CARLOS VILLALBA LAGOS

Analista de Ciberseguridad · SOC · DFIR · Respuesta a Incidentes

España · contact@carlosvillalbalagos.com · +34 665 11 14 80
carlosvillalbalagos.com · linkedin.com/in/carlosvillalba-lagos · github.com/BlueShield-Ch4rl13

PERFIL PROFESIONAL

Analista de SOC con experiencia en operación 24x7 para clientes del sector banca y administración pública. Especializado en el triaje, análisis y respuesta a incidentes (malware, phishing, ataques avanzados, DLP) con SIEM (Wazuh, Devo, Sentinel) y Cortex XSOAR/XSIAM, y en la automatización de la respuesta mediante SOAR y APIs. Base sólida en sistemas, redes e identidades. Orientado al Blue Team, con proyectos propios en forense digital (DFIR) e inteligencia de amenazas (CTI) y manejo habitual de MITRE ATT&CK, NIST e ISO 27001. Mi objetivo es evolucionar hacia roles de analista N2/N3 y respuesta a incidentes.

COMPETENCIAS TÉCNICAS

SIEM y detección: Wazuh, Devo, Cortex XSIAM (XDR), Snort, Suricata (IDS/IPS), Sandbox

Respuesta y automatización (SOAR): Cortex XSOAR / Demisto, Airflow, Jupyter, APIs / Swagger, scripting

Red y perímetro: Firewalls (Palo Alto, Juniper), WAF (Imperva, Radware, Cloudflare), Proxy, RADIUS, Infoblox

Datos e identidades: DLP, CyberArk, Vault, Active Directory / Entra ID, Intune

Cloud, correo y aplicaciones: Proofpoint PRO y TAP, Netskope, Symantec, Netcraft, Microsoft Azure

Ticketing: The Hive, ServiceNow, BMC Remedy, Request Tracker (RT), Maximo

Marcos y normativa: MITRE ATT&CK, NIST, ISO/IEC 27001, ISO 14001, DORA, RGPD, Zero Trust (ZTA)

EXPERIENCIA PROFESIONAL

Analista de SOC L1 (24x7) — Experis — cliente: CaixaBank *09/2025 – 09/2026*

- Triaje, análisis y respuesta a alertas e incidentes de seguridad bajo SLAs (malware, phishing, ataques avanzados y DLP).
- Gestión de consultas y análisis de eventos en SIEM, con monitorización en tiempo real de la seguridad de la red.
- Gestión de automatizaciones de casos en Cortex XSOAR (XDR) y desarrollo de scripts con APIs externas (Jupyter, Swagger).
- Análisis e investigación de IoC con plataformas de Palo Alto; gestión de reglas y monitorización de correo con Proofpoint PRO y TAP.
- Elaboración de informes técnicos y revisión de procedimientos operativos.

Técnico de Sistemas (24x7) — Seidor — cliente: Generalitat de Catalunya *04/2024 – 09/2025*

- Gestión y administración de incidencias (ITSM - Remedy), escalado de incidentes críticos y soporte remoto cumpliendo SLAs.

Técnico de Sistemas — Irium — Dept. Educación (Generalitat) *11/2023 – 02/2024*

- Gestión de incidencias (Remedy), supervisión de despliegues en Microsoft Azure y gestión de usuarios en Intune (desbloqueos y escalados).

Soporte Técnico N1 — Lluch Essence S.L.U. *07/2023 – 10/2023*

- Helpdesk a usuarios finales, administración de Active Directory en Azure, gestión de dispositivos vía Intune, inventario y documentación.

PROYECTOS Y HOMELAB

- **News CTI** — Pipeline en Python con GitHub Actions que recolecta y enriquece IoCs y vulnerabilidades (ThreatFox, URLhaus, OTX, CISA KEV) con scoring de gravedad, reputación y GeoIP; +48.000 IoCs procesados.
  Panel: cti.carlosvillalbalagos.com · github.com/BlueShield-Ch4rl13/ScriptNewsCTI
- **FtriageDFIR** — Herramienta de triage forense multiplataforma (Windows, Linux, macOS) que recolecta artefactos preservando la cadena de custodia (MD5 y SHA-256), los mapea a MITRE ATT&CK y genera informe en HTML y JSON.
  Panel: dfir.carlosvillalbalagos.com · github.com/BlueShield-Ch4rl13/FtriageDFIR
- **Malpipe** — Pipeline automatizado de análisis de malware (estático y dinámico en sandbox con CAPEv2 y YARA) que genera veredicto, IOCs y técnicas ATT&CK; los indicadores realimentan News CTI.
  github.com/BlueShield-Ch4rl13/Malpipe
- **Infra-SocAnalyst** — SOC open source en entorno virtualizado: detección en tres capas (Wazuh, ELK, Sysmon, Suricata) y respuesta automatizada (Shuffle, TheHive, MISP) sobre vectores de ataque reales.
  github.com/BlueShield-Ch4rl13/Infra-SocAnalyst
- **Detection-lab** — Lab de detection engineering y purple team: reglas Sigma como código, emulación de adversario con Atomic Red Team y medición de cobertura sobre MITRE ATT&CK.
  github.com/BlueShield-Ch4rl13/Detection-lab

FORMACIÓN ACADÉMICA

- **Curso Peritaje Informática Forense** — UNIR (2026 – 2027)
- **Máster FP en Ciberseguridad en Entornos de las TI** — Stucom (2025 – 2026)
- **Técnico Superior en Administración de Sistemas Informáticos en Red (ASIR)**, perfil ciberseguridad — IFP Innovación en FP (2021 – 2023)
- **Técnico en Sistemas Microinformáticos y Redes (SMIX)** — Institut Daniel Blanxart i Pedrals (2019 – 2021)

CERTIFICACIONES Y CURSOS

- CompTIA CySA+ CS0-003 — En preparación (2026 – 2027)
- Security Operations Center (SOC) — Skillsoft (2025)
- Inteligencia sobre Amenazas Cibernéticas 101 (2025)
- Introducción a la Ciberseguridad — Cisco (2025)
- Ciberseguridad Avanzada en entornos IT/OT (2025)

IDIOMAS Y OTROS

Castellano — Nativo **Catalán** — Nativo **Inglés** — Básico **Carnet de conducir** — B