Gabriel Ferreira Andrade Cardoso

Email: gabriel448521@gmail.com
Telefone: (61) 99630-3066
LinkedIn: https://www.linkedin.com/in/gabriel-ferreira-5a6b55267/

Objetivo

Atuar em Segurança da Informação com foco em análise de vulnerabilidades, detecção de ameaças, automação e melhoria contínua da postura de segurança. Contribuir com investigações, fortalecimento de infraestrutura e entrega de soluções técnicas de alto impacto.

Experiência Profissional

Estagiário - Tribunal Regional Federal da 1ª Região (TRF1)

04/2024 - 04/2026

- Execução de testes de vulnerabilidade em ativos internos e externos, usando ferramentas automatizadas e validação manual baseada em análise de HTTP, lógica de aplicação e comportamento de serviços.
- Uso de ferramentas como OpenVAS, Tenable, Qualys e scripts de segurança (nmap, utilitários de rede e varredura).
- Automação de processos de gestão de vulnerabilidades com Python, integrando dados e otimizando ciclos de análise.
- Suporte a projetos de gestão de ativos e migração tecnológica, incluindo estudo da solução NetBox e criação de scripts de migração.
- Configuração de ambientes Linux, implantação de serviços e avaliação de ferramentas opensource para gestão de conhecimento.
- Colaboração em decisões técnicas com apresentações de resultados para comitês internos.

- Atuação em chamados N2 usando ESET Protect, ESET Inspect e Wazuh para análise, resposta e investigação de incidentes.
- Atividades de threat hunting, telemetria, análise preliminar de malwares e estudo de engenharia reversa.
- Montagem de relatórios e dashboards em PowerBI para apoiar decisões estratégicas.

Formação Acadêmica e certificações

Engenharia de Software – Uniceplac (Gama/DF)

Previsão de conclusão: 06/2026

CWSE https://hackviser.com/verify?id=HV-CWSE-ERVBWRB1

CAPT https://hackviser.com/verify?id=HV-CAPT-3AGJMNDM

Competências Técnicas

- Linux (administração, shell, troubleshooting)
- Segurança da Informação
- Testes de vulnerabilidade (manual e automatizado)
- HTTP, aplicações web e análise de comportamento
- Python simples aplicado à automação e segurança
- Threat Hunting e análise inicial de malwares
- Ferramentas: OpenVAS, Tenable, Qualys, Wazuh
- Padrões e frameworks: ISO 27001, CIS Controls
- PowerBI para análise e visualização de dados

Idiomas

- Inglês instrumental (leitura e compreensão de material técnico)

Informações Adicionais

- Forte interesse por especialização contínua em segurança ofensiva, análise e detecção de ameaças.
- Proatividade, aprendizado rápido e experiência prática crescente em ambientes corporativos.
    - Disponibilidade para atuação presencial ou remota.