

# Lucas Souza

São Paulo, SP | (11) 9XXXX-XXXX | lucas.souza@42sp.org.br

## Resumo Profissional

Especialista em Cibersegurança com 5 anos de experiência comprovada em desenvolvimento e implementação de soluções de segurança robustas para proteger infraestruturas críticas e dados sensíveis. Experiência abrangente em gerenciamento de riscos, testes de penetração, análise forense, resposta a incidentes e políticas de segurança. Profissional altamente motivado e orientado a resultados, com forte conhecimento técnico em ferramentas e tecnologias de segurança de última geração, incluindo SIEM, EDR, firewalls, VPNs e criptografia. Reconhecido por sua capacidade de identificar vulnerabilidades, implementar medidas preventivas e garantir a resiliência de sistemas e dados.

## Experiência Profissional

### CyberTech Solutions - Especialista em Cibersegurança

Janeiro 2021 - Presente

- Liderou o desenvolvimento e implementação de um sistema de detecção e resposta a incidentes (SIEM) que resultou em uma redução de 80% no tempo médio de resolução de incidentes de segurança, proporcionando uma resposta mais rápida e eficaz a ameaças cibernéticas.
- Realizou testes de penetração regulares em sistemas e aplicações da empresa, identificando e mitigando mais de 50 vulnerabilidades críticas, garantindo a segurança da infraestrutura e dos dados.

- Desenvolveu e implementou políticas de segurança robustas que alinham-se às melhores práticas do setor, garantindo o cumprimento de regulamentações como LGPD e GDPR.

## SecureNet - Analista de Segurança da Informação

Maio 2018 - Dezembro 2020

- Realizou análise forense de incidentes de segurança, identificando a causa raiz de ataques e tomando medidas para evitar sua recorrência, reduzindo o impacto de ataques em 70%.
- Implementou soluções de segurança de rede, incluindo firewalls e VPNs, para proteger a infraestrutura da empresa contra ameaças externas, garantindo a segurança de dados confidenciais e operações críticas.
- Colaborou na elaboração e implementação de planos de recuperação de desastres, garantindo a continuidade das operações em caso de incidentes críticos.

## Educação

---

### Bacharelado em Ciência da Computação - Universidade de São Paulo (USP)

2015 - 2019

- Projeto de graduação: "Análise de Vulnerabilidades em Sistemas de Controle Industrial" - pesquisa e desenvolvimento de um framework para detecção de vulnerabilidades em sistemas de controle industrial.
- Disciplinas relevantes: Segurança da Informação, Redes de Computadores, Criptografia, Análise de Riscos.

## Habilidades Técnicas

---

- **Gerenciamento de Riscos:** NIST Cybersecurity Framework, ISO 27001, OWASP Top 10.

- **Testes de Penetração:** Kali Linux, Metasploit, Burp Suite.
- **Análise Forense:** EnCase, FTK, Sleuth Kit.
- **Sistemas de Detecção e Resposta a Incidentes (SIEM):** Splunk, Elastic Stack, AlienVault OSSIM.
- **Gerenciamento de Pontos de Extremidade (EDR):** CrowdStrike, Carbon Black, SentinelOne.
- **Linguagens de Programação:** Python, Go, Bash.
- **Redes:** TCP/IP, Firewall, VPN, DNS, DHCP.

## Projetos Relevantes

---

### Sistema de Detecção de Ataques em Redes Industriais (SDARI)

- Desenvolvimento de um sistema de detecção de ataques em tempo real para redes industriais, utilizando técnicas de análise de tráfego de rede e aprendizado de máquina.
- O SDARI foi capaz de detectar com sucesso 95% dos ataques simulados em um ambiente de teste, demonstrando sua eficácia na proteção de infraestruturas críticas.

### Análise de Vulnerabilidades em Sistemas de IoT (Internet das Coisas)

- Realização de análise de vulnerabilidades em dispositivos IoT, incluindo análise de código, testes de penetração e análise de protocolos.
- Identificou e reportou mais de 30 vulnerabilidades críticas em dispositivos IoT, contribuindo para a segurança da Internet das Coisas.

## Certificações e Formação Complementar

---

- **Certified Information Systems Security Professional (CISSP)** - ISC<sup>2</sup>, 2020.
- **CompTIA Security+** - CompTIA, 2018.
- **Curso de Segurança em Redes Industriais** - ISA, 2019.

## Idiomas

---

- Português - Nativo
- Inglês - Fluente