



TECHNICAL SKILLS



- **SOC / Blue Team:** SIEM monitoring Microsoft **Sentinel** + Defender XDR/EDR + Cloud, **Wazuh**, Splunk), log analysis, IOC detection, network traffic analysis (Wireshark), APT (rkhunter), Reyes CCN Cert.
- **Digital Forensics:** **Autopsy**, Memory forensics (**Volatility**, LiME), disk imaging & file carving (**Guymager**, dd), timeline building (Plaso).
- **Electronics & IoT:** Circuit design, microcontroller integration (ESP32), low-voltage systems.
- Programming & Systems: **Python**, KQL y PQL queries, Linux, Windows, Vbox, QEMU, YARA sigma rules.
- 4 years studying **Philosophy** (University of Malaga), contributing competences in logic and ethics, precise writing, critical thinking and rigorous analysis applied to Cybersecurity.



RELEVANT EXPERIENCE AND PROJECTS

SOC & Threat Monitoring Project: 2023 – 2025

- Monitored simulated enterprise environments using **Wazuh** and Microsoft Sentinel to detect unauthorized access, phishing attempts, and privilege escalation.
- Conducted log correlation, alert triage, and initial incident response following **NIST and MITRE ATT&CK frameworks**.
- Investigated security alerts using network traffic analysis (**Wireshark**) and identified IOCs for malware and suspicious connections.
- Supported threat containment by performing basic memory and disk forensics (**Volatility**, dd, **Plaso**) for **root cause analysis**.
- Detection (C2) using **beaconing analysis** and suspicious processes (**Cobalt Strike**, Empire, Sliver, Brute Ratel).
- IOC management: IPs, domains, hashes, processes anomalous related to C2 frameworks.
- **Documented incidents** and created structured SOC reports for escalation to Tier 2/3.



Cybersecurity Forensics & Compliance: 2023–2025

- Performed **GDPR/LOPDGDD**-aligned analysis for evidence collection in digital investigations.
- Developed **forensic-ready procedures** to support SOC teams during major incidents.
- **ISO/IEC 27001, 27002, 27035** incident management, 27032, 27701.



Dragos Cornel

SOC Analyst L1, Digital Forensics Analyst, Electronics

+34 643 041 943

[linkedin.com/in/dragos-cia5](https://www.linkedin.com/in/dragos-cia5)

github.com/theforensiqhunter

forensiq.sentinel@outlook.com

PROFESSIONAL PROFILE

SOC Analyst with a multidisciplinary background in Cybersecurity, Digital Forensics (DFIR) and Electronic Systems. Skilled in handling large volumes of security data, correlating logs and events to identify potential threats. Experienced in applying DFIR techniques—such as deep forensic analysis, timeline reconstruction, and memory inspection—to enhance SOC operations, improve incident triage, and uncover hidden compromises.

ACADEMIC BACKGROUND AND CERTIFICATIONS

- Master's Degree in Private Detective, Cyber Investigation and Forensic Analysis – UNIR (2025)
- Computer Forensic Expert Witnesses in Legal Cases – UNIR (2025)
- Higher Degree in Electronic Maintenance – Malaga (2023)
- Cybersecurity Training Programme (Next Generation Europe) Training subsidised by the Recovery, Transformation and Resilience Plan (2023–2025). It included modules on SOC: SIEM, incident management and perimeter defense.

LANGUAGES

- Spanish - Native
- Roumanian - Native
- English - Intermediate/Advanced
- French - Basic

INTERESTS AND PROJECTS

- Studying the possibility of creating a Honeypot with Raspberry Pi and evolving it to ESP32.
- Competitive chess player with strategic skills applicable to cybersecurity analysis.