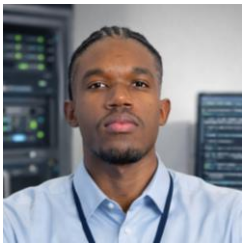
Cleison Máquina



TÉCNICO JÚNIOR DE CIBERSEGURANÇA

930 480 153 | cleisonmq@gmail.com | Portugal, Coimbra.

SOBRE MIM

Técnico Júnior de Cibersegurança com experiência prática em SIEM/SOC, vulnerability assessment e incident response. Em estágio na Universidade de Coimbra, realizei assessments em +120 servidores com metodologia CVSS e MITRE ATT&CK. Orientado para Blue Team e deteção de incidentes.

FORMAÇÃO ACADÉMICA

Técnico de Cibersegurança | INSTITUTO DO EMPREGO E FORMAÇÃO PROFISSIONAL (IEFP) 08/2025 - 08/2026

Administrador de Sistemas Informáticos e de Redes | MASTER D — Concluído com 84% (540h) 11/2024 - 12/2025

Hacking Ético & Pentest | UDEMY 11/2025 - 02/2026

Banco de Dados SQL | UDEMY 10/2025 - 12/2025

Desenvolvedor de Websites (Front-End) | CENTRO INTEGRADO DE FORMAÇÃO TECNOLÓGICA (CINFOTEC) 11/2022 - 12/2022

HABILIDADES

- **SIEM & SOC:** Wazuh, Splunk, Log Analysis, Security Monitoring, MITRE ATT&CK, CVSS.
- **Pentest & Forense:** Nmap, Hydra, Netcat, DIRB, Autopsy, FTK Imager, Burp Suite, WPScan, OWASP ZAP, SpiderFoot.
- **Sistemas:** Linux (Kali, Ubuntu) e Windows (10/server)
- **Programação & Web Dev:** Python, JavaScript, Html, CSS e Bootstrap.
- **Segurança:** Threat Detection, Vulnerability Management, Network Security, Access Control.

IDIOMAS

- Português (Nativo)
- Inglês (Intermédio)

REDES SOCIAIS

LinkedIn: https://www.linkedin.com/in/cleisonmq/

GitHub: https://github.com/cleisonmq

EXPERIÊNCIA PROFISSIONAL

Técnico de Cibersegurança (Estágio) | Universidade de Coimbra UC 04/2026 ⟶ Em curso

- Executei vulnerability assessments em +120 servidores académicos com metodologia CVSS, identificando vulnerabilidades críticas e produzindo relatórios de remediação que reduziram a superfície de ataque nos ambientes de desenvolvimento e produção.
- Produzi relatórios técnicos de segurança com mapeamento para o framework MITRE ATT&CK, comunicando riscos e planos de mitigação a equipas de desenvolvimento e operações.
- Realizei inventariação e descoberta ativa de ativos de rede — hosts, portas abertas, serviços em execução e certificados digitais, contribuindo para visibilidade completa da infraestrutura.
- Revi e melhorei políticas de segurança internas, criando documentação técnica estruturada em Markdown com boas práticas de hardening e mitigação de riscos.
- Conduzi análise forense de logs de um site comprometido, reconstruindo a linha temporal do ataque e documentando os indicadores de comprometimento (IOCs) num relatório técnico formal.

PROJETOS

Simulação de ambiente SOC com Wazuh

- Implementei infraestrutura SIEM com Wazuh em Ubuntu 22.04, integrando 6 agentes Linux/Windows para correlação de eventos em tempo real.
- Detetei e correlacionei +40 eventos de segurança (SSH brute force, port scanning, falhas de autenticação) com alertas configurados por severidade e mapeamento para MITRE ATT&CK.

Active Directory & Windows Server Security Lab

- Implementei AD DS com IAM, GPO e controlo de acessos em Windows Server, aplicando hardening, firewall e Microsoft Defender para redução da superfície de ataque.

CMEasy — Ferramenta CLI de Automação para Administração de Sistemas e Cibersegurança

- Desenvolvi ferramenta CLI em Python com suporte multi-distribuição (Linux/Windows) para automação de tarefas de administração de sistemas e segurança, reduzindo o tempo de execução manual em 70%.

Proxy Squid — Controlo e Monitorização de Tráfego de Rede

- Implementei servidor proxy Squid em Ubuntu 22.04 com ACL, autenticação de utilizadores, firewall (UFW) e IDS/IPS (Fail2Ban) para deteção e bloqueio automático de tráfego suspeito.