NICOLÁS SOTOMAYOR

Técnico Superior en Ciberseguridad | SOC Analyst (Junior) | Blue Team
Mendoza, Argentina • nikosotomayor.cyber@gmail.com • +54 9 261 507-2440
• linkedin.com/in/nikosotomayor-cyber • github.com/nicosotomayor
• Disponible para trabajo remoto: Argentina · América Latina · España

RESUMEN PROFESIONAL

Técnico Superior en Ciberseguridad (egresado diciembre 2024) con formación especializada en operaciones SOC y Blue Team. Experiencia práctica documentada en análisis de malware, detección de beaconing, análisis de tráfico de red e investigación de incidentes aplicando el framework MITRE ATT&CK. Más de 2 años de experiencia en soporte técnico y gestión de sistemas en entorno institucional. Portfolio de proyectos publicado en GitHub con casos reales de análisis forense y detección de amenazas.

PROYECTOS DE CIBERSEGURIDAD

Trickbot Incident Analysis – Active Directory —
github.com/nicosotomayor/trickbot-incident-analysis-ad
- Análisis de incidente de malware en entorno Active Directory.
- Detección de comunicaciones C2, exposición de credenciales en tráfico de red e identificación de movimiento lateral.
- Mapeo completo de tácticas y técnicas con MITRE ATT&CK.

DNS & HTTP Beaconing Detection —
github.com/nicosotomayor/network-traffic-analysis-dns-http-beaconing
- Detección de actividad de beaconing mediante análisis de tráfico DNS y HTTP.
- Identificación de patrones de persistencia y extracción de IoCs.

Mini SIEM – Python — ***github.com/nicosotomayor/mini-siem-python***
- Simulación básica de SIEM: ingesta de logs, correlación de eventos y generación de alertas.

Vulnerability Assessment – Metasploitable 3 —
github.com/nicosotomayor/metasploitable3-vulnerability-assessment
- Evaluación de vulnerabilidades con Nmap y Nessus: enumeración de servicios, clasificación de riesgo y recomendaciones de remediación.

EXPERIENCIA PROFESIONAL

Desarrollador Web con foco en Seguridad | Studio Milano (Freelance)
Agosto 2023 – Actualidad | Remoto
- Implementación de OWASP Top 10 en todos los proyectos web desarrollados.
- Hardening de instalaciones WordPress: gestión de usuarios, control de accesos y actualizaciones.
- Identificación y mitigación de vulnerabilidades en entornos web de producción.
- Configuración de backups automáticos y monitoreo de disponibilidad.

Tutor Tecnológico | Dirección General de Escuelas – Mendoza
Julio 2021 – Julio 2023 | Presencial
- Soporte técnico Nivel 1: hardware, software y conectividad para más de 300 usuarios.
- Administración de usuarios y permisos en sistemas institucionales.
- Capacitación en concientización sobre phishing y buenas prácticas de seguridad informática.
- Coordinación con equipos de soporte para resolución de incidencias escaladas.

PRÁCTICA EN PLATAFORMAS CTF / SOC

TryHackMe | Blue Team Labs Online | CyberDefenders
- Análisis de logs Windows (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 detección de comportamiento anómalo.
- Análisis forense básico con Autopsy, Volatility y FTK Imager.
- Documentación de incidentes en reportes técnicos con evidencias y recomendaciones.

FORMACIÓN ACADÉMICA

Técnico Superior en Ciberseguridad – CEDSA (Centro de Estudios a Distancia de Salta)
Egresado: Diciembre 2024

CERTIFICACIONES Y FORMACIÓN COMPLEMENTARIA

- CompTIA Security+ (SY0-701) – En preparación (objetivo: octubre 2026)
- Security Blue Team – Blue Team Junior Analyst Pathway (2025)
- Fundación Accenture – SOC: Centro de Operaciones de Seguridad (2024)
- Cisco Networking Academy: Introduction to Cybersecurity | Networking Basics | Endpoint Security | Networking Devices

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
- **Vuln. Scanning:** Nessus · OpenVAS
- **Sistemas:** Windows / Windows Server · Linux (Ubuntu, Kali) · Active Directory
- **Scripting:** Python · Bash · PowerShell
- **Frameworks:** MITRE ATT&CK · OWASP Top 10.

IDIOMAS

- **Español –** Nativo
- **Inglés –** Intermedio (lectura técnica fluida, comunicación profesional escrita)