

Carlos Roberto da Silva

Brasileiro, solteiro
Rua Valéria, 308 – Bloco 02, apto 501
Fortaleza/CE

85 98956-9902 | E-mail: roberto.costati@outlook.com

FORMAÇÃO ACADÊMICA

- Graduação em Gestão de TI | Centro Universitário Estácio do Ceará;
- Pós-graduação em Ethical Hacking e CyberSecurity. UNICIV, conclusão em 2023.2 (Em andamento);

EXPERIÊNCIA PROFISSIONAL

- BNB – Banco do Nordeste do Brasil / Wipro Limited (2012 – 2022)

Cargo: Especialista em Segurança da Informação

Principais atividades: Gerenciamento e tratamento de incidentes via plataformas ARCHER e RSA – Netwitness (SOC/SIEM); Atendimento de solicitações via SDM (Service Desk Manager); Análise de mensagens suspeitas (Investigação e Tratamento); Submissão de artefatos maliciosos; Auditoria de grupos de segurança; Categorização/Recategorização de URLs via filtro web Blue Coat e Palo Alto; Monitoramento e controle de ameaças via SEP (Symantec Endpoint Protection); Monitoramento e controle de SPAMs via SMG (Symantec Messaging Gateway); Documentação de procedimentos operacionais, relatórios e atividades correlatas; Atividades de análise e tratamento de incidentes de segurança cibernética: Identificar risco de ataques cibernéticos a sistemas, ativos, dados e recursos utilizando soluções de antimalware, antispam, logs de SIEM, SOAR e comportamentos atípicos na rede corporativa.

- AUTOMATOS /Banco do Nordeste

Cargo: Técnico em Segurança da Informação (2006-2012)

Principais atividades: Análise e Tratamento de incidentes de Segurança cibernética, trabalhando desde a implantação do CSIRT (Grupo de Resposta a Incidentes de Segurança do Banco do Nordeste) em 2006, executando atividades técnicas e estratégicas até os dias atuais. Tratamentos de incidentes de segurança envolvendo malwares, análise de artefatos maliciosos na rede detectados através de alertas, relatórios e análise comportamental, análise e submissão de artefatos supostamente maliciosos às empresas de antimalware (Symantec, VirusTotal, Kaspersky...) para bloqueio ou remoção e alimentação de suas respectivas bases de dados a partir de eurísticas da ferramenta. Configurações de scans diários, semanais e mensais em todo o parque computacional da organização, Atuação em incidente de segurança na contenção do do malware DownAdUp, que fazia downgrade de privilégios administrativos de algumas contas do AD, geração de relatório de incidente, recomendações e correção da vulnerabilidade explorada pelo malware. Análise e sugestão de recategorização de sites por inadequação de categorização automática do produto;

Análise e sugestão de recategorização de sites por comportamento suspeito ou utilização para propagação de golpes cibernéticos;

Criação, edição e validação de processos e procedimentos de atividades do CSIRT relacionadas à Segurança cibernética; Análise e tratamento de golpes cibernéticos por e-mail (Spams, trojan Horses, phishings...);

Gerenciamento da solução Userlock/IS Decisions: Monitoramento de acessos simultâneos (Logins Simultâneos) e contas administrativas do Active Directory;

Análise de páginas falsas, tráfegos maliciosos, denúncias de abuse e solicitações de take down de páginas.

Gerenciamento, emissão e revogação de Certificados nas Autoridades Certificadoras internas do banco do Nordeste; Processo de aquisição Certificados Externos - ICP Brasil:

Elaboração de Infomails educativos periódicos e reports informativos sobre cibersegurança.

IDIOMAS

- Inglês – Intermediário

CURSOS

- CompTIA Security+ | HIVECORE Solutions
- Itil/Cobit Foundations | Disec/Automatos
- Forense Computacional | Axur Information Security
- Norma NBR/ISO/IEC 17799:2001 | Fundação Escola Politécnica da Bahia 16hr/a
- IT Security Specialist | Udemy
- Lei geral de Proteção de Dados Pessoais na Prática | Udemy
- Fórum Nacional de Internet Segura | Conpsys Security Systems
- ITSM - IT SERVICE MANAGEMENT | Udemy
- Mobile Security | Udemy
- Phishing | Udemy
- Gestão de Processos: Como implantar, conduzir e melhorá-los | Udemy
- Simpósio Latino Americano de Segurança Microsoft | Microsoft Ltda.
- Fundamentos, instalação, configuração, manutenção e gerenciamento da Console de Gerenciamento da ferramenta de antimalware e Filtro de Conteúdo Antispam – Symantec Manager Gateway – SMG Symantec
- Fundamentos, instalação, configuração, manutenção e gerenciamento da Ferramenta Data Loss Prevention (DLP)