

Felipe Kauan Penna de Souza

Information Security | SOC · Incident Response | DevSecOps

São Paulo, Brazil | pennasec@protonmail.com | linkedin.com/in/feepenna | github.com/feepenna

PROFESSIONAL SUMMARY

Information Security Intern at a financial institution, working between incident response and DevSecOps, with 2 prior years in IT support and 3 as a backend developer. Associate degree in Systems Analysis and Development (UNIP) and Computer Science student (Impacta). Day to day, I triage, investigate and contain incidents using SIEM, EDR and XDR (including KQL queries), often under 24-hour deadlines. On the DevSecOps side, I run SAST and DAST analysis and automated security reviews of new applications with an AI threat-modeling agent, cutting assessment time from about 2 days to about 6 hours. I took part in a vulnerability base cleanup that cut active vulnerabilities by about 30% in one month.

TECHNICAL SKILLS

- **Monitoring (SOC):** SIEM, EDR/XDR, Microsoft Defender XDR, Microsoft Sentinel, CrowdStrike Falcon, KQL, alert triage
- **Incident Response:** log analysis, IOC identification, containment, MITRE ATT&CK
- **Vulnerability Management:** Qualys, risk-based prioritization, remediation validation, false-positive reduction
- **AppSec / DevSecOps:** SAST and DAST (Veracode, SonarQube), threat modeling (STRIDE, MITRE ATT&CK), JWT, OAuth 2.0
- **Zero Trust, Identity & DLP:** ZTNA (Zscaler), per-application access rules, DLP, Microsoft Entra ID, MFA, PAM (CyberArk)
- **Automation & AI:** Python, Bash, n8n, Power Automate, REST APIs, webhooks, Microsoft Foundry (AI agents)
- **Development, Infrastructure & Networking:** Python, Django/DRF, Node.js, PostgreSQL, Git, CI/CD, Docker, Kubernetes, OpenShift, Linux, Windows Server, TCP/IP, DNS, DHCP
- **Frameworks & Awareness:** ISO 27001, NIST CSF, CIS Controls, LGPD, phishing simulation

PROFESSIONAL EXPERIENCE

Information Security Intern — Banco Toyota do Brasil (financial institution) | São Paulo, Brazil | Mar 2026 – Present

- Triage, investigation and containment of security incidents using SIEM, EDR and XDR, often under 24-hour deadlines.
- Automated security reviews of new applications with an AI threat-modeling agent (STRIDE and MITRE ATT&CK) with mandatory human review: time to deliver a security assessment dropped from about 2 days to about 6 hours.
- Took part in a cleanup of the vulnerability base (duplicate assets, failed patches, undetected false positives) that cut active vulnerabilities by about 30% in one month.
- SAST and DAST analysis of internal applications, supporting development teams on remediation.
- Supported Zero Trust (ZTNA) adoption: created and tuned per-application access rules and DLP policies related to AI usage.
- Automated security routines with Python, n8n and Power Automate, and built AI agents for security.

Backend Developer — Freelance | São Paulo, Brazil | Mar 2023 – Feb 2026

- REST APIs and backend applications with Python, Django/DRF and Node.js for small businesses going digital.
- Authentication and authorization with JWT and OAuth 2.0; PostgreSQL data modeling and optimization.
- Containerization with Docker and Kubernetes, and CI/CD with Git.

IT Support Assistant — M de Araujo Souza Ltda | São Paulo, Brazil | Jul 2022 – Oct 2024

- On-site and remote technical support, opening, handling and resolving tickets.
- Support for operating systems, networking (DHCP and connectivity), access control and information security routines.

PROJECTS

- **Cybersecurity Home Lab (Wazuh + Docker):** Wazuh SIEM on Fedora Server with Docker on a repurposed laptop for log analysis, hardening and incident simulation; documented in a dev.to article and GitHub repository. Incident response practice on TryHackMe.
- **AI Agent Security Lab (Kotlin):** test application to validate multi-tenant isolation and mandatory policy enforcement in AI agent infrastructure.

CERTIFICATIONS

Completed: Cisco Junior Cybersecurity Analyst · Google SecOps Foundation · Cisco Introduction to Cybersecurity · IBSEC Cybersecurity Fundamentals (2026)

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

EDUCATION

B.Sc. in Computer Science — Faculdade Impacta | Feb 2026 – Dec 2029 (in progress)

Associate Degree in Systems Analysis and Development — Universidade Paulista (UNIP) | Mar 2024 – Dec 2025 (completed)

Technical High School Diploma in IT — Senac São Paulo | Feb 2021 – Dec 2023

Languages: Portuguese: native | English: intermediate (B1, EF SET) | Spanish: intermediate (conversational)