# Ailton Rocha

Threat Hunter & Detection Engineer

São Paulo, SP | ailton-1997@hotmail.com.br | linkedin.com/in/aiiltonrocha | github.com/lyonzin | lyonzin.github.io

## RESUMO

Threat Hunter & Detection Engineer com 7 anos na Vivo (Telefônica Brasil), protegendo um ambiente de 50 mil+ endpoints e servidores Linux, Windows e cloud. Conduzo threat hunting orientado a hipóteses com MITRE ATT&CK e TaHiTI, e transformo achados em detecções de produção no CrowdStrike Falcon (LogScale/CQL e IOAs customizados), Cortex XDR e Splunk, com redução de 90% nos falsos positivos. Base ofensiva sólida: trajetória voltada ao lado ofensivo desde 2009 (engenharia reversa, anti-cheat e anti-debug em servidores de jogos online), DCPT e 4 Pro Labs da Hack The Box. Pensar como o atacante é o que torna meu hunting e minhas detecções de Blue Team mais eficientes. Criador do knowledge-rag, servidor MCP de RAG local com 300+ estrelas no GitHub.

## COMPETÊNCIAS

**Threat Hunting e Detecção:** threat hunting orientado a hipóteses, Detection Engineering, MITRE ATT&CK, TaHiTI, regras de correlação, IOA e IOC, tuning de falsos positivos, Purple Team, Breach and Attack Simulation (BAS).

**Plataformas:** CrowdStrike Falcon, Falcon LogScale (CQL), Cortex XDR, Splunk (SPL), Wazuh, Sysmon, Trellix DLP, Trend Micro XDR, Panda Security, Darktrace, Elastic.

**Resposta a Incidentes e Forense:** DFIR, análise de malware, engenharia reversa, forense de memória (Volatility), Velociraptor, Autopsy, FTK, Wireshark.

**Segurança Ofensiva:** Active Directory (Kerberos, delegação, NTLM relay, ADCS ESC1 a ESC14), BloodHound, Impacket, NetExec, Rubeus, Certipy, Mimikatz, pivoting, evasão de EDR.

**Threat Intelligence:** CTI, monitoramento de marca, vazamento de credenciais, phishing e typosquatting, ransomware, relatórios executivos.

**Automação e IA:** Python, PowerShell, Bash, APIs REST, Model Context Protocol (MCP), RAG, agentes LLM autônomos e multi-agentes.

## EXPERIÊNCIA PROFISSIONAL

**Threat Hunter & Detection Engineer (Consultor de Cyber Security)** **02/2025 - Atual**

*Vivo (Telefônica Brasil), São Paulo, SP*

- Conduzo threat hunting orientado a hipóteses em ambiente de 50 mil+ endpoints com CrowdStrike Falcon e Falcon LogScale (CQL), mapeando a cobertura de técnicas no MITRE ATT&CK com a metodologia TaHiTI.
- Desenvolvo regras de detecção e IOAs customizados no CrowdStrike e no Cortex XDR; o tuning reduziu os falsos positivos em 90%.
- Construí agentes autônomos de IA (LLM) para operações de segurança: o agente de triagem N1 de alertas de Threat Intelligence encerrou 62 de 62 ocorrências no primeiro dia, todas confirmadas em revisão cega.
- Produzo o boletim mensal de Threat Intelligence para a liderança: telecom, setor financeiro, vazamentos de dados, ransomware e governo.
- Atuo em Purple Team com o Cymulate nos dois lados: crio testes de Breach and Attack Simulation, mapeio a cobertura de TTPs de grupos APT no MITRE ATT&CK v19 e avalio as soluções de segurança contra esses cenários.
- Tenho experiência prática na avaliação, criação de testes e uso em produção de EDR e XDR: CrowdStrike Falcon e Identity Protection, Cortex XDR, Trend Micro XDR, Panda Security e Darktrace.
- Faço engenharia reversa de binários maliciosos criptografados e avalio soluções de Identity Protection, EDR, XDR e SIEM em testes de estresse.

**Analista de Cyber Security Sênior, Threat Hunting** **07/2023 - 02/2025**

*Vivo (Telefônica Brasil), São Paulo, SP*

- Hunting de ameaças avançadas (APT, ransomware, spear phishing) com metodologia orientada a hipóteses e MITRE ATT&CK.
- Criei regras de detecção em CrowdStrike Falcon, Splunk (SPL), Sysmon, Wazuh e Trend Micro.
- Automatizei fluxos de hunting com Python e PowerShell, reduzindo a triagem manual em 60%.
- Escrevi playbooks, runbooks e a documentação de referência de LogScale usada pelos times de SOC.

**Analista de Cyber Security, CSIRT** **04/2020 - 07/2023**

*Vivo (Telefônica Brasil), São Paulo, SP*

- Investiguei e contive incidentes de ransomware, APT, phishing direcionado e ataques web (SQL injection, XSS, CSRF).
- Analisei malware e tráfego de rede para extrair indicadores de comprometimento (IOCs); monitorei AV, EDR e SIEM.
- Investiguei servidores e acessos VPN e produzi relatórios técnicos de incidente.

**Analista de Redes** **09/2019 - 01/2020**

*Logicalis (cliente Banco Santander), São Paulo, SP*

- Configuração de equipamentos Cisco e troubleshooting de redes LAN, WAN e wireless em ambiente bancário.

