Carlos Felipe Oliveira da Silva

Especialista em Infraestrutura & Segurança da Informação | SOC · SIEM · Cloud Security · DevSecOps

Rio de Janeiro, Brasil · cfelipe.oliveiradasilva@gmail.com · +55 21 98147-2823 · linkedin.com/in/cfelipe-oliveira

RESUMO PROFISSIONAL

Profissional de infraestrutura e segurança da informação com mais de 8 anos de experiência em ambientes corporativos críticos, on-premises e cloud (AWS, Azure, Oracle Cloud). Atuação consolidada em operações de segurança (SOC/SIEM com Wazuh, Suricata e CrowdSec), gestão de identidade (Active Directory, Microsoft Entra ID), automação de infraestrutura (Kubernetes, Terraform, Ansible) e conformidade com frameworks como ISO 27001, PCI-DSS, NIST e MITRE ATT&CK. Histórico de liderança técnica em projetos que reduziram significativamente esforço operacional manual através de automação, observabilidade e governança.

EXPERIÊNCIA PROFISSIONAL

Especialista em Infraestrutura & Segurança — **Open Labs SA** dez/2025 – atual · Rio de Janeiro (Híbrido)

- Liderança técnica em automação e sustentação de ambientes críticos, com estruturação de controles voltados a auditoria e compliance
- Gestão de clusters Kubernetes (Rancher, Helm) e infraestrutura como código com Terraform e Ansible
- Monitoramento de segurança e detecção de ameaças com Wazuh, OpenSearch, Suricata IDS e CrowdSec
- Desenvolvimento de middleware de automação de identidade (Node.js/TypeScript) para Active Directory, com testes automatizados e revisão de segurança alinhada a ISO 27001, PCI-DSS, NIST e MITRE ATT&CK
- Governança e catalogação do ecossistema Aurora Hub (86 projetos/serviços), com monitoramento de integridade em tempo real
- Integração de identidade via Active Directory, Entra ID e Microsoft Graph; redução significativa de atividades manuais

Analista de Infraestrutura, Cloud e Segurança — **Open Labs SA** fev/2025 – dez/2025

- Automação de processos operacionais com Python e PowerShell; padronização de ambientes e redução de incidentes
- Implementação de observabilidade e enriquecimento de eventos; integração com serviços de identidade e APIs Microsoft

Analista de Infraestrutura e Segurança — **Open Labs SA** ago/2021 – fev/2025

- SIEM e detecção de ameaças com Wazuh/OpenSearch, IDS Suricata e avaliação de vulnerabilidades (Greenbone/OpenVAS)
- Administração de segurança de rede (Fortigate, Cisco ASA) e ambientes VMware ESXi 7, com automação via PowerCLI
- Gestão de clusters Kubernetes (Rancher, Helm) e adoção de Terraform/Ansible como infraestrutura como código
- Implantação de clusters Docker Swarm em alta disponibilidade (redução de 90% no tempo de recuperação)
- Criação de pipelines de CI/CD (redução de 30% no tempo de deploy) e automação de rotinas (economia de 15h/semana)
- Integração de ambientes on-premises com cloud (Oracle Cloud Infrastructure e Azure); bancos PostgreSQL/MySQL com alta disponibilidade via Keepalived

Especialista em Suporte de TI — **B2W Digital** jan/2020 – mai/2021 · Rio de Janeiro

- Sustentação de sistemas críticos de e-commerce; suporte em ambientes cloud (AWS, GCP, UOL) e administração de microsserviços/APIs
- Automação de tarefas com redução de 50% no tempo de atendimento

Analista de Sistemas — **Prudential do Brasil** (Terceirizado) mar/2018 – jan/2020 · Rio de Janeiro

- NOC e suporte N1/N2 em infraestrutura e redes; administração de Active Directory e Office 365; suporte a telecom e servidores corporativos

Experiência anterior: TACCONE® (Analista de Desenvolvimento e Suporte, 2017–2018) · E2GO (Técnico de TI/NOC, 2015–2017) · Lan Designers (Técnico de TI/NOC, 2015) · Michelin (Auxiliar de Informática, 2012–2014) — suporte técnico N1/N2, NOC, Active Directory, Office 365 e infraestrutura de redes.

PROJETOS EM DESTAQUE

SIEM e Detecção de Ameaças (Wazuh, Suricata, CrowdSec, Greenbone/OpenVAS) jan/2026 – atual

Ecossistema unificado de SIEM com regras/decoders customizados, IDS de rede e avaliação contínua de vulnerabilidades, reforçado com CrowdSec para detecção de comportamento anômalo.

Middleware de Automação de Identidade (Node.js/TypeScript) jul/2026 – atual

API de automação de identidade para Active Directory multi-DC (desbloqueio de conta, reset de senha), com revisão de segurança ISO 27001/PCI-DSS/NIST/MITRE ATT&CK e ~68 testes automatizados.

Aurora Hub — Catálogo e Governança de 86 Projetos Corporativos ago/2026 – atual

Catálogo de governança para 86 projetos/serviços on-premises e cloud, com monitoramento de integridade em tempo real de serviços críticos.

Transformação de ITSM Corporativo com GLPI nov/2025 – mar/2026

Implantação de plataforma centralizada de ITSM com inventário automático de rede e padronização de workflows de atendimento.

Migração e Automação de Ambiente Microsoft 365 (SharePoint/Graph/Teams) nov/2025 – mar/2026

Migração e reestruturação de sites/bibliotecas SharePoint, automações via Microsoft Graph API e notificações via Teams.

COMPETÊNCIAS TÉCNICAS

Segurança & SOC	SIEM (Wazuh, OpenSearch), IDS/IPS (Suricata, CrowdSec), Firewalls (Fortigate, Cisco ASA, pfSense), Gestão de Vulnerabilidades (Greenbone/OpenVAS, Nmap, Metasploit, Burp Suite), ISO 27001, PCI-DSS, NIST, MITRE ATT&CK
Cloud & DevOps	AWS, Azure, Oracle Cloud (OCI), Kubernetes (Rancher/Helm), Docker/Swarm, Terraform, Ansible, Argo CD, GitLab CI/CD, Azure DevOps
Identidade	Active Directory, Microsoft Entra ID, Microsoft Graph, IAM
Infraestrutura & SO	Linux (RHEL, Oracle Linux, Ubuntu), Windows Server, VMware ESXi/PowerCLI, PostgreSQL, MySQL, Keepalived, NFS
Observabilidade	Grafana, Prometheus, Zabbix, Graylog, Centreon, Telegraf/InfluxDB
Automação & Dev	Node.js/TypeScript, Python, Go, PowerShell, Bash, Redis, GLPI

FORMAÇÃO ACADÊMICA

FIAP jun/2026 – jun/2027

Pós-graduação, Defensive Cyber Security (em andamento)

Estácio fev/2023 – jul/2025

Bacharelado, Gestão de Tecnologia da Informação e Gerenciamento de Projetos

Estácio fev/2012 – dez/2016

Bacharelado, Sistemas de Informação

CERTIFICAÇÕES

Fortinet Certified Associate (FCA) – Cybersecurity

Fortinet Certified Fundamentals (FCF) – Cybersecurity

ISO/IEC 27001 Information Security Associate – SkillFront

Remote Work Professional Certification (RWPC) – CertiProf

IDIOMAS

Português (nativo) · Inglês (básico)