DAVID PADRON

Threat Intelligence Analyst | OSINT | Seguridad Ofensiva
Buenos Aires, Argentina
Email: davidpadron.cyber@gmail.com
LinkedIn: linkedin.com/in/david-padron-9a74aa323
GitHub: github.com/FeathersMcgr4w

PERFIL PROFESIONAL

Analista de Cyber Threat Intelligence con experiencia en OSINT ofensivo, reconocimiento avanzado sobre superficie de ataque y trabajo en conjunto con equipos de Red Team. Especializado en la recolección de información con fuentes abiertas (OSINT) y cerradas, mapeo de infraestructuras web, identificación de vectores de ataque y automatización de tareas en Linux. Experiencia en análisis de amenazas, IOCs, modelado de riesgos bajo estándares MITRE ATTACK, NIST y OWASP. Desarrollo de herramientas personalizadas en Bash y Python para explotar vulnerabilidades, ejecutar scraping de datos y scripting automatizado. Utilizo agentes de inteligencia artificial (IA) como Gpt, Gemini o Copilot para procesar datos y desarrollar inteligencia útil para generar informes y grafos que permitan fundamentar las futuras tomas de decisiones. Ejecuto tareas de inteligencia corporativa, investigación de personas, huella digital, inteligencia de imágenes (IMINT), redes sociales (SOCMINT), y monitoreo de campañas de phishing y filtraciones en Deep y Dark web para protección de marca corporativa.

EXPERIENCIA PROFESIONAL

Cyber Intelligence Analyst

Pentesting Al Palo
12/2025 – Actualidad

- Inteligencia corporativa.
- Investigación de personas.
- Ciber perfilamiento y rastreo de huella digital.
- Inteligencia de imágenes (IMINT).
- Inteligencia de redes sociales (SOCMINT).
- Búsqueda de filtración de datos personales.
- Inteligencia geoespacial y geolocalización.

Cyber Threat Intelligence Analyst

Pentesting Al Palo
01/2024 – Actualidad

- Reconocimiento avanzado de superficie de ataque.
- Recolección de datos con fuentes abiertas (OSINT) y cerradas.
- Mapeo de infraestructura web, servidores, aplicativos, Firewalls (WAF).
- Identificación de vectores de ataque y explotación con pruebas de concepto (POC).
- Análisis de amenazas y riesgos basado en estándares MITRE ATTACK, CVE, CVSS y NIST.
- Desarrollo de herramientas con bash y python para explotar vulnerabilidades, scraping de datos y scripting.
- Monitoreo de campañas de ciberataques y phishing.
- Monitoreo de filtraciones en Deep y Dark web.
- Elaboración de informes técnicos para auditorías de pentesting web.
- Consultoría de seguridad a equipos de desarrollo de software (AppSec).
- Implementación de políticas de seguridad basadas en NIST 800-53
- Tareas de backup, administración básica de infraestructura, hardening, servidores y máquinas virtuales.

Instructor de Seguridad Informática

Encode S.A
05/2025 – 06/2025

- Diseño e impartición de capacitación en seguridad informática al personal de desarrollo de software y lideres.
- Temas: fundamentos de seguridad, amenazas, buenas prácticas, introducción al desarrollo seguro y políticas de seguridad.

Técnico de Soporte Informático

Autónomo
2020 – 2024

- Instalación de sistemas operativos Windows y Linux.
- Análisis y limpieza de malware.
- Optimización de sistemas y mantenimiento preventivo.
- Armado de computadoras empresariales y hogareñas.
- Armado de rigs para minería de criptomonedas.
- Instalación de impresoras y equipos para comercios.

EDUCACIÓN Y CURSOS

Cisco Networking Academy

- Introduction to Cybersecurity
- Networking Basics
- Network Devices and Initial Configuration
- Endpoint Security
- Network Defense
- Cyber Threat Management
- Junior Cybersecurity Analyst Exam

Hack The Box

- Más de 20 laboratorios de pentesting web

Udemy

- Análisis dinámico de malware en Windows
- Análisis estático de malware en Windows

OSINT y Ciberinteligencia

- Técnicas avanzadas en Ciberinteligencia (TACINT) – Hefin
- Ivan Castañeda – Mentoria OSINT y Ciberdelincuencia
- EVILSEC – Técnicas de Investigación e Inteligencia OSINT
- XSEC – Curso de Ciberinteligencia

HABILIDADES TÉCNICAS

Sistemas Operativos: Linux, Windows
Lenguajes y Scripting: Python, Bash, JavaScript, C/C++, SQL, MongoDB
OSINT y Pentesting: BurpSuite, Nmap, Wireshark, Shodan, FOFA, Spiderfoot, Subfinder, Katana, DNSX, HTTPX, Wfuzz, Exiftool, Espoofer, Sherlock, Holehe, Ghunt.
Threat Intelligence: Hybrid Analysis, VirusTotal, URLScan, AbuseDB, OpenCTI, Maltego, Gephi.

Investigación de Ciberdelincuencia: BreachForums, DarkForum, Telegram, Twitter
Análisis de Malware: ProcMon, ProcExp, Autoruns, ESET SysInspector, Detect It Easy, OleTools, Ghidra, Malcat.
Frameworks: MITRE ATTACK, CVE/CVSS, OWASP, NIST 800-53
Virtualización: VirtualBox, VMware
Especialidades: OSINT ofensivo, Seguridad Ofensiva, Red Team Recon, AppSec, Threat Intelligence, Cyber Intelligence Analyst.

HABILIDADES BLANDAS

Creatividad, Autodidacta, Análisis, Investigación, Trabajo en equipo, Resolución de problemas.

IDIOMAS

Inglés B1 – Cambridge Assessment English