GABRIEL LEANDRO PALAZZINI

Operaciones de Red → Transición Blue Team (Entry/Mid-Level)

INFORMACIÓN DE CONTACTO

Email: gabrielleandro.p@outlook.com

Teléfono: +54 11 3097-6948

LinkedIn: linkedin.com/in/gabrielpalazzini

GitHub: github.com/dekapala

Ubicación: Buenos Aires, Argentina

Disponibilidad: Inmediata • Preferencia híbrido/remoto

RESUMEN PROFESIONAL

Analista de Redes con 11+ años en Telecom Argentina gestionando infraestructura crítica DOCSIS/HFC. Actualmente en transición formal a SOC/Blue Team con laboratorios reproducibles y certificaciones en curso.

Combinación única: Experiencia senior en operaciones + formación activa en detección y respuesta de incidentes con enfoque en escenarios reales.

Autodidacta con IA: Todos los proyectos técnicos desarrollados 100% con herramientas de IA (ChatGPT, Claude, Gemini). Dominio avanzado de Prompt Engineering aplicado a seguridad y desarrollo.

Fortalezas clave:

- Profundo conocimiento de operaciones de red y ciclo de vida de incidentes
- Mentalidad proactiva de troubleshooting y análisis de causa raíz
- Experiencia con herramientas de monitoreo (ServAssure NXT, Grafana, Nagios)
- Aprendizaje rápido con capacidad demostrada para dominar nuevas tecnologías de forma autónoma

EXPERIENCIA LABORAL

Analista de Redes – Telecom Argentina S.A.

Febrero 2014 – Presente (11+ años)

OPERACIONES DE RED Y GESTIÓN DE INCIDENTES

Monitoreo y gestión de infraestructura HFC/DOCSIS nacional sirviendo a millones de clientes. Respuesta a incidentes: troubleshooting de problemas complejos de red utilizando SNMP, Grafana y herramientas de monitoreo propietarias. Análisis de causa raíz: investigación de degradación de performance, cortes y eventos de seguridad. Monitoreo proactivo con ServAssure NXT e Icinga/Nagios para detección temprana.

Coordinación con equipos multifuncionales (NOC, vendors, operaciones de campo) para resolución de incidentes. Documentación de incidentes y creación de reportes post-mortem para mejora continua.

Logros clave:

- Reducción del MTTR (Mean Time To Repair) mediante metodologías sistemáticas de troubleshooting
- Implementación de reglas de alertas proactivas que previnieron interrupciones potenciales del servicio
- Mentoría a analistas junior sobre protocolos de red y técnicas de troubleshooting

Tecnologías: DOCSIS 3.0/3.1, HFC, CMTS (ARRIS/CommScope), SNMP, Grafana, ServAssure NXT, Icinga, TCP/IP, routing/switching

Laboratorios Blue Team y Proyectos de Autodesarrollo

2024 – Presente

Formación activa en ciberseguridad con laboratorios reproducibles y herramientas:

DETECTOR DE INTRUSIONES DE RED

Python + Scapy

Detección en tiempo real de escaneos de puertos y ataques de ARP spoofing. Análisis personalizado de paquetes y generación de alertas.

GitHub: github.com/dekapala/network-intrusion-detector

LABORATORIO SURICATA IDS

Docker + Kubernetes

Despliegue de Suricata en entornos containerizados para análisis de tráfico. Creación de reglas de detección personalizadas para patrones de ataque comunes. Integración con stack ELK para visualización de logs.

GitHub: github.com/dekapala/suricata-docker-lab

DESARROLLO DE PLAYBOOKS SOC

Documentación de flujos de trabajo de respuesta a incidentes (detección → contención → erradicación → recuperación). Mapeo de técnicas MITRE ATT&CK a métodos de detección. Todos los playbooks disponibles en GitHub con escenarios reproducibles.

ESCÁNER DE VULNERABILIDADES

Python + Nmap

Escaneo automatizado de redes y reporte de vulnerabilidades. Integración con bases de datos CVE para evaluación de riesgos.

