RUBEN DIAZ FRAGA

Cyber Threat Intelligence Analyst

contact@phi618.cloud | linkedin.com/in/rbd1z | github.com/9intel | Malaga, Spain | Remote · EU

PROFILE

Cyber threat intelligence analyst with 2+ years at Telefonica Tech, one of Europe's largest cybersecurity operations, **promoted twice in under two years**. I turn intelligence requirements into tailored, decision-ready products: I define collection around each stakeholder's **PIRs**, run OSINT and dark-web investigations, and deliver daily, weekly and monthly reporting to technical teams and executives. Hands-on with **Threat Intelligence Platforms** (OpenCTI, Cybersixgill) and **Python automation** for collection and reporting pipelines. Stakeholder-facing by nature, an effective written and verbal communicator, bilingual English/Spanish, and fully remote-native with a growth mindset.

PROFESSIONAL EXPERIENCE

Threat Intelligence Analyst II · Telefonica Tech

Feb 2026 to Present · Digital Risk Protection

- Act as the intelligence point of contact for enterprise organizations: elicit their **intelligence requirements and PIRs**, tune collection to their threat landscape, and advise them on how to act on the intelligence delivered.
- Produce tailored daily, weekly and monthly threat and vulnerability reports, translating raw findings into **impactful, decision-ready intelligence** for both defenders and executive stakeholders.
- Own service operations: onboard new intelligence modules for clients and proactively detect, escalate and close capability gaps in the platform.

Digital Risk Protection & Anti-Fraud Analyst I · Telefonica Tech

Jan 2025 to Jan 2026 · enterprise organizations

- Ran OSINT and dark-web collection across open, deep and dark sources to detect phishing, fraud campaigns, brand abuse and credential/data exposure; authored advisories on ransomware, DDoS and emerging fraud trends.
- Administered **TIP and monitoring platforms** and built custom **Python tooling** to automate collection, keyword alerting and structured reporting, cutting manual effort and speeding delivery to stakeholders.
- Coordinated response with clients and third parties (registrars, ISPs, platforms) to drive domain and social-media takedowns end-to-end.

Threat Intelligence Analyst I · Telefonica Tech

May 2024 to Dec 2024 · Dedicated CTI project, Tier-1 global bank

- Embedded intelligence analyst supporting the bank's **SOC and threat-hunting workflows**: triaged indicators (IPs, hashes, domains, CVEs) and mapped adversary TTPs to **MITRE ATT&CK** to inform hunts and detections.
- Delivered daily threat bulletins and situational-awareness reporting on financial-sector threats directly to the client's security stakeholders.
- Applied Structured Analytic Techniques (SATs) to keep facts and analytical judgement clearly separated across all intelligence products.

SKILLS

CTI Craft: PIRs & intelligence-requirements definition, intelligence lifecycle, threat-hunting use cases, vulnerability reporting, executive & technical intelligence reporting, Structured Analytic Techniques (SATs)

Platforms & Tooling: Threat Intelligence Platforms (OpenCTI, Cybersixgill), TIP administration, SIEM/ticketing workflows, Talkwalker; MITRE ATT&CK, Diamond Model, Cyber Kill Chain

Collection & OSINT: OSINT & SOCMINT, Tor-forum and paste-site collection, source evaluation & grading, dark-web monitoring

Automation & AI: Python (collection, alerting and reporting pipelines), Git, Linux; LLM-assisted analysis, prompt engineering and automation workflows

Advisory: stakeholder-facing communication, onboarding and enablement, written and verbal reporting in English & Spanish, fully remote collaboration

CERTIFICATIONS

CrowdStrike Falcon Intelligence Specialist, CrowdStrike University (2026) · Introduction to SecOps, Palo Alto Networks (2026) · 6 additional cybersecurity certifications (on request)

EDUCATION & LANGUAGES

Cursus, Computer Programming, 42 Malaga (Sep 2023 to Feb 2025) · **Game Development (Programming)**, American University of Malta (Sep 2022 to Jul 2023)

Spanish: native · **English**: full professional proficiency (daily written intelligence production)