



BENJAMIN TITO
VINCENTI

SOC Analyst · Blue Team
Security Technician

CONTACT

LOCATION
Salta, Argentina

EMAIL
benjatitovincenti@gmail.com

GITHUB
github.com/vandalco

TRYHACKME
tryhackme.com/p/vandalco

TECHNICAL SKILLS

BLUE TEAM & SIEM

SplunkELKWazuh

Log AnalysisMITRE ATT&CK

NETWORK & RECON

WiresharkNmapTCP/IP

Firewalls

SYSTEMS & OFFENSIVE

LinuxBashPython

Burp SuiteMetasploit

OWASP

CERTIFICATIONS

Security Technician
Technical degree

TryHackMe SOC Level 1
Learning path

Security Analyst L1 (SAL1)
In progress

LANGUAGES

SpanishNative

EnglishProfessional

Resume

SOC Analyst (Blue Team) · Security Technician · 2026

PROFESSIONAL SUMMARY

Security Technician transitioning into Blue Team / SOC operations, currently training on the TryHackMe SOC Level 1 path. Hands-on with log analysis, SIEM (Splunk, ELK, Wazuh), network traffic analysis and incident response. A developer background gives me an edge to read code, map attack surface and investigate incidents from the inside out.

KEY COMPETENCIES

- Log Analysis & Alert Triage
- Network Analysis (Wireshark)
- Incident Response & Triage
- Linux & Scripting (Bash/Py)
- Packet & Log Investigation
- SIEM: Splunk, ELK, Wazuh
- Threat Detection (MITRE ATT&CK)
- Vulnerability Basics (OWASP)
- Secure Development (RLS/Auth)
- Threat Intelligence Basics

SELECTED PROJECTS

Content Integrity & Tamper Detection

SECURITY

github.com/vandalco/truthstamp

- Anchors SHA-256 and perceptual hashes on the Stellar blockchain to detect tampered media, even after recompression.
- Privacy-preserving design: only the hash is stored, never the original file. Built at PunaTech 2026.

Tech: Python · Flask · React · Stellar SDK · Web Crypto (SHA-256, pHash)

Secure B2B Marketplace

FULL-STACK

github.com/vandalco/milocal-ar

- Hardened Next.js platform with MFA, role-based access control (RBAC) and Supabase Row Level Security.
- CSP + HSTS security headers, rate limiting, Zod input validation and audit logging.

Tech: Next.js · TypeScript · Supabase (RLS) · Prisma · MercadoPago · Sentry

Secure WhatsApp Automation

AUTOMATION

github.com/vandalco/chatbot-inmobiliario

- Multi-tenant automation with secrets in a credential store (no hardcoded keys) and non-guessable UUID webhooks.
- Input validation and careful handling of customer PII across least-privilege sub-workflows.

Tech: n8n · OpenAI GPT-4o · WhatsApp Business API

Inventory PWA — Access Control

SOLO BUILD

github.com/vandalco/grifasi-inventory

- Offline-first PWA using only the Supabase anon key; data access enforced by RLS, never trusting the client.
- PIN authentication and controlled local-to-cloud synchronization.

Tech: JavaScript · Supabase (RLS) · Service Workers · PWA

PERSONAL STATEMENT

I'm building a Blue Team career on solid fundamentals: hands-on labs, clear documentation, and a developer's understanding of how systems break, ready to detect, triage and respond as a SOC L1 analyst.