## HABILIDADES TÉCNICAS

- **SOC / Blue Team**: monitoreo **SIEM** (**Wazuh**, OSSIM AlienVault), análisis de registros, detección de IOC, análisis de tráfico de red (**Wireshark**), investigación de persistencia de malware con herramienta anti rootkit (rkhunter)
- Análisis **forense digital**: análisis forense de memoria RAM (**Volatility**, LiME), imágenes de disco y extracción de memoria (**Guymager**, dd), construcción de líneas de tiempo (**Plaso**), descifrado de hash (John, Hashcat), etc.
- **Electrónica e IoT**: Diseño de circuitos, integración de microcontroladores (**Arduino**, ESP32), sistemas de bajo voltaje.
- Programación y sistemas: **Python, Bash**, Linux, Windows, Docker, (Vbox, QEMU).

## EXPERIENCIA Y PROYECTOS RELEVANTES

### Proyectos de monitoreo de amenazas y SOC – 2023 – presente

- **Monitoreo** de entornos empresariales simulados utilizando **Wazuh y OSSIM AlienVault:** detección accesos no autorizados, intentos de **phishing** y **escalada de privilegios**.
- Correlación de registros, clasificación de alertas y la respuesta inicial a incidentes siguiendo los marcos **NIST y MITRE ATT&CK**.
- Investigación de alertas de seguridad mediante el análisis de tráfico de red (**Wireshark**).
- Contención de amenazas mediante la realización de análisis forenses de memoria y de disco (Volatility, dd, Plaso) para el **análisis** de la **causa raíz**.
- Documentación de incidentes y creación de **informes SOC** estructurados para **escalar al Nivel 2/3**.

### Ciberseguridad forense y normativa – 2023– presente

- Análisis alineados con **GDPR / LOPDGDD** para la recopilación de evidencia en investigaciones digitales.
- Desarrollo procedimientos listos para la ciencia forense para apoyo a los equipos de SOC durante incidentes importantes.

### Proyectos de seguridad de IoT y electrónica - 2022-2024

- Sistemas integrados de monitoreo basados en sensores con **CCTV** y protecciones de bajo voltaje. Diseño de prueba de implementaciones seguras de IoT (**ESP32, Arduino**), incluido el control de acceso, registro remoto, etc.


# Dragos Cornel

**Analista SOC y Analista Forense Digital, Electrónica**

+34 643 041 943
linkedin.com/in/dragos-cia5
github.com/theforensiqhunter
forensiq.sentinel@outlook.com


## PERFIL PROFESIONAL

Analista SOC con formación multidisciplinar en Ciberseguridad: Forense Digital (DFIR) y Sistemas Electrónicos. Experiencia en el manejo de grandes volúmenes de datos de seguridad, correlacionando registros y eventos para identificar amenazas potenciales. Experiencia en la aplicación de técnicas DFIR, como análisis forense profundo, reconstrucción de línea de tiempo e inspección de memoria, para mejorar las operaciones de SOC, mejorar la clasificación de incidentes y descubrir compromisos ocultos.

## FORMACIÓN Y CERTIFICACIONES

- Máster Universitario en Detective Privado, Investigación Cibernética y Análisis Forense – UNIR (2025)
- Curso Avanzado de Peritaje Forense Informático en Causas Judiciales – UNIR (2025)
- Grado Superior en Mantenimiento Electrónico – Málaga (2023)
- Programa de Formación en Ciberseguridad (Next Generation Europe) Formación subvencionada por el Plan de Recuperación, Transformación y Resiliencia (2023-2025). (Módulos SIEM, gestión de incidentes, análisis forense y defensa perimetral, etc.).

## IDIOMAS

- Español - Nativo
- Rumano - Nativo
- Inglés - Intermedio/Avanzado

## INTERESES Y PROYECTOS

- Trabajando en crear una Honeypot con Raspberry Pi y evolucionarlo a ESP32.
- Ajedrecista competitivo con habilidades de pensamiento estratégico aplicables al análisis en ciberseguridad.