Javier González Casares

Cyber Threat Intelligence & Malware Analyst • Penetration Tester • OSCP Candidate

Córdoba, Spain | +34 652 601 501 | javiergc100@protonmail.com

javiergc.es | github.com/i12gocaj | linkedin.com/in/javier-gonzalez-casares

PROFESSIONAL SUMMARY

Computer Engineer with an **MSc in Offensive Security**, focused on **cyber threat intelligence**, **threat hunting**, **malware analysis**, **DFIR** and **offensive security**. **OSCP candidate**. Internships at **AllPentesting** (DFIR & CTI), **Indra Group** (OT Security) and **Navantia** (defence). Active collaborator with the **Spanish National Police** on cybercrime investigations. Member of the **Caliphal Hounds** CTF team, **ranked #2 in Spain (2024)** on CTFTime, **Talent4Cyber 2025 semifinalist** and **$1,000 Meta Bug Bounty** researcher. Recognized by **NASA's Vulnerability Disclosure Program (2026)** for responsibly reporting a security vulnerability.

CERTIFICATIONS

Offensive Security Certified Professional (OSCP), Offensive Security — *In progress*

EDUCATION

MSc in Offensive Security — **Oct 2025 | Oct 2026**
Campus Internacional de Ciberseguridad — *Spain (online)*
MSc thesis: *AllOsint*, local OSINT investigation platform from an email address or phone number.

VIII Expert Diploma: Reverse Engineering & Malware Intelligence — **Sep 2026 | Dec 2026**
University of Málaga (NICS Lab / Google-VirusTotal) — *Málaga, Spain*

BSc in Computer Engineering, Specialisation in Computing — **Sep 2021 | Sep 2025**
Escuela Politécnica Superior de Córdoba, Universidad de Córdoba — *Córdoba, Spain*
BSc thesis: directional prediction of financial assets with ML, DL and news sentiment (GDELT), **graded 10/10**. **[GitHub]**

Erasmus Exchange, Computer Engineering — **Sep 2024 | Jun 2025**
Gheorghe Asachi Technical University of Iasi — *Iasi, Romania*

PROFESSIONAL EXPERIENCE

Digital Forensics Analyst & Cyber Threat Intelligence Intern — **Jan 2026 | May 2026**
AllPentesting — *Córdoba, Spain*

- Supported cybercrime investigations for law enforcement, private investigators and research teams with OSINT, intelligence analysis and tracing of fraudulent infrastructure (domains, IPs, exposed services, phishing kits) across surface, deep and dark web.
- Performed forensic acquisition, cloning, data recovery and technical reporting on mobile devices, computers, USB drives and memory cards (FTK Imager, Autopsy, NirSoft, Proxmark3).
- Analysed Android APKs and malware samples for IoCs, fraud patterns and attacker TTPs; reviewed VPN, RDP, NAS, Microsoft 365 and OneDrive logs during incident investigations.
- Built n8n automations and internal tooling for evidence collection, security audits, threat simulation and phishing campaign analysis. Trained users on and deployed ATAK-CIV / TAK Server with plugins for tactical coordination.

OT Security Engineer Intern — **Nov 2025 | Dec 2025**
Deuser (Indra Group) — *Córdoba, Spain*

- Designed OT industrial network diagrams: device mapping, segmentation and trust zones.
- Deployed and configured Microsoft Hyper-V virtual machines for internal labs and test scenarios.
- Completed firewall configuration training and hands-on lab work with Siemens PLCs.

Cybersecurity Engineer Intern, COEX Naval Systems — **Jun 2025 | Sep 2025**
Navantia, S.A., S.M.E. (Defence Sector) — *San Fernando, Spain*

- Designed and deployed the centre's monitoring and defence stack (SIEM, IDS, router/firewall).
- Built a network testing laboratory for the passive combat systems of naval vessels.
- Delivered cybersecurity training sessions to colleagues across the department.
- Automated repetitive operational processes to improve efficiency and traceability.

Cybercrime Investigations Collaborator — **Jun 2025 | Present**
Spanish National Police (Policía Nacional) — *Remote, Spain*

- Provide OSINT and technical analysis for active investigations into web-based scams and online fraud targeting Spanish citizens, tracing domains, IPs, phishing infrastructure and blockchain transactions.

- Document findings in case-ready evidence packages, applying chain-of-custody and operational discretion.

