

VALDÊNIO MARINHO

Analista de Cibersegurança

Ativamente envolvido na exploração de metodologias, frameworks, ferramentas e tendências. Realiza avaliações de vulnerabilidades para detectar e relatar problemas críticos, colaborando com equipes para desenvolver estratégias de segurança robustas. Comprometido em se manter atualizado com os últimos avanços em cibersegurança e ameaças emergentes, garantindo a entrega de soluções eficazes.

vm.jobhunt@pm.me 

+55 (83) 9 8214 63 41 

linkedin.com/in/0xrh0d4m1n 

Campina Grande, PB, Brasil 

@0xrh0d4m1n 

Experiência Profissional

Analista de Cibersegurança SOC

Nexusguard, Singapura

2024 - Atual

- Monitoro e analiso eventos de segurança em sistemas corporativos usando ferramentas SIEM para detectar, investigar e responder a possíveis ameaças.
- Colaboro com equipes de resposta a incidentes para mitigar riscos e conter incidentes de segurança de forma eficaz.
- Realizo análises detalhadas de alertas para identificar padrões indicativos de ameaças cibernéticas, aprimorando as capacidades de detecção e resposta.
- Gero relatórios detalhados e apresentações sobre descobertas de inteligência de ameaças, compartilhando insights acionáveis com stakeholders para fortalecer a postura de segurança organizacional.
- Utilizo as tecnologias proprietárias de mitigação de DDoS da Nexusguard para proteger as infraestruturas dos clientes contra ataques volumétricos, baseados em protocolo e de camada de aplicação.

Pesquisador de Cibersegurança

Plataformas de Testes de Segurança, Internacional

2023 - Atual

- Utilizou plataformas avançadas de testes de segurança para realizar avaliações abrangentes de vulnerabilidades, identificando falhas e fraquezas críticas de segurança.
- Analizou e relatou descobertas de ferramentas de identificação de vulnerabilidades para fornecer recomendações e insights acionáveis para aprimorar a segurança de sistemas.
- Colaborou com equipes multifuncionais para abordar vulnerabilidades identificadas, desenvolvendo e implementando estratégias eficazes de remediação.

Desenvolvedor Web Full-stack

Freelancer, Brasil

2018 - 2022

- Projetou e desenvolveu aplicações web escaláveis e de alto desempenho utilizando tecnologias como HTML, CSS, JavaScript, além de frameworks frontend e backend.
- Gerenciou o ciclo de vida do desenvolvimento de software, desde o planejamento inicial e design até a implantação e manutenção, garantindo a entrega dos projetos no prazo e dentro do orçamento.
- Integrava APIs e serviços de terceiros para aprimorar a funcionalidade e a experiência do usuário, mantendo altos padrões de qualidade e segurança de código.

Formação Acadêmica

Bacharelado de Tecnologia em Cibersegurança

Centro Universitário Cesumar, Brasil

2025

Bacharelado em Engenharia Elétrica

Universidade Federal de Campina Grande, Brasil

2018

Especialização Profissional em Cibersegurança da Fortinet

Instituto de Treinamento da Fortinet

2024

1. **Fortinet Certified Associate (FCA):** Treinamento abrangente em configuração e gerenciamento de firewalls FortiGate, incluindo criação de políticas, NAT, VPNs e inspeção de tráfego.
2. **Fortinet Certified Fundamentals (FCF):** Conceitos essenciais de cibersegurança, cobrindo protocolos básicos, configurações de firewall e gerenciamento seguro de rede usando produtos Fortinet.
3. **Network Security Associate 3 (NSE3):** Exploração detalhada dos produtos avançados da Fortinet, com foco em controle de aplicativos, segurança de endpoints e redes sem fio seguras.
4. **Network Security Associate 2 (NSE2):** Princípios essenciais de segurança para compreender o cenário de ameaças e as melhores práticas para mitigar riscos comuns de cibersegurança.
5. **Network Security Associate 1 (NSE1):** Introdução aos conceitos básicos de segurança de rede, cobrindo fundamentos de cibersegurança e o Fortinet Security Fabric.

