# Lucas Martins Oliveira | Engenheiro de Segurança Cibernética | OSCP | Cloud Security

Av. Paulista, 1578, Bela Vista, São Paulo, SP, Brasil, 01310-200
+55 11 98765-4321 • lucas.oliveira@cybersec.dev • https://lucasoliveira.dev
@lucas-martins-oliveira • @lucas-moliveira

## Informações Básicas

- Engenheiro de segurança cibernética com mais de 8 anos de experiência em proteção de ambientes corporativos e cloud.
- Especialista em segurança ofensiva, resposta a incidentes e arquitetura de segurança em AWS e Azure.
- Certificado OSCP, CISSP e AWS Security Specialty, com forte atuação em conformidade (ISO 27001, LGPD, PCI DSS).
- Liderança técnica de equipes e implementação de programas de segurança desde a concepção até a operação.

## Formação

**Universidade de São Paulo** **https://www.usp.br**

*Bacharelado, Engenharia de Computação, Nota: 8.7/10* *mar. de 2014–dez. de 2018*

- Formação sólida em fundamentos de computação, redes e segurança da informação.
- Desenvolvimento de projetos práticos em segurança de aplicações e análise de vulnerabilidades.
- Participação em grupo de estudos de cibersegurança e competições de CTF.

**Cursos**: Segurança de Sistemas, Criptografia, Redes de Computadores, Sistemas Operacionais, Banco de Dados, Engenharia de Software, Computação em Nuvem, Inteligência Artificial

## Experiência Profissional

**Banco Digital Aurora** **https://www.bancaurora.com.br**

*Engenheiro de Segurança Cibernética Sênior* *jan. de 2022–Atual*

- Liderança técnica na definição de arquitetura de segurança para serviços em cloud (AWS e Azure).
- Implementação de programa de threat modeling e revisão de segurança de aplicações.
- Condução de resposta a incidentes críticos e análise forense.
- Desenvolvimento de automação de controles de segurança com Terraform e Python.
- Mentoria de engenheiros júniores e disseminação da cultura de segurança.

**Palavras-chave**: Threat Modeling, Cloud Security, SIEM, Incident Response, Terraform

**Consultoria RiskTech** **https://www.risktech.com.br**

*Engenheiro de Segurança da Informação* *fev. de 2019–dez. de 2021*

- Realização de testes de intrusão em aplicações web, APIs e infraestrutura.
- Avaliação de conformidade com ISO 27001, PCI DSS e LGPD.
- Implementação de soluções SIEM e correlação de eventos.
- Elaboração de relatórios técnicos e planos de remediação.
- Atuação em projetos de resposta a incidentes para clientes dos setores financeiro e saúde.

**Palavras-chave**: Penetration Testing, ISO 27001, SIEM, LGPD, Risk Assessment

**TechSecure Soluções** **https://www.techsecure.com.br**

*Estagiário de Segurança da Informação* *ago. de 2017–dez. de 2018*

- Monitoramento de alertas de segurança e triagem inicial de incidentes.
- Apoio na configuração de firewalls e sistemas de detecção de intrusão.
- Documentação de procedimentos operacionais de segurança.
- Participação em simulações de phishing e conscientização de usuários.

**Palavras-chave**: Firewalls, IDS/IPS, Phishing, Monitoring

## Idiomas

**Português**: Nativo ou Bilíngue

**Inglês**: Proficiência Profissional Fluente — **Palavras-chave**: TOEFL 105, Cambridge C1

**Espanhol**: Proficiência Profissional Limitada

## Competências

**Segurança Ofensiva**: Avançado — **Palavras-chave**: Penetration Testing, Metasploit, Burp Suite, OSCP, Nmap

**Segurança em Cloud**: Avançado — **Palavras-chave**: AWS Security, Azure Security, IAM, Terraform, Kubernetes Security

**Resposta a Incidentes**: Especialista — **Palavras-chave**: SIEM, Splunk, Forensics, SOAR, Threat Hunting

**Redes e Infraestrutura**: Avançado — **Palavras-chave**: Firewalls, VPN, IDS/IPS, TCP/IP, Zero Trust

**Governança e Conformidade**: Intermediário — **Palavras-chave**: ISO 27001, LGPD, NIST, PCI DSS, Risk Assessment

## Prêmios

**Profissional de Segurança do Ano**

*Banco Digital Aurora* — *nov. de 2023*

Reconhecimento pela liderança na implementação do programa de segurança em cloud e redução de 40% nos incidentes críticos.

## Certificados

**OSCP - Offensive Security Certified Professional** — **https://www.offsec.com/certifications/oscp/**

*Offensive Security* — *jun. de 2021*

**CISSP - Certified Information Systems Security Professional** — **https://www.isc2.org/certifications/cissp**

*ISC2* — *set. de 2022*

**AWS Certified Security - Specialty** — **https://aws.amazon.com/certification/certified-security-specialty/**

*Amazon Web Services* — *mar. de 2023*

**CompTIA Security+** — **https://www.comptia.org/certifications/security**

*CompTIA* — *fev. de 2020*

## Publicações

**Revista Brasileira de Segurança Cibernética** — **https://www.revistabsc.com.br/artigos/deteccao-intrusao-cloud-native**

*Detecção de Intrusão em Ambientes Cloud-Native* — *out. de 2023*

Artigo sobre abordagens de detecção de intrusão em ambientes de contêineres e Kubernetes, com foco em machine learning e correlação de eventos.

## Projetos

**ThreatIntel BR** — **https://github.com/lucas-moliveira/threatintel-br**

*Plataforma open-source para agregação e correlação de indicadores de ameaça.* — *jan. de 2023–dez. de 2023*

Desenvolvimento de plataforma para coleta de feeds de threat intelligence e correlação com eventos de segurança; integração com SIEM e geração de alertas contextualizados. **Palavras-chave**: Threat Intelligence, Python, SIEM, Open Source

**LogHunter** — **https://github.com/lucas-moliveira/loghunter**

*Ferramenta de análise forense de logs para ambientes Linux.* — *abr. de 2022–out. de 2022*

Criação de ferramenta em Python para análise de logs de autenticação e detecção de comportamentos anômalos; redução do tempo de triagem em 30%. **Palavras-chave**: Python, Forensics, Log Analysis, Linux

## Interesses

**Cibersegurança**: CTFs, Bug Bounty, Malware Analysis

**Esportes**: Corrida, Natação, Ciclismo

**Leitura**: Ficção Científica, Biografias

## Voluntariado

**OWASP São Paulo Chapter** **https://owasp.org/www-chapter-sao-paulo/**

*Mentor e Palestrante* *mar. de 2020–Atual*

- Atuação como mentor em programas de capacitação em segurança de aplicações.
- Palestras sobre OWASP Top 10 e boas práticas de desenvolvimento seguro.
- Organização de encontros técnicos e workshops para a comunidade.