TULIO CRUVINEL GOMES

Piracicaba, SP • (19) 995-777-123 • tulio.c.gomes@gmail.com
Linkedin – Github - Blog

OBJETIVO

Trabalhar o mais próximo das ameaças, seja antecipando-as ao realizar um Threat Hunting antes que o incidente se conclua ou trazendo inteligência aos sensores de detecção ao mapear seu comportamento. Meu objetivo é no futuro poder trabalhar como pesquisador na área de ameaças, porém tenho interesse em Ethical Hacking, Pentest e estou tendo o primeiro contato com análise de malwares e engenharia reversa para aumentar meu leque de análise. Metódico, dedicado, ético, resiliente e sempre exercitando o aprendizado contínuo. Possuo uma excelente comunicação, com foco em relatórios técnicos. Eu também possuo:

- Experiência em traduzir informações de cunho técnico para a terminologia de gerência/usuários.
- Experiência em programação de scripts utilizando Python e Bash.
- Experiência com RegEx.
- Experiência em administração de serviços em ambiente Linux/Windows/Containers.
- Experiência em infraestrutura de redes.
- Inglês Intermediário, com grande ênfase em leitura técnica e acadêmica.
- Estudo de machine learning aplicados a problemas na área de segurança.
- Estudo de conjuntos de ferramentas de segurança como Kali Linux, Metasploit e Burp Suite para aplicar em CTF, HTB, THM e VulnHub.
- Iniciando o estudo das linguagens Go e Assembly.
- Iniciando os estudos em análise de malware.

EDUCAÇÃO

DARYUS – Pós-Graduação Cyber Threat Intelligence (2022-2022)

- Início das Atividades em Fev/2022

FATEC Americana – Tecnólogo em Segurança da Informação (2017-2020)

- Iniciação Científica: Machine Learning aplicado a Esteganálise.
- Monografia: Aprendizado de Máquina na detecção de Tráfego de Botnet

CERTIFICAÇÕES

- Fortinet – Network Security Associate (NSE1)
- ICSI – Cietified Network Security Specialist (CNSS)
- Linuxtips – Uncomplicating Docker
- Oracle - OCI Foundations 2021
- Desec – Novo Pentest Profissional
- Desec Security – DCPT (Em progresso)

EXPERIÊNCIA

ISH, Piracicaba - SP — Out de 2021 até o presente

Cyber Defense Analyst – Threat Hunting

- Operação do SIEM Arcsight.
- Instalação de sensores para coleta de logs.
- Criação de parsers customizados (RegEx) utilizando conforme necessidade do cliente.
- Criação de ferramentas que integram a inteligência do fabricante ao SIEM.
- Conteinerização de ferramentas que integram ao SIEM.
- Análise de visibilidade dos logs e sugestão de novas fontes (Windows/Linux/WAF).
- Análise de logs de várias fontes (Windows/Linux/Firewall/WAF/etc).
- Criação de cenários de ataques para testes de regras.
- Criação de regras e correlação de logs no SIEM.
- Auxílio na melhoria contínua dos procedimentos operacionais do SOC.

Securityfirst, Piracicaba - SP Mai de 2021 até Out de 2021
Cyber Security Analyst

- Operação do SIEM Wazuh Stack.
- Monitoração de logs e eventos de segurança, análise e triagem de incidentes.
- Analisar, criar e sintonizar alertas gerados pelo SIEM Wazuh, IPS ou Firewall.
- Criação de regras e correlação de logs no SIEM.
- Gerenciamento de Vulnerabilidades.
- Contato com clientes no processo de investigação e resposta a incidentes.
- Auxílio na melhoria contínua dos procedimentos operacionais do SOC.

FATEC Piracicaba, Piracicaba - SP Fev de 2017 até Mai de 2021
Auxiliar de Docente de TI

- Responsável pela manutenção e gestão dos computadores da instituição.
- Criação de Políticas e normas para o departamento de TI utilizando COBIT/NIST/ISO.
- Gerenciamento dos serviços de rede, como: AD, CUPS, Squid, OpenBiblio e Firewall (PfSense).
- Manutenção dos servidores e gerenciamento de scripts ativos.
- Suporte Técnico aos discentes, docentes e funcionários.
- Treinamento e supervisão de estagiários, incentivando projetos para implementação na instituição.

Biocapital Participações S.A, Charqueada - SP Jan de 2013 até Dez de 2016
PJ - Assistente de TI

- Administração de usuários/grupos no AD.
- Administração de contas de e-mail Exchange 2010.
- Gerenciamento de servidor proxy (Linux-BRMA/OMNE).
- Configuração de servidor Windows Server 2012 (AD/FileServer).
- Implementação do ERP Ti9.
- Suporte aos usuários/equipamentos e consultoria para adesão de novas tecnologias.

FUMEP, Piracicaba - SP Jan de 2010 até Out de 2011
Estagiário de TI

- Gestão nos laboratórios de informática e manutenção de computadores.
- Atendimento a alunos e professores da instituição.
- Treinamento de novos estagiários de acordo com as políticas de TI.

CURSOS E EVENTOS

- Cisco – Cybersecurity Essentials
- Cisco – Introduction to Networks (CCNA R&S)
- FATEC Americana - Iniciação Científica 2019/2020 - "Machine Learning aplicado a Esteganálise"
- Beco do Exploit – Desafio 2 “Hackear 30 máquinas em 30 dias”
- Uniciv – 1º Bootcamp de Ethical Hacking
- FIAP Nano Courses – DevOps & Agile Culture
- DESEC – Novo Pentest Profissional
- AttackIQ – Foundations: Purple Team, Breach & Attack Simulation, MITRE ATT&CK

CTFS

Esses são os que tenho jogado ultimamente, mais detalhes sobre os desafios estão no meu blog https://0xNymerio.github.io .

- HacktheBox
- TryHackMe
- Root-me.org
- OverTheWire
- CryptoHack

INFORMAÇÕES ADICIONAIS

- Disponível para trabalho remoto.
- Horários flexíveis.