Certificação Google Profissionalizante em Cibersegurança

Google, Especializações Profissionais - Coursera

2024

1. **Automação de Tarefas de Cibersegurança com Python:** Uso do Python para automação de tarefas em cibersegurança.
2. **Técnicas de Detecção e Resposta a Incidentes de Segurança:** Técnicas para detecção e resposta a incidentes de segurança.
3. **Gerenciamento de Ativos, Ameaças e Vulnerabilidades:** Gerenciamento de ativos críticos, ameaças e vulnerabilidades.
4. **Segurança em Linux e SQL:** Segurança para sistemas Linux e bancos de dados SQL.
5. **Fundamentos de Redes e Segurança de Redes:** Conceitos fundamentais de redes e segurança de redes.
6. **Gestão de Riscos de Segurança:** Estratégias para avaliação e mitigação de riscos de segurança.
7. **Fundamentos de Cibersegurança:** Conceitos e práticas centrais de cibersegurança.
8. **Preparação para Carreiras em Cibersegurança:** Orientação para preparação profissional e entrevistas.

Pentester

Cybrary, Certificações de Carreira

2023

1. **Certificação de Carreira em Teste de Penetração:** Introdução aos fundamentos de teste de penetração.
2. **Testes de Penetração Ofensivos:** Técnicas ofensivas para testes de segurança.
3. **Métodos Avançados de Teste de Penetração:** Métodos avançados para teste de penetração.
4. **Teste de Penetração:** Testes de penetração, metodologias e ferramentas.
5. **Framework MITRE ATT&CK para Simulações de Ataque:** Uso do framework MITRE ATT&CK para simulações de ataque.
6. **Cybersecurity Kill Chain:** Análise e defesa contra ciberataques.
7. **OWASP Top 10 2021:** As 10 principais vulnerabilidades de aplicações web.
8. **Habilidades de Analista SOC:** Competências para atuar em um Centro de Operações de Segurança (SOC).
9. **Administração de Sistemas para Segurança de TI:** Administração de sistemas para segurança de TI.
10. **CompTIA Security+:** Conceitos e práticas essenciais de segurança.
11. **CompTIA Linux+:** Habilidades de administração em Linux para cibersegurança.
12. **CompTIA A+:** Competências fundamentais de TI.

Cibersegurança & Hacking Ético

TCM Security, Bootcamps

2023

1. **Hacking Ético Prático:** Técnicas práticas de hacking ético.
2. **Segurança e Teste de Aplicações Web:** Avaliação e proteção de aplicações web.
3. **Teste e Segurança de APIs:** Teste e segurança de APIs.
4. **Estratégias para Testes de Penetração Externos:** Estratégias para testes de penetração externos.
5. **Movimentação, Pivoting e Persistência em Redes:** Técnicas para movimentação em uma rede.
6. **Escalação de Privilégios em Windows:** Escalação de privilégios em sistemas Windows.
7. **Escalação de Privilégios em Linux:** Escalação de privilégios em sistemas Linux.
8. **Curso Avançado de GRC (Governança, Riscos e Conformidade):** Habilidades em governança, riscos e conformidade (GRC).
9. **Inteligência de Fontes Abertas (OSINT):** Técnicas para coleta de informações de fontes públicas.

Competências

- Red Team Engagement
- Penetration Testing
- Vulnerability Assessment
- Malware Analysis
- Computer Security Incident Response Team (CSIRT)
- Security Operations Center (SOC)
- SOAR (EDR/XDR) & SIEM
- Cyber Threat Intelligence
- Information Security
- Governance, Risk and Compliance (GRC)

Outras Habilidades

Cibersegurança

- Penetration Testing Execution Standard (PTES)
- Cyber Kill Chain (Lockheed Martin)
- MITRE ATT&CK
- MITRE D3FEND
- NIST 800-53
- ISO 27001

Programação

- Python
- JavaScript
- Rust
- Shell Script
- Assembly
- SQL

Idiomas

- English
- Portuguese
- Spanish