FELIPE GASPARINO

CYBERSECURITY | SOC | DETECTION ENGINEERING | INFRASTRUCTURE SECURITY

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

PROFESSIONAL SUMMARY

Final-semester Computer Science student at Mackenzie, Co-founder of Kairon Systems, IT Infrastructure Intern at CHS Brazil and Cybersecurity Freelancer at Uspery. Hands-on experience in infrastructure, networking and security operations, including Wazuh/SIEM, log analysis, monitoring, tuning, alert investigation and MITRE ATT&CK.

CORE SKILLS

SOC / Detection Engineering: Wazuh SIEM, Sysmon, Windows Event Logs, Linux logs, Threat Hunting, 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 / Dev: 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)

- Corporate infrastructure, ITSM and security operations, including event analysis and environment availability.
- Asset and configuration management with ServiceNow/CMDB and infrastructure monitoring with SolarWinds Orion.
- Support for Palo Alto, Fortinet, switching, routing and VPN environments, plus Disaster Recovery and connectivity projects.
- Development of IT automation tools and technical documentation.

Uspery | Cybersecurity / Wazuh Freelancer (Aug/2026 - Present)

- Administration and continuous improvement of a production Wazuh environment receiving high-volume events from Windows and Linux endpoints.
- Mapping of agents and log sources, event investigation, authentication analysis, alert tuning and identification of noisy or security-relevant behavior.
- Structuring of monitoring, detection rules, dashboards, reports, metrics and risk prioritization.

Kairon Systems | Co-founder / Full Stack Developer (Mar/2026 - Present)

- Development of applications, REST APIs, integrations and automations with TypeScript, React/Next.js, Node.js and Python.
- Authentication, authorization, RBAC and secure development practices; Linux/VPS deployments with Docker, Cloudflare, Git and GitHub.
- Integration of 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 for monitoring and analyzing security events on Windows endpoints.
- Created and validated custom detection rules, applying log analysis, tuning and false-positive testing.
- Performed threat hunting and alert investigation, correlating processes, users, hashes and commands with MITRE ATT&CK.

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)