Ailton Rocha

Threat Hunter & Detection Engineer

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

SUMMARY

Threat Hunter and Detection Engineer with 7 years at Vivo (Telefônica Brasil), protecting a 50K+ endpoint environment with Linux, Windows and cloud servers. I run hypothesis-driven threat hunting with MITRE ATT&CK and TaHiTI, and turn findings into production detections on CrowdStrike Falcon (LogScale/CQL and custom IOAs), Cortex XDR and Splunk, cutting false positives by 90%. Solid offensive foundation: a career on the offensive side since 2009 (reverse engineering, anti-cheat and anti-debug for online game servers), DCPT and 4 Hack The Box Pro Labs. Thinking like the attacker is what makes my hunting and Blue Team detections more effective. Creator of knowledge-rag, a local RAG MCP server with 300+ stars on GitHub.

SKILLS

Threat Hunting & Detection: hypothesis-driven threat hunting, Detection Engineering, MITRE ATT&CK, TaHiTI, correlation rules, IOA and IOC, false positive tuning, Purple Team, Breach and Attack Simulation (BAS).

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

Incident Response & Forensics: DFIR, malware analysis, reverse engineering, memory forensics (Volatility), Velociraptor, Autopsy, FTK, Wireshark.

Offensive Security: Active Directory (Kerberos, delegation, NTLM relay, ADCS ESC1 to ESC14), BloodHound, Impacket, NetExec, Rubeus, Certipy, Mimikatz, pivoting, EDR evasion.

Threat Intelligence: CTI, brand monitoring, credential leaks, phishing and typosquatting, ransomware, executive reporting.

Automation & AI: Python, PowerShell, Bash, REST APIs, Model Context Protocol (MCP), RAG, autonomous and multi-agent LLM systems.

PROFESSIONAL EXPERIENCE

Threat Hunter & Detection Engineer (Cyber Security Consultant) **02/2025 - Present**

Vivo (Telefônica Brasil), São Paulo, Brazil

- Run hypothesis-driven threat hunting across a 50K+ endpoint environment with CrowdStrike Falcon and Falcon LogScale (CQL), mapping technique coverage in MITRE ATT&CK with the TaHiTI methodology.
- Develop detection rules and custom IOAs on CrowdStrike and Cortex XDR; tuning reduced false positives by 90%.
- Built autonomous AI (LLM) agents for security operations: the N1 triage agent for Threat Intelligence alerts closed 62 of 62 cases on day one, all confirmed in blind review.
- Produce the monthly Threat Intelligence bulletin for leadership: telecom, financial sector, data leaks, ransomware and government.
- Run Purple Team with Cymulate on both sides: I create Breach and Attack Simulation tests, map APT TTP coverage in MITRE ATT&CK v19 and evaluate security solutions against those scenarios.
- Hands-on experience evaluating, testing and running EDR and XDR in production: CrowdStrike Falcon and Identity Protection, Cortex XDR, Trend Micro XDR, Panda Security and Darktrace.
- Reverse engineer encrypted malicious binaries and stress-test Identity Protection, EDR, XDR and SIEM solutions.

Senior Cyber Security Analyst, Threat Hunting **07/2023 - 02/2025**

Vivo (Telefônica Brasil), São Paulo, Brazil

- Hunted advanced threats (APT, ransomware, spear phishing) with hypothesis-driven methodology and MITRE ATT&CK.
- Created detection rules on CrowdStrike Falcon, Splunk (SPL), Sysmon, Wazuh and Trend Micro.

- Automated hunting workflows with Python and PowerShell, reducing manual triage by 60%.
- Wrote playbooks, runbooks and the LogScale reference documentation used by SOC teams.

Cyber Security Analyst, CSIRT **04/2020 - 07/2023**

Vivo (Telefônica Brasil), São Paulo, Brazil

- Investigated and contained ransomware, APT, targeted phishing and web attacks (SQL injection, XSS, CSRF).
- Analyzed malware and network traffic to extract indicators of compromise (IOCs); monitored AV, EDR and SIEM.
- Investigated servers and VPN access and produced technical incident reports.

Network Analyst **09/2019 - 01/2020**

Logicalis (Banco Santander account), São Paulo, Brazil

- Cisco equipment configuration and LAN, WAN and wireless troubleshooting in a banking environment.

Network Infrastructure Analyst **06/2019 - 09/2019**

Central IT (São Paulo Municipal Department of Education), São Paulo, Brazil

- Operated 10,000 switches and 8,000 access points across 1,500 schools; SonicWall and pfSense firewalls; Zabbix monitoring.

Network Analyst (Intern) **03/2017 - 02/2019**

NIC.br, IX.br project, São Paulo, Brazil

- BGP configuration in a multi-vendor environment (Cisco, Brocade, Extreme, Huawei) at IX.br, Brazil's internet exchange point; LACP and bilateral VLANs.

Online Game Server Administrator & Reverse Engineer (self-employed) **01/2009 - 01/2014**

Break GunZ, online game server, São Paulo, Brazil

- Built and administered online game servers on Linux and Windows VPS with SQL Server databases.
- Developed an anti-cheat system and anti-debug and anti-tamper protections for 64-bit Windows binaries, with DLLs in C++ and Assembly.
- Reverse engineered client and server binaries (OllyDbg, Immunity Debugger, Process Hacker) to find and close the flaws cheaters exploited.
- Protected the web layer with WAF and DDoS mitigation on Cloudflare plus anti-SQL injection scripts in PHP.

PROJECTS

- **knowledge-rag** (creator and maintainer), github.com/lyonzin/knowledge-rag: 100% local RAG MCP server for AI agents, with hybrid search (BM25, semantic and RRF), cross-encoder reranking and 20 file formats. 300+ stars, 49 forks, 28K+ downloads on PyPI and npm, CI with 35+ checks across 9 OS and Python combinations.
- **LogonHoursRobot** (private repository): fully automated PowerShell robot that applies and audits logon-hour restrictions across multiple Active Directory domains, with delta processing, byte-level verification, SHA-256 forensic evidence, an HTML dashboard and granular rollback; paginated LDAP tested with 23K+ users.
- **X-SHELL** (private repository): red team framework for authorized operations, with reverse shell session management, artifact signing and MCP automation with AI agents (Claude Code, OpenAI and Cursor).

CERTIFICATIONS

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

PRACTICAL LABS: HACK THE BOX PRO LABS

RastaLabs, red team in Active Directory with defense evasion 11/2026
Zephyr, multi-domain Active Directory, relay, trusts and pivoting | HTBCERT-D6337FFDC3 04/2026
Puppet, C2 operations, Active Directory and DevOps | HTBCERT-86470B4B5B 02/2026
Dante, corporate network pentest with pivoting | HTBCERT-AAB49A3E31 12/2025

ADDITIONAL TRAINING

Detection, forensics and response
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, no date

Offensive security
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

AI and networking
Formação em Inteligência Artificial | branas.io 2026
IPv6 | NIC.br 2018
CCNA (course) | no date

EDUCATION

Postgraduate, Applied AI Engineering | UNIPDS | in progress 2026
Postgraduate, Cyber Security | Instituto Daryus 2019 - 2021
Computer Networks (Technologist) | Faculdade Impacta 2016 - 2018

LANGUAGES

Portuguese: native. English: basic.