# Guilherme Lima Santos

*Blue Team · Linux System Administration · Network Security · FullStack Development*

guilherme.softwarengineer@gmail.com | github.com/devguilhrm | linkedin.com/in/guilhermelima-dev/ | Sergipe, BR

## PERFIL TÉCNICO

Desenvolvedor com foco em desenvolvimento seguro, segurança defensiva e administração de sistemas Linux. Experiência prática em captura e análise de tráfego de rede (raw sockets, BPF, wire format de protocolos), análise estática de artefatos maliciosos (PE parsing, YARA, heurísticas MITRE ATT&CK), hardening de infraestrutura Linux e monitoramento contínuo com detecção de anomalias. Background em backend (Go, Java, TypeScript) aplicado à construção de ferramentas de segurança, pipelines de observabilidade e automação de operações em ambientes corporativos.

## PROJETOS - SEGURANÇA & INFRAESTRUTURA

### DNS Sniffer Passivo

**Go · Raw Sockets · BPF · RFC 1035 · Análise de Protocolo**

- Captura passiva de tráfego DNS via raw sockets AF_PACKET no Linux (acesso direto ao frame Ethernet L2, sem libc intermediária) e Npcap/gopacket no Windows.
- Parser próprio do DNS wire format (RFC 1035) - decodificação manual de header, sections e descompressão de labels com pointer 0xC0.
- Filtro BPF compilado em kernel-space (porta 53 UDP/TCP), eliminando context switches desnecessários para tráfego irrelevante.
- Suporte a DNS over TCP com reassembly de segmentos e tratamento do length prefix de 2 bytes.
- Decode de RRs: A, AAAA, CNAME, MX, TXT, SOA, SRV, OPT, HTTPS, PTR, NS; RDATA exibido em hex para tipos sem decoder.
- Modo verbose com TTL, RDATA raw, MAC src/dst, tamanho do frame L2, Transaction ID e RCODE.
- Vetores de análise futura: correlação query/response por TXID para latência de resolução e detecção de DNS rebinding / exfiltração via TXT.

### Static Malware Analyzer

**Go · PE Parsing · YARA · MITRE ATT&CK · VirusTotal API · Threat Intelligence**

- Análise estática de binários PE (.exe, .dll, .sys) sem execução - triagem inicial de amostras sem sandbox.
- PE parsing completo: arquitetura, machine type, subsystem, image base, entry point, timestamp de compilação, seções com entropia, overlay detection e packer hints.
- Extração e agrupamento de imports por DLL com import hash aproximado para clustering de famílias de malware.
- Mapeamento de imports suspeitos para TTPs do MITRE ATT&CK: T1055, T1486, T1056, T1622 e T1071.

- Motor YARA com fallback interno para ambientes sem instalação do engine oficial.
- Enriquecimento via VirusTotal API, relatório JSON por amostra com score de risco (0-100) e verdict.
- Modo batch com exportação CSV - estrutura adaptável a pipelines básicos de triagem em SOC.

### Sentinela - Plataforma de Monitoramento e Detecção de Incidentes Linux

**Go · Linux · Syslog · Detecção de Anomalias · File Integrity · Automação**

- Plataforma de monitoramento contínuo para ambientes Linux com foco em observabilidade, análise de logs e detecção de incidentes em tempo real.
- Módulos de detecção: brute force em SSH, port scanning, falhas de autenticação repetidas, execução de binários suspeitos e anomalias comportamentais de processos.
- File integrity monitoring com checksums de arquivos sensíveis e análise de eventos de segurança do Windows.
- Pipelines automatizados de análise de logs com geração de alertas, relatórios operacionais e integração com Syslog.
- Automação de rotinas de remediação via Shell Script e ferramentas nativas Linux.

### Lab-Controlado - Infraestrutura Corporativa Simulada

**Linux · Zabbix · Ansible · pfSense · Proxmox · PostgreSQL · Grafana · Go**

- Ambiente de laboratório simulando infraestrutura corporativa completa: Zabbix 7.x, PostgreSQL 16, Grafana 11, pfSense, AD DS, File Server, Ubuntu Server e Rocky Linux.
- Rede segmentada com VLANs (Management /24, Linux /24, Windows /24) e gateway pfSense com monitoramento SNMP v2c/v3.
- Templates Zabbix customizados para AD, File Server e segurança Linux; UserParameters, LLD, web scenarios e discovery rules versionados em repositório.
- Hardening SSH e baseline Linux via Ansible - fail2ban, checksums de arquivos críticos, monitoramento de eventos de autenticação.
- Actions de auto-remediação e relatório semanal via Zabbix API em Go.
- Ferramentas auxiliares em Go com testes automatizados e modo mock para CI em ambientes sem Linux.