VULNERABILITY RESEARCH & RECOGNITIONS

- **NASA Vulnerability Disclosure Program (VDP) Recognition** (Jun 2026): Letter of Recognition from NASA's Office of the Chief Information Officer (SAISO) for responsibly reporting a vulnerability in NASA systems.
- **$1,000 Meta Bug Bounty, Instagram Notes Audio Leakage** (May 2025): privacy bypass exposing the original audio of Instagram Notes videos through direct URL extraction. Validated and patched by Meta. **[GitHub]**
- **Instagram Password Change Bypass** (Meta Bug Bounty, Apr 2025): account-takeover flaw allowing a password change without the current password in an active session. Reported to Meta and fixed. **[GitHub]**
- **Club Gym Sierra Client-Side Time Manipulation** (2025): logic flaw allowing early class booking by changing the device clock. Responsibly disclosed; the vendor moved validation server-side and patched it in v4.4.19. **[GitHub]**

AWARDS & COMPETITIONS

- **Caliphal Hounds CTF Team (2024)**: team **ranked #2 in Spain** on CTFTime.
- **Talent4Cyber 2025 Semifinalist, 8th nationally** (MCCE & INCIBE, Dec 2025): 100+ teams, representing the University of Córdoba.
- **1st Prize**, Hackademics Forum III CTF (Apr 2025), sponsored by Hack The Box.
- **Week 4 Winner**, "El Bug de la Semana" (INCIBE & IMMUNE, Dec 2025).
- **Best Device Award**, 4th Biotechnological Hackathon (IMIBIC & EPSC, Apr 2026): real-time surgical material counting prototype.

FEATURED PROJECTS

- **SecEmail** (open source, 2026): SPF/DKIM/DMARC/ARC auditor and authorised SMTP/phishing simulator for Red Team engagements. Cryptographic DKIM verification, IDN homograph detection, MTA-STS, TLS-RPT, DANE and BIMI checks and campaign dashboard. **[GitHub]**
- **AllOsint** (MSc thesis, 2026): local OSINT investigation app from an email or phone number: 54 email checkers, WhatsApp, Telegram and Signal signals, breach correlation, GHunt, WhatsMyName and PDF reporting. **[GitHub]**
- **Atlas** (Atmira × OpenAI × Big Data Hackathon, 2026): local-first, read-only auditor of AI copilot usage: policy-as-code compliance, secret and PII detection (regex, entropy, detect-secrets), FinOps cost anomalies and offline dashboard. **[GitHub]**

TECHNICAL SKILLS

Threat Intelligence & OSINT: MITRE ATT&CK, threat hunting, threat actor profiling, IoC analysis, phishing and fraud infrastructure tracing (domains, IPs, exposed services), surface/deep/dark web and blockchain investigation, Maltego, Shodan.
Malware Analysis & Reverse Engineering: static, dynamic and code analysis of APTs, ransomware, infostealers and RATs; anti-VM, anti-disassembly, anti-decompilation, anti-debugging and obfuscation techniques; sandboxing (CAPEv2, Cuckoo); memory analysis (VMMap, Volatility 2 and 3); network traffic analysis (Wireshark); IDA Pro, Ghidra, Process Monitor, Process Explorer, PEstudio, Detect It Easy, YARA, VirusTotal.
Digital Forensics & DFIR: acquisition, cloning and data recovery from computers, mobile devices and storage media; Android APK analysis; log analysis (VPN, RDP, NAS, Microsoft 365, OneDrive); FTK Imager, Autopsy, NirSoft, Proxmark3; chain of custody.
Offensive Security: Nmap, Burp Suite, ffuf, Gobuster, Metasploit, Nessus, NetExec, Impacket, BloodHound, Mimikatz, Responder, Evil-WinRM, Hashcat, John the Ripper, LinPEAS/WinPEAS, Chisel, Ligolo-ng; Linux and Windows privilege escalation, Active Directory attacks (Kerberoasting, AS-REP roasting, pass-the-hash), pivoting, OWASP Top 10.
OT/ICS & Infrastructure: industrial network design, Siemens PLCs, firewalls, Hyper-V.
Automation & Tooling: n8n, Python scripting for analysis and evidence generation, ATAK-CIV / TAK Server.
Programming & Platforms: Python, Bash, C, C++; MySQL, MongoDB, MariaDB; Linux, Windows Server.
Languages: Spanish (native), English (B2, upper-intermediate).

EXTRACURRICULAR ACTIVITIES

- **Cybersecurity & Free Software Classroom**, EPSC, Universidad de Córdoba (2021-2025): talks, workshops and CTF coaching for peers.
- **Scout Movement**, local youth group (2008-present): **President** (2023-2024), coordinating volunteer teams and community projects.
- **Debate Team**, La Salle Córdoba (2018-2021): two-time inter-school champion and mentor for younger students.