Pablo Gutiérrez 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:** www.linkedin.com/in/pabloinfosec | **Address:** Barcelona, Spain (Home)

ABOUT ME

As a curious, proactive and highly adaptable cybersecurity professional with an engineering background, I have specialised in offensive security and the analysis of how complex systems fail —and how they can be secured against real-world attack conditions. My motivation for working in cybersecurity is driven by a strong technical curiosity about technology, infrastructure, and human behaviour, combined with a disciplined and methodical approach to security assessment.

My academic and professional experience has been firmly hands-on, with a focus on penetration testing activities, security engineering, and the development of tools and automations that enhance the effectiveness and reliability of security operations. Comfortable working in multidisciplinary and international settings, I place high importance on clear communication, thorough documentation, and close collaboration with stakeholders. I am especially motivated by Red Team activities, where deep technical expertise, strategic thinking, and creativity converge as part of everyday work.

I am eager to further strengthen my expertise and actively contribute to the vibrant, dynamic and multicultural environment I have always aspired to be a part of, helping organisations to identify, understand, and address their most critical risks before they can be exploited by real adversaries.

WORK EXPERIENCE

CYBERSECURITY ANALYST – INDRA | MINSAIT CYBER – 10/2025 – Current – BARCELONA, SPAIN

Website: https://www.indragroup.com/es

Full-time job (40 hours per week). Remote from Luxembourg
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. – 12/2024 – 10/2025 – MARTORELL, BARCELONA, SPAIN

Website: https://www.bertrandt.com/en/

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

- 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 – MARTORELL, BARCELONA, SPAIN

Website: https://www.bertrandt.com/en/

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 – 12/2025

MASTER'S 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.

Website https://www.racks.academy/ | **Level in EQF** EQF level 7

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.

Website https://www.imf-formacion.com/ | **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.

Website https://www.uab.cat/web/universitat-autonoma-de-barcelona-1345467950436.html | **Level in EQF** EQF level 6

LANGUAGE SKILLS

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

Other language(s): **ENGLISH | B2 UPPER INTERMEDIATE (CEFR)**

PROJECTS

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.

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.

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.

ACTIVE TRAINING AND 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 path, I am preparing for the CJCA and CPTS certifications from Hack The Box, selected as intermediate milestones to assess and validate my practical skill level through continuous hands-on CTF practice. This structured approach focuses on real exploitation techniques, Active Directory attacks, privilege escalation and operational security.

SKILLS

Offensive Security

Hands-on offensive security practice through Hack The Box CTFs, following an OSCP-oriented methodology. Experience with Kali Linux and core tooling (Nmap, Metasploit, Burp Suite, Impacket, BloodHound, LinPEAS). Strong focus on Active Directory attacks, lateral movement, privilege escalation and common web exploitation techniques (SQLi, XSS, LFI, RCE).

Security Engineering, IAM & Data Governance

Security engineering focused on Identity and Access Management (IAM), permissions governance and data access control within a large-scale government data platform. Experience with Databricks security, SCIM-based automation, and compliance with ENS and GDPR. Design and implementation of IAM automation and access-relationship modelling.

Cloud Platforms & Infrastructure

Administrator-level experience in Microsoft Azure (IAM, access control, identity management). Initial experience with AWS deployments. Deployment and maintenance of projects on Railway and Vercel, with solid understanding of API integrations and credential security.

Programming & Security Automation

Daily use of Python, Bash, PowerShell and SQL for security operations, automation, access management and custom tooling.

AI, Data & Advanced Engineering

Applied use of LLMs and automation pipelines to support cybersecurity workflows, documentation and analysis. Academic background in neural networks and applied AI.

Methodology & Professional Mindset

Structured, analytical and documentation-driven approach. Red Team profile with strong focus on methodology, realism and continuous improvement.