

Felipe Kauan Penna de Souza

Segurança da Informação | SOC · Resposta a Incidentes | DevSecOps

São Paulo – SP | pennasec@protonmail.com | linkedin.com/in/feepenna | github.com/feepenna

RESUMO PROFISSIONAL

Estagiário de Segurança da Informação em instituição financeira, atuando entre resposta a incidentes e DevSecOps, com 2 anos anteriores em suporte de TI e 3 como desenvolvedor backend. Tecnólogo em Análise e Desenvolvimento de Sistemas (UNIP) e estudante de Ciência da Computação (Impacta). No dia a dia, faço triagem, investigação e contenção de incidentes com SIEM, EDR e XDR (incluindo consultas KQL), frequentemente com prazo inferior a 24 horas. Em DevSecOps, faço análises SAST e DAST e automatizei a análise de segurança de novas aplicações com um agente de IA de threat modeling, reduzindo o tempo de parecer de cerca de 2 dias para cerca de 6 horas. Participei do saneamento da base de vulnerabilidades, com redução de cerca de 30% das vulnerabilidades ativas em um mês.

COMPETÊNCIAS TÉCNICAS

- **Monitoramento (SOC):** SIEM, EDR/XDR, Microsoft Defender XDR, Microsoft Sentinel, CrowdStrike Falcon, KQL, triagem de alertas
- **Resposta a Incidentes:** análise de logs, identificação de IOCs, contenção, MITRE ATT&CK
- **Gestão de Vulnerabilidades:** Qualys, priorização por risco, validação de correções, redução de falsos positivos
- **AppSec / DevSecOps:** SAST e DAST (Veracode, SonarQube), threat modeling (STRIDE, MITRE ATT&CK), JWT, OAuth 2.0
- **Zero Trust, Identidade e DLP:** ZTNA (Zscaler), regras de acesso por aplicação, DLP, Microsoft Entra ID, MFA, PAM (CyberArk)
- **Automação e IA:** Python, Bash, n8n, Power Automate, APIs REST, webhooks, Microsoft Foundry (agentes de IA)
- **Desenvolvimento, Infra e Redes:** Python, Django/DRF, Node.js, PostgreSQL, Git, CI/CD, Docker, Kubernetes, OpenShift, Linux, Windows Server, TCP/IP, DNS, DHCP
- **Frameworks e Conscientização:** ISO 27001, NIST CSF, CIS Controls, LGPD, simulação de phishing

EXPERIÊNCIA PROFISSIONAL

Estagiário de Segurança da Informação — Banco Toyota do Brasil | São Paulo – SP | Mar/2026 – Atual

- Triagem, investigação e contenção de incidentes de segurança com SIEM, EDR e XDR, frequentemente com prazo inferior a 24 horas.
- Automação da análise de segurança de novas aplicações com agente de IA de threat modeling (STRIDE e MITRE ATT&CK) e revisão humana obrigatória: tempo de parecer reduzido de cerca de 2 dias para cerca de 6 horas.
- Saneamento da base de vulnerabilidades (ativos duplicados, patches mal aplicados, falsos positivos não detectados), com redução de cerca de 30% das vulnerabilidades ativas em um mês.
- Análises SAST e DAST de aplicações internas, apoiando os times de desenvolvimento na correção.
- Apoio à adoção de Zero Trust (ZTNA): criação e ajuste de regras de acesso por aplicação e de políticas de DLP relacionadas ao uso de IA.
- Automação de rotinas de segurança com Python, n8n e Power Automate, e criação de agentes de IA para segurança.

Desenvolvedor Backend — Freelance | São Paulo – SP | Mar/2023 – Fev/2026

- APIs REST e aplicações backend com Python, Django/DRF e Node.js para pequenas empresas em digitalização.
- Autenticação e autorização com JWT e OAuth 2.0; modelagem e otimização de bancos PostgreSQL.
- Containerização com Docker e Kubernetes e CI/CD com Git.

Assistente de Suporte de TI — M de Araujo Souza Ltda | São Paulo – SP | Jul/2022 – Out/2024

- Suporte técnico presencial e remoto, com abertura, tratamento e resolução de chamados.
- Suporte a sistemas operacionais, redes (DHCP e conectividade), controle de acesso e rotinas de segurança da informação.

PROJETOS

- **Homelab de Cibersegurança (Wazuh + Docker):** SIEM Wazuh em Fedora Server com Docker num notebook reaproveitado, para análise de logs, hardening e simulação de incidentes; documentado em artigo no dev.to e repositório no GitHub. Prática de resposta a incidentes no TryHackMe.
- **Laboratório de Segurança de Agentes de IA (Kotlin):** aplicação de teste para validar isolamento multi-tenant e enforcement obrigatório de políticas em infraestrutura de agentes.

CERTIFICAÇÕES

Concluídas: Cisco Junior Cybersecurity Analyst · Google SecOps Foundation · Cisco Introduction to Cybersecurity · IBSEC Fundamentos em Cibersegurança (2026)

Em preparação: Microsoft SC-200 (Security Operations Analyst) · CompTIA Security+ · Zscaler Certified Associate Administrator

FORMAÇÃO ACADÊMICA

Bacharelado em Ciência da Computação — Faculdade Impacta | Fev/2026 – Dez/2029 (em andamento)

Tecnólogo em Análise e Desenvolvimento de Sistemas — Universidade Paulista (UNIP) | Mar/2024 – Dez/2025 (concluído)

Ensino Médio Técnico em Informática — Senac São Paulo | Fev/2021 – Dez/2023

Idiomas: Português: nativo | Inglês: intermediário (B1, EF SET) | Espanhol: intermediário (conversação)