Portfolio
Área de Informática

Apresentando meu portfólio de habilidades e experiências em Tecnológica da Informação (TI), com foco em Segurança Cibernética, Redes, Analise de vulnerabilities, Analise de dados, Desenvolvimento, Manutenção de Computadores, Etc.

por Joerbeth Serra Costa

Resumo Profissional

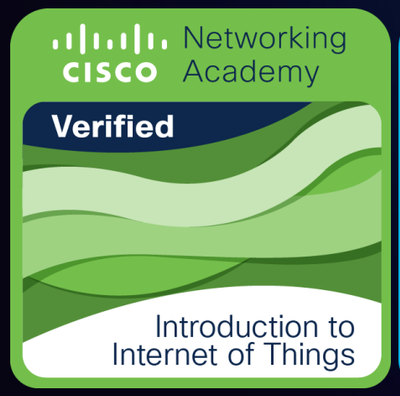
SOU UM PROFISSIONAL COM AMPLO CONHECIMENTO EM REDES, SEGURANÇA CIBERNÉTICA, PENTEST, BLUE TEAM, RED TEAM, COM CERTIFICAÇÕES DE FUNDAMENTOS PELA CISCO NETWORKING ACADEMY E OUTRAS INSTITUIÇÕE, COM EXPERIÊNCIA EM AMBIENTES DE N1 SOC, ANÁLISE DE VULNERABILIDADES , RESPOSTA A INCIDENTES , ANÁLISE DE DADOS, ENTRE OUTROS.

Atuação

ATUO COMO; ANALISTA DE SISTEMAS, ANALISTA DE REDES, TECNICO EM INFORMÁTICA, ANALISTA DE DADOS, DESENVOLVEDOR, ANALISTA DE PROJETOS, COORDENADOR DE TECNOLOGIA DA INFORMAÇÃO, ESPECIALISTA EM CYBERSECURITY, ANÁLISTA DE DADOS, MIGRAÇÃO DE DADOS, POWER BI...

Contatos

Certificados de Fundamentos Cisco Networking Academy



Certificados CertiProf

Certificados Aws

Certificados EC-Council/Hacker do Bem

Conhecimentos em Segurança
Segurança Cibernética

1 **Fundamentos de Segurança**

Compreensão dos princípios básicos de segurança cibernética, incluindo análise de riscos, políticas e procedimentos.

2 **Ataques Cibernéticos**

Familiaridade com técnicas de ataque, como phishing, malware e engenharia social.

3 **Vulnerabilidades de Software**

Conhecimento sobre diferentes tipos de vulnerabilidades e como explorá-las.

Experiência em Pentest / Red Team / Blue Team

Pentest

Experiência em testes de penetração, incluindo varredura de vulnerabilidades, exploração e relatório de descobertas.

Red Team

Participação em exercícios de Red Team, simulando ataques cibernéticos para avaliar a segurança de sistemas.

Blue Team

Experiência em defesa cibernética, incluindo monitoramento de sistemas, resposta a incidentes e mitigação de ataques para fortalecer a segurança da organização.

Purple Team

Atuação integrada entre Red Team e Blue Team, promovendo a colaboração para identificar lacunas de segurança, validar defesas e melhorar continuamente a postura de segurança.

Habilidades em Análise de Vulnerabilidades

Análise de Código

Habilidade em analisar código-fonte para identificar vulnerabilidades e falhas de segurança.

Ferramentas de Análise Análise

Domínio de ferramentas de análise de vulnerabilidades, como scanners de segurança e analisadores de código estático.

Metodologia de Análise

Conhecimento de metodologias de análise de vulnerabilidades, como OWASP e SANS.

Atuação em Ambientes de N1 SOC

Monitoramento de Segurança

Experiência em monitoramento de eventos de segurança, análise de logs e detecção de ameaças.

Resposta a Incidentes

Conhecimento de procedimentos de resposta a incidentes, incluindo contenção, remediação e recuperação.

Gestão de Incidentes

Habilidades em lidar com incidentes de segurança, investigar causas e implementar medidas corretivas.

Resposta a Incidentes de Segurança

1

Detecção

Identificação de eventos suspeitos e análise de logs para confirmar a ocorrência de um incidente.

2

Contensão

Medidas para impedir a propagação do incidente e proteger os sistemas afetados.

3

Investigação

Análise do incidente para determinar a causa, o impacto e a extensão do ataque.

4

Remediação

Implementação de medidas para corrigir as vulnerabilidades e restaurar a segurança dos sistemas.

5

Recuperação

Restauração dos sistemas afetados ao seu estado normal de operação.

Conhecimentos em CyberOps

1

Monitoramento de Segurança

Monitoramento contínuo de sistemas e redes para detectar atividades suspeitas.

2

Análise de Logs

Análise de registros de eventos de segurança para identificar padrões e anomalias.

3

Detecção de Ameaças

Utilização de ferramentas e técnicas de detecção de ameaças para identificar ataques em andamento.

4

Resposta a Incidentes

Implementação de ações para conter, investigar e remediar incidentes de segurança.