Pedro Carvalho

São Paulo, SP | (11) 9XXXX-XXXX | pedro.carvalho@42sp.org.br

Resumo Profissional

Profissional de Cibersegurança com mais de 7 anos de experiência em desenvolvimento e implementação de soluções de segurança robustas para ambientes corporativos complexos. Experiência comprovada em gerenciamento de riscos, análise de vulnerabilidades, resposta a incidentes e desenvolvimento de políticas de segurança. Habilidade comprovada em liderança de equipes, comunicação estratégica e gerenciamento de projetos, com foco em mitigação de riscos e proteção de ativos digitais. Especialista em tecnologias como SIEM, EDR, SOAR, Pentesting, análise forense e criptografia, com um histórico comprovado de sucesso na identificação e resolução de ameaças cibernéticas avançadas.

Experiência Profissional

SecureCorp - Especialista em Cibersegurança

Janeiro 2021 - Presente

- **Liderou o desenvolvimento e implementação de uma solução de SIEM personalizada, resultando em uma redução de 80% no tempo médio de detecção e resposta a incidentes.**
- **Desenvolveu e implementou um programa abrangente de awareness de segurança, reduzindo em 65% o número de incidentes relacionados a phishing e engenharia social.**
- **Realizou testes de penetração regulares, identificando e mitigando vulnerabilidades críticas em sistemas e aplicativos, garantindo a conformidade com os padrões de segurança da indústria.**

- **Responsável por gerenciar o processo de resposta a incidentes, incluindo análise forense, contenção e recuperação de sistemas comprometidos.**
- **Coordenou a implementação de políticas de segurança e treinamentos para funcionários, promovendo uma cultura de segurança proativa.**

DataProtect - Analista de Segurança da Informação

Julho 2018 - Dezembro 2020

- **Implementou e gerenciou uma solução de EDR, proporcionando detecção e resposta em tempo real a ameaças de endpoint, resultando em uma redução de 70% no tempo de resposta a incidentes.**
- **Realizou avaliações de vulnerabilidades em sistemas críticos, identificando e corrigindo falhas de segurança, garantindo a conformidade com normas de segurança como PCI DSS e ISO 27001.**
- **Desenvolveu e documentou procedimentos de segurança para diversas áreas da empresa, garantindo a padronização e o cumprimento das políticas de segurança.**
- **Participou ativamente de projetos de implementação de novas tecnologias, garantindo a segurança e a conformidade desde o início do ciclo de vida.**

Educação

Bacharelado em Ciência da Computação - Universidade de São Paulo

2015

- **Projeto de graduação: Sistema de detecção de intrusão baseado em aprendizado de máquina, utilizando técnicas de análise de comportamento e inteligência artificial.**
- **Especialização em Segurança da Informação - Pontifícia Universidade Católica de São Paulo.**

Habilidades Técnicas

- **Linguagens de programação:** Python, Go, PowerShell
- **Ferramentas de segurança:** SIEM (Splunk, Elastic Stack), EDR (CrowdStrike, Carbon Black), SOAR (Palo Alto Networks, Demisto), Nessus, Burp Suite, Metasploit
- **Protocolos de segurança:** TCP/IP, TLS/SSL, VPN, SSH, DNS
- **Análise forense:** EnCase, FTK, Wireshark
- **Criptografia:** AES, RSA, ECC
- **Cloud Security:** AWS, Azure, GCP

Projetos Relevantes

Sistema de Detecção de Ataques de Ransomware

- **Desenvolvido utilizando Python, Elasticsearch e Kibana, este sistema monitora o comportamento de arquivos e processos, detectando atividades suspeitas e alertando a equipe de segurança em tempo real.**
- **A solução foi capaz de detectar e bloquear 95% dos ataques de ransomware simulados durante os testes, reduzindo significativamente o risco de perda de dados e interrupção de negócios.**

Plataforma de Segurança para Aplicações Web

- **Desenvolveu uma plataforma de segurança para aplicações web utilizando frameworks como OWASP ZAP e Docker, com foco em automatizar testes de vulnerabilidades e fornecer relatórios detalhados.**
- **A plataforma reduziu em 70% o tempo necessário para realizar testes de segurança, permitindo que a equipe de desenvolvimento identificasse e corrigisse vulnerabilidades com mais rapidez e eficiência.**

Certificações e Formação Complementar

- **Certified Information Systems Security Professional (CISSP)** - ISC², 2020

- **Certified Ethical Hacker (CEH)** - EC-Council, 2019
- **CompTIA Security+** - CompTIA, 2018
- **Curso de Análise Forense Digital** - Instituto de Pesquisas Tecnológicas (IPT), 2017

Idiomas

- Português - Nativo
- Inglês - Fluente