NICOLÁS SOTOMAYOR

SOC Analyst Jr · Blue Team · Analista de Ciberseguridad · Soporte IT N1/N2

Ubicación Mendoza, Argentina | Teléfono +54 9 261 507-2440 | Email nikosotomayor.cyber@gmail.com

Portfolio nicolassotomayor.com.ar | LinkedIn /in/nikosotomayor-cyber | GitHub /nicosotomayor

Instagram @nikosotomayor.cyber | TikTok @nicolassotomayor.soc | YouTube @nicolassotomayorcyber

Disponible para trabajo remoto, híbrido o presencial — Argentina · LATAM · España

PERFIL PROFESIONAL

Técnico Superior en Ciberseguridad orientado a operaciones SOC y Blue Team. Experiencia práctica documentada en **triage de alertas, análisis de logs y tráfico de red, detección de amenazas e investigación de incidentes** aplicando el framework MITRE ATT&CK, con casos reales publicados en GitHub. Más de 2 años en soporte técnico N1 y una sólida trayectoria previa en atención al cliente, gestión de stock y coordinación de equipos. Busco incorporarme como **SOC Analyst L1 / Jr, Blue Team Jr, Analista de Ciberseguridad o Soporte IT N1-N2**. Disponibilidad inmediata.

EXPERIENCIA PROFESIONAL

Desarrollador Web · Plugins WordPress · Seguridad Web Ago 2023 – Actualidad

Studio Milano (studiomilano.com.ar) — Agencia de diseño web y marketing digital · Freelance · Remoto

- Diseño, desarrollo y mantenimiento de sitios web en WordPress + Elementor para clientes de la agencia: consultoras, estudios profesionales, turismo, inmobiliario y portales de información.
- Proyectos destacados: Securytas (consultora de ciberseguridad), Wine Trip Mendoza (tours de bodegas), Quequén Playa Fideicomiso (landing inmobiliaria), CotizaYa (cotizaciones de dólar y mercados) y sitios de estudios contables y jurídicos.
- Tiendas online con WooCommerce (Pau Gráfica Ok, tienda de recursos digitales).
- Desarrollo de plugins de WordPress a medida: **CyberLab** (análisis de seguridad web: HTTPS, certificado TLS, cabeceras de seguridad y recomendaciones), plugin propio que gestiona el contenido de la home de Studio Milano y **Jugando con Neo** (juegos educativos infantiles).
- Tarjetas de contacto digitales con QR para profesionales y sitios-invitación para eventos.
- Prototipo **StudioMilano Immersive**: app de propiedades inmobiliarias recorribles en 3D con exportación a video MP4.
- Servicio de auditoría, optimización y seguridad web: hardening de WordPress (usuarios, control de accesos y actualizaciones), mitigación de vulnerabilidades (OWASP Top 10), backups automáticos y monitoreo de disponibilidad.

Tutor Tecnológico · Soporte IT N1 Jul 2021 – Jul 2023

Dirección General de Escuelas — Mendoza · Presencial

- Soporte técnico Nivel 1 (hardware, software y conectividad) a más de 300 usuarios.
- Administración de usuarios y permisos en sistemas institucionales.
- Capacitación en concientización sobre phishing y buenas prácticas de seguridad al personal.
- Coordinación con equipos de soporte para el escalamiento y la resolución de incidencias.

EXPERIENCIA LABORAL PREVIA

Trayectoria en atención al cliente, gestión de stock y coordinación de equipos, con progresión a roles de responsabilidad.

Chofer profesional y dueño de flota 2020 – Actualidad

Uber — Mendoza

- Gestión integral de una flota de vehículos: administración, control de costos y coordinación de choferes.
- Atención al cliente con altos estándares de calidad y puntaje, cumpliendo políticas de la plataforma.

Repositor de salón · Postulante a Jefe de Salón 2015 – 2020

Coto CICSA — Sector Alimentos

- Reposición y control de stock en el sector de alimentos, asegurando disponibilidad y rotación de productos.
- Ejercicio del rol de Postulante a Jefe de Salón: coordinación de repositores internos y externos.
- Gestión de pedidos y control de stock, y manejo de proveedores.

Cajero · Repositor 2014 – 2015

Millán S.A.

- Atención en caja y reposición de mercadería, con manejo de efectivo y atención al cliente.

