ALFONSO ROLDÁN AMADOR

Analista de Ciberseguridad | Red Team & Pentesting

Utrera, Sevilla | megaalfonso84@gmail.com | +34 629 178 163 | alfonsora6.com | linkedin.com/in/alfonsora6

Profesional en transición hacia ciberseguridad, con base sólida en administración de sistemas, redes, virtualización y cloud (Azure). Cursando el Máster en Ciberseguridad e IA en Evolve, con especialización en Red Team y técnicas ofensivas. Autor de IOC Correlator, una plataforma de threat intelligence multi-tenant desplegada en producción. Practicante activo en Hack The Box, en preparación para la certificación eJPTv2. Perfil autodidacta con experiencia práctica en entornos Linux, Docker, Git y automatización de infraestructura.

FORMACIÓN

Máster en Ciberseguridad e IA
Evolve | 2026

Administrador de sistemas informáticos en red (C.F.G.S)
I.E.S. Gonzalo Nazareno, Dos Hermanas (España) | 2023

Técnico en sistemas microinformáticos y redes (C.F.G.M)
I.E.S. Gonzalo Nazareno, Dos Hermanas (España) | 2021

HABILIDADES TÉCNICAS

- Nociones de Pentesting (Active Directory, Impacket, Hashcat)
- Metodología de Auditoría (OWASP, PTES, NIST)
- Reconocimiento y OSINT (Nmap, CVE/NVD)
- Redes y Seguridad (Firewall, VPN, Wireshark, Certificados SSL/TLS)
- Threat Intelligence (VirusTotal, AbuseIPDB, Shodan, AlienVault OTX)
- Scripting aplicado a Seguridad (Bash, Python)
- IA Aplicada a Ciberseguridad (LLMs, detección de anomalías)
- Normativa y Cumplimiento (RGPD, NIS2, ENS)
- Fundamentos SOC / Blue Team (SIEM, EDR, IOC vs. IOA)
- Respuesta ante Incidentes y Forense Básico (contención, hardening)

PROYECTOS DESTACADOS

IOC Correlator | Proyecto personal **2026**

- Plataforma multi-tenant de threat intelligence, desplegada en producción, que correla IOCs (IPs, dominios, URLs, hashes) contra VirusTotal, AbuseIPDB, Shodan y AlienVault OTX.
- Calcula una puntuación de amenaza agregada (0-100) con niveles de severidad LOW/MEDIUM/HIGH/CRITICAL.
- Stack: FastAPI (Python 3.12), React/TypeScript, PostgreSQL, Redis, Celery y Docker Compose; autenticación JWT y cifrado Fernet AES-128 para claves API.
- Despliegue autónomo en VPS Hetzner (Debian): configuración de Nginx, SSL (Let's Encrypt) y Docker.
- Repositorio: github.com/alfonsora6/ioc-correlator

FORMACIÓN PRÁCTICA

- Hack The Box: nivel Apprentice, más de 50 máquinas completadas; preparación activa para la certificación eJPTv2 (eLearnSecurity Junior Penetration Tester).
- Práctica de técnicas de Active Directory: Pass-the-Hash, DCSync, Kerberoasting/AS-REP Roasting y movimiento lateral.
- Estudio de fundamentos Blue Team: arquitectura SIEM (Splunk, Sentinel, Wazuh, QRadar), EDR, IOC vs. IOA y gestión de parches.

EXPERIENCIA PROFESIONAL

IT Support Technician | Keycoes Comunicaciones (Cliente: Caja Rural del Sur)	Mar 2026 - May 2026
Support Technician L2 | Randstad Digital	Jun 2025 - Jul 2025
Implementation and Support Specialist | Guadaltel, S.A	Nov 2023 - Jun 2024
Azure Cloud Administrator | Kyndryl	Mar 2023 - Jun 2023
Técnico Informático | Sithus IT Services, S.L	Mar 2021 - Jun 2021

IDIOMAS

- Español | Nativo
- Inglés | Intermedio