JONAS FERNANDEZ

ANALISTA DE CIBERSEGURIDAD | SOC / BLUE TEAM | DETECTION ENGINEERING

Valencia, España | Disponible para reubicación en la UE | Remoto | jonas.ezequiel.fernandez.munoz@gmail.com |
linkedin.com/in/jonás-fernández-as | github.com/jonas-fernandez-as | jonas-fernandez-as.github.io

PERFIL PROFESIONAL

Analista de ciberseguridad orientado a SOC, Blue Team y Detection Engineering, con base sólida en redes, sistemas y seguridad ofensiva. Trabajo con Wazuh, Windows Event Logs, MITRE ATT&CK, CAPE Sandbox y Procmon para analizar actividad maliciosa, extraer IOCs y validar detecciones en laboratorios controlados. Cuento con OSCP+ y CRTO, además de experiencia práctica en investigación de vulnerabilidades, incluida la CVE-2026-14856 coordinada con INCIBE. Mi enfoque combina fundamentos técnicos, análisis de amenazas y conocimiento ofensivo aplicado a detección y defensa.

COMPETENCIAS TÉCNICAS

Fundamentos de redes y sistemas: OSI, TCP/IP, TCP/UDP, DNS, HTTP/HTTPS, SMB, LDAP, Kerberos, Wireshark, Windows y Linux

SOC / Detección: Wazuh (SIEM/EDR), Windows Event Logs, MITRE ATT&CK, correlación de eventos, IOCs, Detection Engineering, CVSS v3.1/v4.0

Threat / Malware / CTI: CAPE Sandbox, análisis conductual, TTPs, ransomware, entornos aislados, análisis de indicadores e inteligencia de amenazas

Active Directory / Offensive Security: Active Directory, BloodHound, Kerberoasting, OWASP Top 10, Burp Suite, Metasploit, Sliver, Cobalt Strike

Scripting: Python, PowerShell, Bash, C

EXPERIENCIA

Investigador de Seguridad Independiente

Autónomo | Remoto | 2024 - Actualidad

- **Analizo muestras de malware** con CAPE Sandbox y documento comportamiento, IOCs y TTPs relevantes para detección.
- **Simulo actividad adversaria** con Sliver en laboratorios controlados y correlaciono la telemetría generada con Wazuh, Procmon y Windows Event Logs para validar casos de uso de detección.
- **Mapeo técnicas observadas** a MITRE ATT&CK y traduzco hallazgos ofensivos en hipótesis y oportunidades de detección defensiva.
- **Identifiqué 4 vulnerabilidades** en software en producción, incluida CVE-2026-14856, coordinando la divulgación con INCIBE.
- **Completé 200+ máquinas** en Hack The Box y Proving Grounds y elaboré 70+ informes técnicos de seguridad con evidencias, impacto, CVSS y recomendaciones.
- **Creador de contenido técnico** de ciberseguridad en YouTube (@JonaStrikeX).

INVESTIGACIÓN DE VULNERABILIDADES

- **CVE-2026-14856** - Stored XSS + CSRF to Administrator account takeover en TastyIgniter Media Manager v4.3.0. CVSS v4.0 – 6.3 (Medium) . Coordinada por INCIBE.
- **3 vulnerabilidades adicionales** actualmente en divulgación coordinada con INCIBE: Local Privilege Escalation (CVSS 9.3), Remote Code Execution (CVSS 8.6) y Sensitive Information Disclosure (CVSS 8.7). CVEs pendientes de asignación oficial.

CERTIFICACIONES Y FORMACIÓN

OSCP+ | Offensive Security | 2026
CRTO | Zero-Point Security | 2026
eJPTv2 | INE / eLearnSecurity | 2025
Maldev Academy | Malware Development in C | En curso
Técnico Superior en ASIR | Administración de Sistemas Informáticos en Red | Inicio septiembre 2026 - remoto
Cisco Networking Essentials | Cisco Networking Academy | 2023

IDIOMAS

Español - Nativo | Inglés - B2 | Italiano - B2