Playero con cartera · Encargado de turno 2011 – 2014

Rumaos S.A. — Estación de servicio

- Atención al cliente y manejo de cartera de clientes como playero.
- Encargado de turno: coordinación del personal, manejo de proveedores y control de stock.

PROYECTOS DESTACADOS DE CIBERSEGURIDAD

Análisis de incidente Trickbot en Active Directory

github.com/nicosotomayor

- Investigación de un incidente de malware en entorno Active Directory: detección de comunicación con el servidor de comando y control (C2) y exposición de credenciales en el tráfico de red.
- Identificación de movimiento lateral y mapeo completo de la cadena de ataque con MITRE ATT&CK, con extracción de IoCs y recomendaciones de contención.

Detección de beaconing por DNS y HTTP

github.com/nicosotomayor

- Análisis de tráfico DNS y HTTP (Wireshark, TShark) para detectar patrones de beaconing compatibles con un canal de C2.
- Identificación de persistencia y extracción de indicadores de compromiso (IoCs) listos para bloquear y alimentar el SIEM.

Evaluación de vulnerabilidades — Metasploitable 3

github.com/nicosotomayor

- Enumeración de servicios y escaneo autenticado de vulnerabilidades con Nmap y Nessus.
- Clasificación de hallazgos por severidad (CVSS) e informe priorizado con recomendaciones de remediación.

Mini SIEM en Python + simuladores interactivos

nicolassotomayor.com.ar

- Mini SIEM en Python: ingesta de logs, correlación de eventos y generación de alertas.
- Cuatro simuladores propios publicados en la web: turno de SOC con triage y MITRE ATT&CK, analizador de phishing, práctica de Security+ (SY0-701) y análisis de logs.

PRÁCTICA EN PLATAFORMAS SOC / BLUE TEAM

TryHackMe · Blue Team Labs Online · CyberDefenders

- Análisis de logs de Windows (Event IDs 4624, 4625, 4672, 4688, 4768/4776): detección de fuerza bruta, movimiento lateral y escalada de privilegios.
- Correlación de eventos con Splunk y Wazuh para detectar comportamiento anómalo.

- Análisis forense básico con Autopsy, Volatility y FTK Imager.
- Documentación de incidentes en reportes técnicos con evidencia y recomendaciones.

STACK TÉCNICO

SIEM / SOC: Splunk · Wazuh · Sigma Rules · MISP · DeepBlueCLI
Análisis de red: Wireshark · tcpdump · TShark · Nmap · TCP/IP · DNS · HTTP
Forense digital: Autopsy · Volatility · FTK Imager
Threat Intel / OSINT: VirusTotal · ANY.RUN · Maltego · TheHarvester · Shodan
Vulnerability scanning: Nessus · OpenVAS
Sistemas: Windows / Windows Server · Linux (Ubuntu, Kali) · Active Directory
Scripting: Python · Bash · PowerShell
Desarrollo web: WordPress · Elementor · WooCommerce · Plugins WordPress a medida
Frameworks: MITRE ATT&CK · OWASP Top 10 · NIST (respuesta a incidentes)

CERTIFICACIONES Y FORMACIÓN

Relevantes para SOC / Blue Team

- CompTIA Security+ (SY0-701) — CompTIA — En preparación · examen dic. 2026
- Blue Team Junior Analyst Pathway — Security Blue Team — 2025
- Bootcamp Analista SOC Nivel 1 (v.5) — ComunidadDOJO — 2024
- SOC: Centro de Operaciones de Seguridad — Fundación Accenture — 2024
- Endpoint Security — Cisco Networking Academy — 2024
- Curso Completo de Ciberseguridad Defensiva — Udemy — 2025

Formación complementaria

- Cisco Networking Academy: Introduction to Cybersecurity · Networking Basics · Networking Devices and Initial Configuration
- Curso Completo de Hacking Ético y Ciberseguridad — Udemy
- Fundamentos de Ciberseguridad I y II — Fundación Accenture
- Introducción al Sistema Operativo Kali Linux — Comunidad Reparando

FORMACIÓN ACADÉMICA

Técnico Superior en Ciberseguridad — Dic 2024
CEDSA — Centro de Estudios a Distancia de Salta

IDIOMAS

Español — nativo. Inglés — intermedio (lectura técnica fluida, comunicación profesional escrita).