GitHub: github.com/dekapala/vuln-scanner

EDUCACIÓN Y CERTIFICACIONES

ISC2 Candidate – En Curso *Fecha estimada: Q1 2025*

Cursos de Ciberseguridad:

- Operaciones Blue Team y estrategias defensivas
- Flujos de trabajo de detección y respuesta a incidentes
- Monitoreo y análisis de seguridad de red

Título: Escuela Técnica – Electrónica (EET N°3, Argentina)

HABILIDADES TÉCNICAS

INTERMEDIO (USO ACTIVO)

Monitoreo de Redes: ServAssure NXT, Grafana, Nagios/Icinga, SNMP

Protocolos de Red: TCP/IP, DNS, DHCP, HTTP/HTTPS, routing/switching

Sistemas Operativos: Linux (Ubuntu/Debian), Windows Server

Herramientas: Wireshark, tcpdump, Git/GitHub

Scripting: Python (automatización de redes, herramientas de seguridad)

APRENDIZAJE/ENTORNO DE LABORATORIO

Herramientas de Seguridad: Suricata IDS/IPS, Snort, pfSense

Contenedores: Docker, Kubernetes (despliegues de seguridad)

Gestión de Logs: Stack ELK (Elasticsearch, Logstash, Kibana)

Fundamentos SIEM: Splunk, Wazuh (labs de autoestudio)

Threat Intelligence: Framework MITRE ATT&CK, herramientas OSINT

INFRAESTRUCTURA DE RED (11+ AÑOS)

DOCSIS/HFC: ARRIS C4/E6000, CommScope CMTS, cable modems

RF/Cable: Análisis de señal, troubleshooting, mantenimiento

Monitoreo: Alertas en tiempo real, planificación de capacidad, gestión de SLA

HABILIDADES BLANDAS

- Mentalidad analítica y troubleshooting sistemático
- Comunicación técnica clara (Inglés: intermedio lectura/escritura)
- Aprendizaje autodirigido y adaptación a nuevas tecnologías
- Colaboración multidisciplinaria y coordinación de incidentes

ENFOQUE DE DESARROLLO CON IA

Filosofía: Desarrollo ético y transparente con IA como copiloto.

DESARROLLO 100% ASISTIDO POR IA

Todos los proyectos desarrollados usando Prompt Engineering avanzado con ChatGPT, Claude y Gemini. Refinamiento iterativo: prompt → código → prueba → mejora. Prompts anonimizados y toma de decisiones auditable (historial de commits).

ESTÁNDARES GITHUB

Cada repositorio incluye archivos README completos. Instrucciones de setup reproducibles (dependencias, config, uso). Datasets de prueba y outputs de ejemplo incluidos. Documentación clara del proceso de aprendizaje y desafíos enfrentados.

POR QUÉ ESTO IMPORTA PARA ROLES BLUE TEAM

Demuestra capacidad de aprender e implementar rápidamente nuevas tecnologías de seguridad. Muestra enfoque práctico de resolución de problemas con tooling moderno. Prueba capacidad de aprendizaje autodirigido esencial para entornos SOC. Las habilidades de IA son cada vez más críticas para automatización y análisis de seguridad.

OBJETIVOS PROFESIONALES

Objetivo inmediato: Rol Entry a Mid-level en Blue Team / Analista SOC

LO QUE APORTO:

- 11+ años en operaciones de red: Profundo entendimiento de infraestructura y ciclo de vida de incidentes
- Laboratorios hands-on de ciberseguridad: Experiencia práctica con IDS/IPS, detección de amenazas y respuesta
- Aprendizaje proactivo: Autodidacta con proyectos reproducibles en GitHub y documentación completa
- Mentalidad operacional: Experiencia gestionando incidentes reales bajo presión
- Dominio de IA: Capacidad de desarrollar y desplegar rápidamente herramientas y automatización de seguridad

LO QUE BUSCO:

- Mentoría de profesionales experimentados de Blue Team
- Oportunidades para aplicar expertise de redes a operaciones de seguridad
- Entorno que valore el aprendizaje continuo y el intercambio de conocimiento
- Rol híbrido/remoto con foco en detección, análisis y respuesta a incidentes

INFORMACIÓN ADICIONAL

Autorización de Trabajo: Argentina (no requiere sponsorship local para roles remotos)

Idiomas: Español (nativo), Inglés (intermedio - lectura/escritura para documentación técnica)

Disponibilidad: Inicio inmediato para la oportunidad correcta

Industrias Preferidas: Telecom, MSP/MSSP, Empresas tech con equipos SOC establecidos

PRESENCIA ONLINE

GitHub: github.com/dekapala (laboratorios de seguridad reproducibles)

LinkedIn: linkedin.com/in/gabrielpalazzini