Gustavo Jatene de Oliveira

CYBER SECURITY ANALYST

(71) 3039-1960 / (71) 99377-0038

jateneg@protonmail.com

https://www.linkedin.com/in/jateneg/

PERFIL PROFISSIONAL

Profissional de cyber segurança, CTF Player, curioso em buscar e aprender novas skills com enfoque em ataque e defesa de cyber ameaças. Com competências em desenvolvimento de automação com scripts python, mitigação de vulnerabilidades, hunting de ameaças, tratamento e resposta a incidentes, e análise forense de evidências.

HABILIDADES

Ansible	Cyber Kill Chain
Pentest Web	Python
Linux	AWS
TCP/IP	NIST
OWASP	MITRE

IDIOMAS

Português

Inglês

CERTIFICAÇÕES

- Badge IBM Qradar SIEM
- Badge CISCO Introduction Cybersecurity
- Badge CISCO Cybersecurity Essentials
- EC-Council Certified Ethical Hacker
- EC-Council Certified Incident Handler
- HybridCloud Security. Virtualization-Agentless
- Kaspersky Industrial CyberSecurity

CURSOS

- AWS Partner: AWS: Cloud Practitioner Essentials
- Firewall Linux com IPTables
- Gestão de Redes Linux
- MITRE ATT&CK Defender
- Programação em Python
- Thycotic PAM
- Web Hacking na Prática

FORMAÇÃO ACADÊMICA

Bacharel em Sistemas de Informação

Faculdade UNINASSAU

Técnico em Redes de Computadores

Serviço Nacional de Aprendizagem Industrial

EXPERIÊNCIA PROFISSIONAL

ISH (01/12/2021)

Cargo: Threat Hunting Analyst
Atividades: Hunting/Operação do SIEM Qradar/Netwitness; Desenvolvimento de casos de uso baseados em TTPs e relatórios de ameaça; Criação de parsers customizados em RegEx; Criação e análise da matriz de visibilidade dos logs baseadas no MITRE; Criação de POCs para geração de inteligência; Análise de artefatos maliciosos; Participação na resposta a incidentes e criação de runbooks baseado no NIST 800-61; Auxílio na melhoria contínua dos procedimentos operacionais do SOC.

PartnerOne (02/06/2021 a 30/11/2021)

Cargo: Analista de Segurança da Informação.
Atividades: Implantação e Monitoramento de DLP, PROXY e E-MAIL SECURITY da ForcePoint Implantação de políticas de compliance com LGPD, Resposta e Tratamento a incidentes.

X-Testing (11/01/2021 à 07/06/2021)

Cargo: Analista de Segurança da Informação.
Atividades: Implementação do IBM QRadar SIEM, IBM Security Secret Server e IBM Security Privilege Manager; Criação, validação e tunning de regras; Identificação e correlação de incidentes de segurança; Elaboração de relatórios gerenciais e técnicos; Documentação de Runbook para casos de uso.

Minas Pneus (01/09/2020 à 08/01/2021)

Cargo: Assistente de T.I

USE Telecom (02/04/2018 à 11/03/2020)

Cargo: Analista de suporte Jr.
Atividades: Gerenciamento do AD; Gestão e Monitoramento do VMWare; Monitoramento da rede com o LibreNMS; Gerenciamento de servidores Linux [Apache, NGINX]; Gerenciamento do CISCO ASA; Gerenciamento seguro de DNS com a CloudFlare; Criação de documentação para processos; Help Desk/ Service Desk.