MATHEUS AUGUSTO VARELA TEIXEIRA

Engenheiro de Automação de Segurança | SecOps · DevSecOps · Engenharia de Detecção

Duque de Caxias, RJ — Brasil | (21) 98939-0637 (Ligação / WhatsApp) | ae_augusto33@proton.me

LinkedIn: linkedin.com/in/augustoae | GitHub: github.com/masterazul

RESUMO PROFISSIONAL

Engenheiro de Automação de Segurança (SecOps/DevSecOps) que resolve a dor da operação com código — do pipeline CI/CD (Shift Left, SAST/DAST/SCA, IaC, Kubernetes, Policy as Code) ao SOAR. Projetei e desenvolvi, em Rust (dockerizado, com APIs, filas e PostgreSQL), um SOAR interno que centraliza/correlaciona alertas e executa playbooks — cobrindo toda a operação de SOC: 40+ clientes e +10 mil alertas. Acoplei um pipeline de IA (embeddings, modelos locais, n8n) que reduziu em mais de 50% o tempo de triagem. Automatizo porque entendo o adversário (CTI: MITRE ATT&CK, OSINT) e a conformidade (GRC / ISO 27001).

COMPETÊNCIAS TÉCNICAS

Engenharia & Automação (SecOps): Python | Rust | Docker | Kubernetes | PostgreSQL | Filas | APIs | CI/CD | n8n | Selenium

DevSecOps & AppSec: Shift Left | SAST | DAST | SCA | IaC | Cloud Security | Policy as Code | Gestão de Segredos | Runtime Security

IA & Detecção: Embeddings | Modelos locais (LLM) | Triagem preditiva | SOAR & Playbooks | SIEM | MITRE ATT&CK | OSINT

Vulnerabilidades & GRC: Tenable.io | Nessus | Hardening | CIS Benchmark | ISO/IEC 27001

Projetos (open-source): keyrot — cofre de segredos em Rust (AES-256-GCM, rotação, audit log) | kostwatch — FinOps de Kubernetes (Prometheus) | github.com/masterazul

Idiomas: Português (nativo) | Inglês B2 (Upper Intermediate)

EXPERIÊNCIA PROFISSIONAL

Engenheiro de Automação de Segurança / DevSecOps

abr/2025 – Atual

Service IT Security

- **Desenvolvi e mantenho, em Rust (dockerizado, com APIs, filas e PostgreSQL), um SOAR interno** que centraliza e correlaciona alertas e executa playbooks de resposta — abrangendo toda a operação de SOC: 40+ clientes e +10 mil alertas.
- **Acoplei um pipeline de IA (embeddings, modelos locais e scripts próprios, via n8n)** para triagem preditiva, reduzindo em mais de 50% o tempo de triagem e liberando o time para investigação de maior valor.
- **Implementei segurança no pipeline CI/CD (Shift Left):** SAST/DAST/SCA, segurança de IaC e Cloud, hardening de containers e Kubernetes, gestão de segredos, Policy as Code e ISO/IEC 27001.

Analista de Threat Intelligence & Prevenção a Fraudes

jul/2024 – abr/2025 · 10 meses

Service IT Security

- **Conduzi análise de fraudes e de vazamentos de dados,** com monitoramento contínuo e forense digital em deep e dark web, fóruns e Telegram, via investigações OSINT proativas e sob demanda.
- **Produzi inteligência de ameaças (CTI)** com modus operandi, timeline de incidentes, Diamond Model, TTPs, MITRE ATT&CK e IoCs estruturados, identificando padrões de ataque.
- **Administrei SIEM e operei detecção com Machine Learning,** além de DRP e monitoramento de transações; automações em Python para correlação e relatórios (Jira, OTRS, GLPI).

Estágio em SOC — GRC / Compliance

jun/2023 – mar/2024 · 10 meses

Vortex Security

- **Atuei em Governança de TI e Policy Compliance,** com gestão de vulnerabilidades, gestão de patches e monitoramento SIEM e de ativos em ambientes de alta criticidade (Tenable.io/.sc, Nessus).
- **Elaborei relatórios de conformidade e estratégias de segurança,** convertendo dados de vulnerabilidades em indicadores de risco; hardening de servidores e bancos de dados.

CERTIFICAÇÕES & CURSOS

- **Tenable Cloud Security Administration (TSCA)** — Tenable
- **Nessus Engineer** — Tenable
- **From IT To Cyber** — Cecyber
- **Analista de Cybersegurança** — IBSEC

FORMAÇÃO ACADÊMICA

Tecnólogo em Defesa Cibernética e em Gestão de Segurança — **Centro Universitário UniDomBosco** *Concluído em 2024*