

DIEGO URBANEJA PORTAL

JUNIOR SOC ANALYST / BLUE TEAM • COMPUTER ENGINEER

Burgos, Spain • Open to relocation (Spain/EU) • urbanejaportaldiego@gmail.com
diegourbaneja.dev • [LinkedIn](#) • [GitHub: Urbii22](#) • [TryHackMe: Urbi22](#)

PROFESSIONAL SUMMARY

Computer Engineer seeking a first role as a Tier 1 SOC Analyst. TryHackMe Security Analyst Level 1 (SAL1) certified, top 2% globally on TryHackMe with 220+ labs completed. Hands-on practice in alert triage, suspicious email and network traffic analysis with Splunk, Elastic and Wireshark, and builder of a personal SOC lab with 30 investigation scenarios. Professional experience in Python development. English C1.

CERTIFICATIONS

TryHackMe Security Analyst Level 1 (SAL1)

Sep 2026

Credential ID: [THM-6ab3e910351ee3b99abf475b](#)

HANDS-ON CYBERSECURITY TRAINING

TryHackMe – SOC Level 1 Path

Aug 2026 – Present

- Alert triage in Splunk and Elastic: queries, event correlation and true/false positive assessment.
- Suspicious email analysis: headers, SPF and review of SMTP communications with Wireshark.
- Investigation reports with context, timeline, IOCs, MITRE ATT&CK techniques and conclusion.

TryHackMe – Systems and Offensive Security Labs

Jan 2024 – Present

- 220+ rooms: networking, Linux/Windows, Active Directory, reconnaissance, vulnerabilities and web security.
- Knowledge of attack techniques applied to recognizing suspicious activity during investigations.

SECURITY PROJECTS

SOC-Simulator – SOC Training Lab

TypeScript • Node.js • Elastic/Kibana • Docker • 2026

- Web-based SOC console with 30 triage, investigation and response scenarios over ~2,950 synthetic events from 12 sources (Windows/Sysmon, Linux, DNS, Suricata, firewall, email, cloud), with an alert queue, evidence and explained resolution.
- Reference KQL, SPL and Sigma queries per scenario, automated grading, and reproducibility and IOC tests.
github.com/Urbii22/SOC-Simulator

THM Fieldbook

JavaScript • Python • GitHub Actions • 2026

- Tool to log lab findings with evidence, hypotheses and a prioritized next check; exports sanitized write-ups and playbooks. Tests and CI. github.com/Urbii22/thm-fieldbook

Evidence Atlas – Security Architecture

Next.js • TypeScript • Supabase/PostgreSQL • 2026

- Threat modeling and separation of a private workspace from its public surface through server-side authorization, RLS and sanitized snapshots. Unit and E2E tests in CI.

TECHNICAL SKILLS

Detection & analysis: Splunk and Elastic (lab), SPL/KQL queries, Sigma rules, alert triage, log analysis (Windows, Sysmon), phishing, Wireshark, IOCs, MITRE ATT&CK.

Systems & networking: Linux, Windows, Active Directory; TCP/IP, DNS, HTTP/HTTPS.

Offensive foundations: Nmap, Burp Suite, Metasploit and BloodHound in lab environments; web and API security.

Development: Python, Java, SQL, TypeScript; Git, Docker, GitHub Actions, Streamlit, OpenCV, Pandas.

PROFESSIONAL EXPERIENCE

Associate Technical Staff – University of Burgos

Mar 2025 – Jun 2025

- Developed EcoVid (Dig4Vitis project): a web application to detect and quantify copper deposits on grapevine leaves using hyperspectral imaging.
- Reproducible processing, alignment and visualization pipelines in Python and Streamlit, with OpenCV, NumPy and Docker.
github.com/Urbii22/TFG_Dig4Vitis_V2

EDUCATION

Bachelor's Degree in Computer Engineering – University of Burgos

2021 – 2025

GPA: 7.98/10. Bachelor's thesis: Hyperspectral image analysis for copper detection in vineyards.

LANGUAGES

Spanish: native • English: C1 (advanced)