Daily use of Python, Bash, PowerShell and SQL for security operations, automation and data access management.
Development of custom tooling and scripts for IAM enforcement, permissions auditing, deployment automation and security workflows. Additional projects and tooling are publicly documented in GitHub and the personal portfolio.

## AI, Data & Advanced Engineering

Practical use of LLMs (ChatGPT, Claude, Gemini) and local models via Ollama, combined with a strong academic foundation in neural networks and signal-based entropy generation.
Applied AI to cybersecurity workflows, including:

- Automated generation of technical writeups using n8n pipelines, transforming structured notes into high-quality reports with manual review and refinement.
- Experimental local models that analyze command output (e.g., Nmap scans) to suggest attack paths, highlight interesting services and recall previously observed vulnerabilities.
- AI is used as an augmentation tool, not a replacement, with a medium but focused weight in the overall skill set.

## Methodology & Professional Mindset

Highly structured and analytical working style, with strong emphasis on documentation, evidence collection and clear reporting for both technical and non-technical audiences.
Known for maintaining efficiency under high workloads, prioritizing tasks by impact and deadlines, and working calmly in complex environments.
Hybrid profile combining engineering mindset and Red Team orientation, with a long-term objective to operate in advanced Red Team environments while continuing to design tools and automations that improve efficiency, reliability and security outcomes.