FELIPE GASPARINO

CYBERSECURITY | SOC | DETECTION ENGINEERING

São Paulo, SP | LinkedIn | Portfolio | GitHub: Gaspa04

PROFESSIONAL SUMMARY

Final-semester Computer Science student at Universidade Presbiteriana Mackenzie, Co-founder of Kairon Systems, and IT Infrastructure Intern at CHS Brazil. Hands-on experience in infrastructure, networking, secure software development, and security operations, supported by practical SOC, SIEM, Detection Engineering, Threat Hunting, and MITRE ATT&CK lab work. Seeking opportunities as a SOC Analyst, Cybersecurity Analyst, Junior Detection Engineer, or Junior Security Engineer.

CORE SKILLS

SOC / Detection Engineering: Wazuh SIEM, Sysmon, Windows Event Logs, Threat Hunting, detection rule creation and validation, log analysis, event correlation, alert investigation, and SIEM/EDR fundamentals.
Frameworks & AppSec: MITRE ATT&CK, OWASP Top 10, authentication, authorization, RBAC, access control, security headers, CORS, and vulnerability assessment.
Infrastructure / Networking: Linux, Windows, VMware, Docker, TCP/IP, DNS, DHCP, VPN, VLAN, ServiceNow/CMDB, SolarWinds Orion, Palo Alto, Fortinet, Wireshark, and tcpdump.
Scripting / Development: PowerShell, Python, TypeScript, JavaScript, Node.js, React/Next.js, REST APIs, Git/GitHub, Cloudflare, and automation.

PROFESSIONAL EXPERIENCE

CHS Brazil | IT Infrastructure Intern (Oct 2024 - Present)
- Support corporate infrastructure, ITSM, and security operations, including event analysis and environment availability.
- Manage assets and configuration items with ServiceNow and CMDB; monitor infrastructure using SolarWinds Orion.
- Support Palo Alto, Fortinet, switching, routing, and VPN environments, as well as Disaster Recovery and connectivity projects.
- Develop tools and automations for IT operations and produce technical documentation in Azure DevOps and Microsoft Planner.

Kairon Systems | Co-founder / Full Stack Developer (Mar 2026 - Present)
- Develop applications, REST APIs, integrations, and automations using TypeScript, React/Next.js, Node.js, and Python.
- Implement authentication, authorization, RBAC, and secure development practices; deploy Linux/VPS environments using Docker, Cloudflare, Git, and GitHub.
- Integrate LLMs, AI agents, and RAG into business solutions.

CYBERSECURITY PROJECT - SOC / DETECTION ENGINEERING

Wazuh CyberLab | *Wazuh • Sysmon • MITRE ATT&CK • PowerShell • Linux • VMware*
- Built a hands-on SOC/SIEM lab with Wazuh and Sysmon to monitor and analyze security events from Windows endpoints.
- Created and validated custom detection rules for suspicious behaviors, applying log analysis, tuning, and false-positive testing.
- Performed threat hunting and alert investigation by correlating process, user, hash, and command context with the MITRE ATT&CK framework.
- Documented the architecture, rules, tests, and technical evidence on GitHub, structuring the project for expansion with additional detections.

EDUCATION, CERTIFICATIONS & LANGUAGES

Universidade Presbiteriana Mackenzie - B.S. in Computer Science (Expected graduation: 2026)
Certifications: Harvard CS50x • Microsoft Cybersecurity Education Program • Fortinet NSE 1, 2 & 3 • Ekahau Wi-Fi Survey • OWLK IAM Tech Day
Languages: Portuguese (Native) • English (Fluent) • Spanish (Basic)