

Lucas Souza

<https://www.linkedin.com/in/olucassouza/> | <https://lucassouza.io>

Tecnologia da Informação | Cibersegurança | Red Team

Resumo Profissional

Profissional com mais de 10 anos de experiência em TI, atuando nos últimos anos em Cibersegurança e Infraestrutura, com foco na identificação e exploração de vulnerabilidades, análise de riscos cibernéticos e avaliação da resiliência de aplicações e infraestruturas corporativas. Domínio de frameworks como PTES, MITRE ATT&CK, OWASP, NIST CSF, CIS Control e Cyber Kill Chain em execução de projetos de testes de intrusão, engenharia de ataques e modelagem de ameaças.

Experiência Profissional

Under Protection – Curitiba/PR

Analista Sênior em Cibersegurança | 2021 – 2025

Segmento / Projetos que Atuei:

- Atuação em uma empresa do segmento de Segurança da Informação, realizando testes de intrusão, mapeamento e análise de riscos em aplicações (Web, APIs, Mobile), redes internas e externas.
- Execução de exercícios de Red Team para simulação de ataques direcionados em projetos para empresas do core Financeiro, e-commerce, Agronegócio, Multimídia, Saúde, Telecomunicação, entre outros.

Metodologia de Trabalho:

- Modelagem de cadeias de exploração e pivotagem.
- Elaboração de relatórios técnicos com evidências, criticidade e recomendações práticas.
- Validação técnica de vulnerabilidades e análise de impacto.
- Apoio à equipe de defesa (Blue Team) na correção de falhas.

Composição de Time:

- Integrante da equipe de segurança ofensiva (Red Team).
- Colaboração com equipes defensivas (Blue Team) e desenvolvimento.
- Atuação em projetos multidisciplinares de cibersegurança.

Tecnologias / Frameworks / Ferramentas:

- Burp Suite, Postman, Metasploit, Nmap, BloodHound, Mimikatz, Impacket, NetExec, Python, PowerShell, SQLmap, OWASP, NIST CSF, Cyber Kill Chain, Cis Controls.

Agropecuária Masutti – Vilhena/RO

Analista Sênior de Infraestrutura de TI | 2016 – 2021

Segmento / Projetos que Atuei:

- Atuei em uma empresa do Agronegócio realizando a administração e hardening de servidores Windows e Linux.
- Implementação de controles de segurança e segmentação de rede.
- Gerenciamento de operações de infraestrutura e monitoramento de segurança.

Metodologia de Trabalho:

- Adoção de boas práticas de segurança (CIS Controls).
- Implementação de políticas de segurança e melhoria contínua de processos.

Composição de Time:

- Integrante da equipe de infraestrutura de TI.
- Suporte a usuários e sistemas críticos.

Tecnologias / Frameworks / Ferramentas:

- Windows Server, Linux, Active Directory, Zabbix, Nagios, GLPI, Veeam Backup, VMware, Proxmox.

Formação Acadêmica

Pós-graduação em Computação Forense e Segurança da Informação – IPOG – 2022–2023

Graduação em Análise e Desenvolvimento de Sistemas – UNOPAR – 2018–2020

Técnico em Manutenção e Suporte em Informática – SENAI – 2014–2016

Certificações

C-APIPen – Certified API Pentester - The SecOps Group - 2025

eJPT – Junior Penetration Tester - INE Security - 2025

CRTA – Certified Red Team Analyst - CyberWarFare Labs - 2025

CNSP – Certified Network Security Practitioner - The SecOps Group - 2025

CRT-ID – Certified Red Team Infra Dev - CyberWarFare Labs - 2025

CRT-COI – Certified Red Team CredOps Infiltrator - CyberWarFare Labs - 2025

DCPT – Dsec Certified Penetration Tester - Dsec Security - 2022

Projetos e Pesquisas de Destaque

CVE-2020–29134 – Totvs Fluig Platform

Vulnerabilidade crítica, **Path Traversa (CWE-22)** em versões do sistema TOTVS Fluig.

- <https://nvd.nist.gov/vuln/detail/CVE-2020-29134>

ThreatTrack – Ferramenta de Consulta e Análise de Superfície de Ataque

Script em Python para análise de IPs e domínios, integrando dados da NVD, ExploitDB e GitHub.

- <https://github.com/Ls4ss/ThreatTrack>