Alberto Hidalgo

SOC Analyst · Blue Team

bitsofalber@gmail.com
github.com/bitsofalber
linkedin.com/in/ahidalgotech
bitsofalber.github.io

PERFIL PROFESIONAL

Estudiante de Administración de Sistemas Informáticos en Red con gran interés en la ciberseguridad defensiva y la monitorización de sistemas. Experiencia práctica en análisis de logs, detección de amenazas con Splunk (SIEM), ingeniería de detección (Sigma, mapeo MITRE ATT&CK) y pruebas de penetración en entornos controlados. Creador de **KrakenSOC-Labs**, una colección de 9 laboratorios Blue Team en Docker.

EXPERIENCIA

Vigilante de Seguridad
Viten Seguridad y Transportes Blindados S.A. · 2018 – 2026

– Aplicación de protocolos de seguridad y gestión de incidentes.
– Vigilancia preventiva y detección de riesgos.
– Toma de decisiones críticas bajo presión.

PROYECTOS DESTACADOS

KrakenSOC-Labs — Laboratorios Blue Team en Docker
9 labs · 30+ técnicas MITRE ATT&CK · reglas Sigma/Suricata

– Forense de red (PCAP) y caza de amenazas con un Splunk real.
– Data-forge determinista, detección y write-ups por lab.

EDUCACIÓN

Administración de Sistemas Informáticos en Red (ASIR)
FP Euroformac · 2025 – Actualidad

CERTIFICACIONES

eJPTv2 — eLearnSecurity Junior Penetration Tester v2 (2025) · verificar
Curso de Splunk
Introducción al Web Hacking
Blue Team Path — TryHackMe

HABILIDADES

Splunk | SPL | SIEM | Sysmon | Sigma | **MITRE ATT&CK** | Wireshark | tcpdump | Threat Hunting | DFIR | Linux | Windows | Redes | Docker | Python | **eJPTv2** | Nmap | Burp Suite | OWASP Top 10

INFO ADICIONAL

– Inglés: nivel intermedio
– Carnet de conducir y vehículo propio
– Disponibilidad para viajar