FELIPE GASPARINO

CIBERSEGURANÇA | SOC | DETECTION ENGINEERING | SEGURANÇA DE INFRAESTRUTURA

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

RESUMO PROFISSIONAL

Estudante do último semestre de Ciência da Computação no Mackenzie, Cofundador da Kairon Systems e Estagiário de Infraestrutura de TI na CHS Brasil. Experiência prática em infraestrutura, redes, desenvolvimento seguro e operações de segurança, com laboratório hands-on em SOC, SIEM, Detection Engineering, Threat Hunting e MITRE ATT&CK. Interesse em posições de Analista SOC, Analista de Cibersegurança, Detection Engineer Jr. e Security Engineer Jr.

COMPETÊNCIAS-CHAVE

SOC / Detection Engineering: Wazuh SIEM, Sysmon, Windows Event Logs, Threat Hunting, criação e validação de regras, análise de logs, correlação de eventos, investigação de alertas e fundamentos de SIEM/EDR.
Frameworks e AppSec: MITRE ATT&CK, OWASP Top 10, autenticação, autorização, RBAC, controle de acesso, Security Headers, CORS e avaliação de vulnerabilidades.
Infraestrutura / Redes: Linux, Windows, VMware, Docker, TCP/IP, DNS, DHCP, VPN, VLAN, ServiceNow/CMDB, SolarWinds Orion, Palo Alto, Fortinet, Wireshark e tcpdump.
Scripting / Dev: PowerShell, Python, TypeScript, JavaScript, Node.js, React/Next.js, REST APIs, Git/GitHub, Cloudflare e automações.

EXPERIÊNCIA PROFISSIONAL

CHS Brasil | Estagiário de Infraestrutura de TI (Out/2024 - Atual)

- Atuação em infraestrutura corporativa, ITSM e operações de segurança, com análise de eventos e disponibilidade de ambientes.
- Gerenciamento de ativos e itens de configuração com ServiceNow e CMDB; monitoramento de infraestrutura com SolarWinds Orion.
- Suporte a ambientes Palo Alto, Fortinet, switching, roteamento e VPN, além de projetos de Disaster Recovery e conectividade.
- Desenvolvimento de ferramentas e automações para operações de TI e documentação técnica em Azure DevOps e Microsoft Planner.

Kairon Systems | Cofundador / Desenvolvedor Full Stack (Mar/2026 - Atual)

- Desenvolvimento de aplicações, APIs REST, integrações e automações com TypeScript, React/Next.js, Node.js e Python.
- Implementação de autenticação, autorização, RBAC e práticas de desenvolvimento seguro; deploy de ambientes Linux/VPS com Docker, Cloudflare, Git e GitHub.
- Integração de LLMs, Agentes de IA e RAG em soluções empresariais.

PROJETO DE CIBERSEGURANÇA - SOC / DETECTION ENGINEERING

Wazuh CyberLab | *Wazuh • Sysmon • MITRE ATT&CK • PowerShell • Linux • VMware*

- Desenvolveu laboratório prático de SOC/SIEM com Wazuh e Sysmon para monitoramento e análise de eventos de segurança em endpoints Windows.
- Criou e validou regras customizadas de detecção para comportamentos suspeitos, aplicando análise de logs, tuning e testes de falsos positivos.
- Realizou threat hunting e investigação de alertas, correlacionando contexto de processos, usuários, hashes e comandos com o MITRE ATT&CK.
- Documentou arquitetura, regras, testes e evidências técnicas no GitHub, estruturando o projeto para expansão com novas detecções.

FORMAÇÃO, CERTIFICAÇÕES E IDIOMAS

Universidade Presbiteriana Mackenzie - Bacharelado em Ciência da Computação (conclusão prevista: 2026)
Certificações: Harvard CS50x • Microsoft Cybersecurity Education Program • Fortinet NSE 1, 2 e 3 • Ekahau Wi-Fi Survey • OWLK IAM Tech Day
Idiomas: Português (Nativo) • Inglês (Fluente) • Espanhol (Básico)