### Keylogger Simulator - Lab de Análise Comportamental Defensiva

**Go · EDR Evasion Analysis · SMTP Exfil Simulation · Threat Modeling**

- Simulador educacional de keylogger em ambiente controlado para estudo de detecção comportamental e controles defensivos.
- Captura restrita ao terminal local - sem hooks globais de teclado, sem persistência e sem execução oculta.
- Módulo de exfiltração SMTP opt-in para simulação de C2 via e-mail e análise de controles de saída.
- Base para discussão de controles defensivos: EDR com detecção comportamental, MFA, análise de tráfego de saída e treinamento de usuários.

### LatesOS - Plataforma SaaS de Gestão Clínica (Fullstack)

**NestJS · Angular · React Native · PostgreSQL · Kafka · JWT/RBAC · Docker**

- Plataforma completa de gestão operacional para clínicas: agendamentos, financeiro recorrente, relatórios gerenciais e auditoria.
- Autenticação JWT com RBAC (ADMIN, RECEPTIONIST, PROFESSIONAL, CLIENT), refresh token e guards por role.
- Eventos assíncronos via Apache Kafka para processamento de agendamentos e notificações; suporte alternativo a RabbitMQ.
- App mobile em React Native para agendamentos e confirmações em tempo real.
- CORS configurável por ambiente, validação de entrada com class-validator, estrutura preparada para rate limit e rotação de segredos em produção.
- Deploy containerizado com Docker Compose; documentação de API via Swagger/OpenAPI.

## EXPERIÊNCIA PROFISSIONAL

### Analista de Sistemas Júnior

Tempo integral · abr/2025 - mai/2026

- Desenvolvimento de pipeline automatizado para processamento e arquivamento de Ordens de Serviço com OCR (OpenCV), validação de placas Mercosul/CONTRAN e geração de PDFs - redução de aproximadamente 80% no tempo operacional.
- Implementação de assinatura digital auditável: hash SHA-256, timestamp imutável e rastreabilidade por usuário/IP.
- Integração assíncrona com ERP via webhooks; arquitetura containerizada com Docker, logging estruturado, testes e pipelines CI/CD.
- Administração de banco de dados PostgreSQL, diagnóstico e troubleshooting de falhas de rede em ambientes Linux/Windows.
- Suporte técnico N1, manutenção de infraestrutura e sustentação de aplicações em ambiente operacional.

### Desenvolvedor Freelancer

mai/2026 – atual

- Integração de LLM para pesquisa de satisfação hospitalar (TypeScript/NestJS): gerenciamento de contexto conversacional, análise de sentimento em tempo real e lógica adaptativa de follow-up - aumento de 75% na taxa de conclusão.
- Desenvolvimento de sistemas fullstack e consultoria técnica.
- Desenvolvimento do Sistema LatesOS Plataforma completa de gestão operacional para clínicas: agendamentos, financeiro recorrente, relatórios gerenciais e auditoria.com aplicativo mobile para clientes agendarem e confirmarem agendamentos com base na disponibilidade dos profissionais,

### Estagiário de TI

Meio período · jun/2024 - abr/2025

- Suporte técnico a usuários, manutenção de hardware, diagnóstico inicial de falhas e suporte a infraestrutura básica de TI.

## HABILIDADES TÉCNICAS

### Segurança e Redes

Raw sockets (AF_PACKET), BPF filters, packet capture passiva, DNS wire format (RFC 1035), PE parsing, análise estática de malware, YARA, MITRE ATT&CK, file integrity monitoring, detecção de anomalias, hardening SSH, fail2ban, JWT/RBAC, SHA-256 audit trails, SNMP v2c/v3.

### Sistemas Operacionais

Debian - administração, hardening, automação e monitoramento, Kali Linux, RockyLinux.

### Infraestrutura e DevOps

Docker, Docker Compose, Proxmox VE, Ansible, pfSense, CI/CD (GitHub Actions), Zabbix, Grafana, PostgreSQL

### Backend

Go, Java (Spring Boot), TypeScript (NestJS) , JavaScript.

### Frontend / Mobile

Angular, React, React Native, TypeScript, SCSS, Tailwind

### Cloud

AWS EC2, S3, IAM, Lambda (AWS Cloud Practitioner)

## CERTIFICAÇÕES

IBSEC - Desenvolvimento Seguro de Software (DevSecOps)

IBSEC - Cybersecurity Awareness

IBSEC - Fundamentos de Redes

IBSEC - Hacker ético

IBSEC Analista Privacidade e Proteção de Dados Profissional (APDP)

AWS - Fundamentos da Computação em Nuvem

IFRS - Programador Web - 200h (HTML, CSS, JS, BD, Projetos Web)

Linux COMPLETO + SERVIDORES

Java Completo: POO + Projetos - 54h (Nélio Alves)

## FORMAÇÃO ACADÊMICA

Tecnólogo em Análise e Desenvolvimento de Sistemas · Unopar · 2026 - 2028

## IDIOMAS

Inglês - Fluente (leitura técnica de RFCs, documentação e especificações, escrita e conversação).