Jorge Luis Sánchez Casanova

Especialista em Cibersegurança | SOC Nível 3 | Incident Response | DevSecOps

R. Hélio Dirceu Woitikiw, 40 - Pinheirinho, Curitiba - PR, 81870-350 | jorgeluis961224@gmail.com | +55 (41) 99228-0044

linkedin.com/in/jorgelsc-dev | github.com/jorgelsc-dev | jorgelsc.dev

Cargos-alvo: Cybersecurity Specialist, Especialista em Cibersegurança, Ciberseguridad, Analista de Segurança, Analista SOC, SOC Level 3, SOC Nível 3, Incident Response Analyst, Blue Team Analyst, DevSecOps Engineer, Cloud Security Engineer.

Resumo Profissional

Especialista em cibersegurança com mais de 6 anos de experiência em resposta a incidentes, operações SOC/CERT, SOC Nível 3, blue team, SIEM, hardening, infraestrutura crítica, cloud security e DevSecOps. Apoiou empresas afetadas por ransomware na contenção, recuperação e prevenção de recorrência, restabelecendo ambientes críticos em menos de 72 horas. Elevou em mais de 3 vezes a capacidade de detecção por meio de tuning de regras, correlação de eventos e melhorias em SIEM. Criou uma área de cibersegurança alinhada à ISO 27001 e atualmente integra segurança, cloud security e liderança técnica em ambientes AWS e Kubernetes.

10+ profissionais liderados | **5+ projetos simultâneos** | **AWS + Kubernetes + CI/CD** | **Recuperação em menos de 72 horas** | **Detecção de ameaças 3x maior**

Competências Técnicas

SOC e resposta a incidentes: triagem, contenção, erradicação, recuperação, ransomware, playbooks, incident response, incident management, coordenação de incidentes, blue team e proteção de infraestrutura crítica.

Detecção e monitoramento: SIEM, Elastic Stack, Elasticsearch, Suricata, IDS/IPS, network security monitoring, análise de tráfego, tuning de regras, correlação de eventos, threat hunting, investigação e redução de falsos positivos.

Segurança ofensiva e governança: vulnerability management, gestão de vulnerabilidades, testes de penetração, penetration testing, hardening, políticas, controles, gestão de riscos, risk management e práticas alinhadas à ISO 27001.

Cloud e DevSecOps: AWS, Kubernetes, Docker, Linux, IAM, WAF, CloudTrail, CloudWatch, cloud security, security automation, GitHub Actions e GitLab CI/CD.

Automação: Python, Bash, integração de ferramentas de segurança, APIs HTTP, WebSocket e PostgreSQL.

Experiência Profissional

Líder Técnico de Desenvolvimento e DevOps | Marox
abr 2025 - atual

- Lidera uma equipe multidisciplinar com mais de 10 profissionais e atuação em mais de 5 projetos, orientando arquitetura, revisão técnica, priorização, troubleshooting e resolução de incidentes.
- Projeta e opera infraestrutura para aplicações frontend e backend, bancos de dados e servidores web em AWS, Kubernetes, Docker, Linux, Nginx e PostgreSQL, com foco em confiabilidade e escalabilidade.
- Modernizou workloads baseados em EC2 para uma arquitetura conteinerizada e autoescalável, com balanceamento, health checks, monitoramento e alertas, reduzindo pontos únicos de falha e intervenção manual.
- Padronizou pipelines CI/CD e processos de deploy para criar ambientes reproduzíveis, melhorar a rastreabilidade das mudanças e fortalecer a continuidade operacional.

Consultor DevOps | DiangTech
2025

Contrato part-time, com escopo definido e concluído

- Conduziu a migração de repositórios e do fluxo de entrega para GitHub, estruturando automações e pipelines com GitHub Actions.
- Padronizou branches, rotinas de integração e documentação de operação, concluindo a transferência das funcionalidades previstas no contrato.

Líder de Cibersegurança | Avangenio S.R.L.
jul 2024 - jan 2025

- Criou a área de cibersegurança e definiu políticas, controles, responsabilidades, gestão de riscos e práticas alinhadas à ISO 27001.
- Conduziu auditorias técnicas, hardening, testes de penetração e priorização da correção de vulnerabilidades críticas, fortalecendo governança e postura defensiva.
- Capacitou mais de 80 colaboradores em cultura de segurança, prevenção de incidentes e boas práticas operacionais.

Experiência Profissional - Continuação

Especialista SOC Nível 3 e Instrutor | ETECSA **nov 2023 - mai 2024**

- Atuou em um SOC responsável por apoiar organizações afetadas por incidentes de alta criticidade em telecomunicações e serviços essenciais, com triagem, investigação, escalonamento e coordenação de resposta.
- Apoiou empresas atingidas por ransomware na contenção, recuperação operacional, análise de causa e prevenção de recorrência, restabelecendo ambientes críticos em menos de 72 horas.
- Elevou em mais de 3 vezes a capacidade de detecção por meio de tuning de regras, integração de fontes de dados e aprimoramento de casos de uso em SIEM.
- Formou especialistas em análise, resposta a incidentes e operação SOC, disseminando procedimentos para investigação e escalonamento.

Especialista em Cibersegurança | OSRI CuCERT **jan 2021 - nov 2023**

- Gerenciou e coordenou incidentes cibernéticos em colaboração com organismos nacionais e internacionais, estruturando comunicação, análise e resposta operacional.
- Implementou monitoramento para infraestruturas críticas com SIEM, IDS/IPS, Suricata, análise de tráfego, investigação de eventos e resposta operacional.
- Participou da proteção do evento G77 + China por meio de monitoramento preventivo, análise de ameaças, inteligência operacional e mitigação de incidentes.

Projetos Open Source

wsbuilder github.com/jorgelsc-dev/wsbuilder
Framework modular em Python para servidores HTTP e WebSocket, com ORM SQLite, cache, segurança, métricas, tarefas em background, DNS local e replicação. Projeto mantido com documentação, testes, versionamento e releases públicas.

PortHound github.com/jorgelsc-dev/porthound
Scanner de rede em Python para auditorias autorizadas, com TCP, UDP, ICMP e SCTP, banner grabbing, persistência SQLite, API HTTP/WebSocket e interface em Vue 3; distribuído publicamente como **porthound4**.

SniffHound github.com/jorgelsc-dev/sniffhound
Capturador e analisador de tráfego em Python nativo, com modos sniffer e honeypot, parsing de protocolos, autenticação, persistência SQLite, dashboard Vue 3 e eventos em tempo real via WebSocket.

Formação Acadêmica

Engenheiro em Ciências da Computação
Universidade de Ciências Informáticas (UCI), Cuba | 2017 - 2023

Tese de graduação aplicada à infraestrutura crítica nacional, avaliada com nota máxima (5/5). Tutor de duas teses de graduação, ambas avaliadas com nota máxima (5/5).

Certificações

- Forense Digital | QAX Qianxin, 2024
- Monitoramento de Redes Sem Fio | QAX Qianxin, 2024
- Governança e Gestão do Ciberespaço | AIBO / Ministério do Comércio da China, 2024
- ISO 9001 em Profundidade | Lloyd's Register, 2019

Idiomas

Espanhol: nativo | **Português:** básico, compreende e interage em situações simples | **Inglês:** básico