GABRIEL LEANDRO PALAZZINI

Network Operations → Blue Team Transition (Entry/Mid-Level)

CONTACT INFORMATION

Email: gabrielleandro.p@outlook.com

Phone: +54 11 3097-6948

LinkedIn: linkedin.com/in/gabrielpalazzini

GitHub: github.com/dekapala

Location: Buenos Aires, Argentina

Availability: Immediate • Hybrid/Remote preferred

PROFESSIONAL SUMMARY

Network Analyst with 11+ years at Telecom Argentina managing critical DOCSIS/HFC infrastructure. Currently in formal transition to SOC/Blue Team with hands-on reproducible labs and certifications in progress.

Unique combination: Senior operations experience + active cybersecurity training with real-world incident detection and response focus.

Self-taught with AI: All technical projects 100% developed using AI tools (ChatGPT, Claude, Gemini). Advanced Prompt Engineering applied to security and development.

Key strengths:

- Deep understanding of network operations and incident lifecycle
- Proactive troubleshooting and root cause analysis mindset
- Experience with monitoring tools (ServAssure NXT, Grafana, Nagios)
- Quick learner with proven ability to master new technologies independently

WORK EXPERIENCE

Network Analyst – Telecom Argentina S.A.

February 2014 – Present (11+ years)

NETWORK OPERATIONS & INCIDENT MANAGEMENT

Monitor and manage national HFC/DOCSIS infrastructure serving millions of customers. Incident response: troubleshoot complex network issues using SNMP, Grafana, and proprietary monitoring tools. Root cause analysis: investigate performance degradation, outages, and security events. Proactive monitoring with ServAssure NXT and Icinga/Nagios for early detection.

Coordinate with cross-functional teams (NOC, vendors, field ops) for incident resolution. Document incidents and create post-mortem reports for continuous improvement.

Key achievements:

- Reduced MTTR (Mean Time To Repair) through systematic troubleshooting methodologies
- Implemented proactive alerting rules that prevented potential service disruptions
- Mentored junior analysts on network protocols and troubleshooting techniques

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

Blue Team Labs & Self-Development Projects

2024 – Present

Active cybersecurity training with reproducible labs and tools:

NETWORK INTRUSION DETECTOR

Python + Scapy

Real-time detection of port scans and ARP spoofing attacks. Custom packet analysis and alert generation.

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

SURICATA IDS LAB

Docker + Kubernetes

Deployed Suricata in containerized environments for traffic analysis. Created custom detection rules for common attack patterns. Integrated with ELK stack for log visualization.

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

SOC PLAYBOOK DEVELOPMENT

Documented incident response workflows (detection → containment → eradication → recovery). Mapped MITRE ATT&CK techniques to detection methods. All playbooks available in GitHub with reproducible scenarios.

VULNERABILITY SCANNER

Python + Nmap

Automated network scanning and vulnerability reporting. Integration with CVE databases for risk assessment.

GitHub: github.com/dekapala/vuln-scanner

EDUCATION & CERTIFICATIONS

ISC2 Candidate – In Progress

Expected: Q1 2025

Cybersecurity Courses:

- Blue Team operations and defensive strategies
- Incident detection and response workflows
- Network security monitoring and analysis

Degree: Technical High School – Electronics (EET N°3, Argentina)

TECHNICAL SKILLS

INTERMEDIATE (ACTIVE USE)

Network Monitoring: ServAssure NXT, Grafana, Nagios/Icinga, SNMP

Network Protocols: TCP/IP, DNS, DHCP, HTTP/HTTPS, routing/switching

Operating Systems: Linux (Ubuntu/Debian), Windows Server

Tools: Wireshark, tcpdump, Git/GitHub

Scripting: Python (network automation, security tools)

LEARNING/LAB ENVIRONMENT

Security Tools: Suricata IDS/IPS, Snort, pfSense

Containers: Docker, Kubernetes (security deployments)

Log Management: ELK Stack (Elasticsearch, Logstash, Kibana)

SIEM Basics: Splunk, Wazuh (self-study labs)

Threat Intelligence: MITRE ATT&CK framework, OSINT tools

NETWORK INFRASTRUCTURE (11+ YEARS)

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

RF/Cable: Signal analysis, troubleshooting, maintenance

Monitoring: Real-time alerting, capacity planning, SLA management

SOFT SKILLS

- Analytical mindset and systematic troubleshooting
- Clear technical communication (English: intermediate reading/writing)
- Self-directed learning and adaptation to new technologies
- Cross-team collaboration and incident coordination

AI-POWERED DEVELOPMENT APPROACH

Philosophy: Ethical and transparent development with AI as copilot.

100% AI-ASSISTED DEVELOPMENT

All projects developed using advanced Prompt Engineering with ChatGPT, Claude, and Gemini. Iterative refinement: prompt → code → test → improve. Anonymized prompts and auditable decision-making (commit history).

GITHUB STANDARDS

Every repository includes comprehensive README files. Reproducible setup instructions (dependencies, config, usage). Test datasets and example outputs included. Clear documentation of learning process and challenges faced.

WHY THIS MATTERS FOR BLUE TEAM ROLES

Demonstrates ability to quickly learn and implement new security technologies. Shows practical problem-solving approach with modern tooling. Proves self-directed learning capability essential for SOC environments. AI skills are increasingly critical for security automation and analysis.

CAREER GOALS

Immediate target: Entry to Mid-level Blue Team / SOC Analyst role

WHAT I BRING:

- 11+ years network operations: Deep understanding of infrastructure and incident lifecycle
- Hands-on cybersecurity labs: Practical experience with IDS/IPS, threat detection, and response
- Proactive learning: Self-taught with reproducible GitHub projects and documentation
- Operational mindset: Experience managing real-world incidents under pressure
- AI proficiency: Ability to rapidly develop and deploy security tools and automation

WHAT I'M SEEKING:

- Mentorship from experienced Blue Team professionals
- Opportunities to apply network expertise to security operations
- Environment that values continuous learning and knowledge sharing
- Hybrid/remote role with focus on detection, analysis, and incident response

ADDITIONAL INFORMATION

Work Authorization: Argentina (local sponsorship not required for remote roles)

Languages: Spanish (native), English (intermediate - reading/writing for technical docs)

Availability: Immediate start for the right opportunity

Preferred Industries: Telecom, MSP/MSSP, Tech companies with established SOC teams

ONLINE PRESENCE

GitHub: github.com/dekapala (reproducible security labs)

LinkedIn: linkedin.com/in/gabrielpalazzini