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, Estagiário de Infraestrutura de TI na CHS Brasil e Freelancer de Cibersegurança na Uspery. Experiência prática em infraestrutura, redes e operações de segurança, incluindo Wazuh/SIEM, análise de logs, monitoramento, tuning, investigação de alertas e MITRE ATT&CK.

COMPETÊNCIAS-CHAVE

SOC / Detection Engineering: Wazuh SIEM, Sysmon, Windows Event Logs, logs Linux, 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, incluindo análise de eventos e disponibilidade dos ambientes.
- Gestão de ativos e itens de configuração com ServiceNow/CMDB e monitoramento com SolarWinds Orion.
- Suporte a Palo Alto, Fortinet, switching, roteamento e VPN, além de projetos de Disaster Recovery e conectividade.
- Desenvolvimento de ferramentas de automação para operações de TI e documentação técnica.

Uspery | Freelancer de Cibersegurança / Wazuh (Ago/2026 - Atual)

- Administração e evolução de ambiente Wazuh em produção, com alto volume de eventos de endpoints Windows e Linux.
- Mapeamento de agentes e fontes de logs, investigação de eventos, análise de autenticações, tuning de alertas e identificação de ruído e comportamentos relevantes.
- Estruturação de monitoramento, regras de detecção, dashboards, relatórios, métricas e priorização de riscos.

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*

- Desenvolvimento de laboratório prático de SOC/SIEM com Wazuh e Sysmon para monitoramento e análise de eventos em endpoints Windows.
- Criação e validação de regras customizadas, com análise de logs, tuning e testes de falsos positivos.
- Threat hunting e investigação de alertas, correlacionando processos, usuários, hashes e comandos com MITRE ATT&CK.

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)