**Analista de Infraestrutura de Redes** **06/2019 - 09/2019**

*Central IT (Secretaria Municipal de Educação de São Paulo), São Paulo, SP*

- Operação de 10 mil switches e 8 mil access points em 1.500 escolas; firewalls SonicWall e pfSense; monitoramento com Zabbix.

**Estagiário de Redes** **03/2017 - 02/2019**

*NIC.br, projeto IX.br, São Paulo, SP*

- Configuração de BGP em ambiente multivendor (Cisco, Brocade, Extreme, Huawei) no IX.br, ponto de troca de tráfego da internet brasileira; LACP e VLANs bilaterais.

**Administrador de Servidores de Jogos Online e Engenharia Reversa (autônomo)** **01/2009 - 01/2014**

*Break GunZ, servidor de jogo online, São Paulo, SP*

- Construí e administrei servidores de jogos online em VPS Linux e Windows, com banco SQL Server.
- Desenvolvi sistema anti-cheat e proteções anti-debug e anti-tamper para binários Windows de 64 bits, com DLLs em C++ e Assembly.
- Fiz engenharia reversa de cliente e servidor (OllyDbg, Immunity Debugger, Process Hacker) para encontrar e fechar as falhas usadas por trapaceiros.
- Protegi a camada web com WAF e mitigação de DDoS na Cloudflare e scripts anti-SQL injection em PHP.

## PROJETOS

- **knowledge-rag** (criador e mantenedor), github.com/lyonzin/knowledge-rag: servidor MCP de RAG 100% local para agentes de IA, com busca híbrida (BM25, semântica e RRF), reranking por cross-encoder e 20 formatos de arquivo. 300+ estrelas, 49 forks, 28 mil+ downloads no PyPI e npm, CI com 35+ verificações em 9 combinações de sistema e versão de Python.
- **LogonHoursRobot** (repositório privado): robô 100% automático em PowerShell que aplica e audita restrições de horário de logon em vários domínios do Active Directory, com processamento por delta, verificação byte a byte, evidência forense com SHA-256, dashboard HTML e rollback granular; LDAP paginado testado com 23 mil+ usuários.
- **X-SHELL** (repositório privado): framework de Red Team para operações autorizadas, com gerenciamento de sessões de reverse shell, assinatura de artefatos e automação via MCP com agentes de IA (Claude Code, OpenAI e Cursor).

## CERTIFICAÇÕES

**eCTHP**, Certified Threat Hunting Professional (v2) | INE Security | ID 96700960 — 03/2024

**eCIR**, Certified Incident Responder | INE Security | ID 104767045 — 05/2024

**GCSE**, Guardicore Certified Segmentation Engineer | Akamai Guardicore | ID GCSE-171243106 — 12/2023

**GCSA**, Guardicore Certified Segmentation Administrator | Akamai Guardicore | ID GCSA-170342830 — 12/2023

**DCPT**, Desec Certified Penetration Tester | Desec Security | ID FVNS-QIJMH-OUVZ 12/2022
**SCFE**, Sec4US Certified Forensics Expert | Sec4US 10/2022
**PDPE**, Privacy and Data Protection Essentials | EXIN 02/2021

## LABORATÓRIOS PRÁTICOS: HACK THE BOX PRO LABS

**RastaLabs**, red team em Active Directory com evasão de defesas 11/2026
**Zephyr**, Active Directory multi-domínio, relay, trusts e pivoting | HTBCERT-D6337FFDC3 04/2026
**Puppet**, operações com C2, Active Directory e DevOps | HTBCERT-86470B4B5B 02/2026
**Dante**, pentest em rede corporativa com pivoting | HTBCERT-AAB49A3E31 12/2025

## FORMAÇÃO COMPLEMENTAR

**Detecção, forense e resposta**
**Advanced Digital Forensics for Windows** (GHADFW) | GoHacking 2025
**Reverse Engineering Malware** (EHREM) | GoHacking 2023
**Security Operation Center Foundations** | GoHacking 2023
**Splunk Enterprise 9.0 System Administration** | Splunk 2023
**Splunk Cloud Administration** | Splunk 2023
**Digital Forensics Advanced** | Sec4US 2022
**Active Directory Defense** (GHADD) | GoHacking, sem data

**Segurança ofensiva**
**Active Directory Certificate Services** (GHADCS) | GoHacking 2024
**Active Directory Operations** (EHADOP) | GoHacking 2023
**Endpoint Protection Evasion** (EHEPE) | GoHacking 2023
**Active Directory Exploitation** | Sec4US 2023
**Web API Exploitation** | Sec4US 2023
**Web Hacking na Prática 2.0** | CrowSec 2023
**Pentest Experience** | Desec Security 2022
**Pentest Profissional** | Desec Security 2022
**Wi-Fi Hacking Enterprise 1.0** | Desec Security 2021

**IA e redes**
**Formação em Inteligência Artificial** | branas.io 2026
**IPv6** | NIC.br 2018
**CCNA** (curso) | sem data

## FORMAÇÃO ACADÊMICA

**Pós-graduação em Engenharia de IA Aplicada** | UNIPDS | em andamento 2026
**Pós-graduação em Cyber Security** | Instituto Daryus 2019 - 2021
**Tecnólogo em Redes de Computadores** | Faculdade Impacta 2016 - 2018

## IDIOMAS

Português: nativo. Inglês: básico.