

Yasmin Teixeira de Freitas

Analista de Cibersegurança Pleno · Blue Team · SOC · Resposta a Incidentes · Proteção de Dados

São Paulo, SP · (11) 99425-8125 · yasminteixe@gmail.com · linkedin.com/in/freitas-yasmin · Portfólio: yfreitas.krowncode.tech

RESUMO PROFISSIONAL

Analista de Cibersegurança Pleno com **mais de 6 anos em segurança defensiva**, da operação de SOC à consultoria. Atuo de ponta a ponta no ciclo de detecção e resposta: monitoramento contínuo, engenharia de detecção no SIEM, threat hunting, investigação, contenção e documentação de incidentes em ambientes corporativos híbridos. Experiência sólida com **IBM QRadar**, **Trellix EDR**, firewalls multifabricante (FortiGate, VMware NSX, Hillstone, Cisco), WAF (F5, Imperva) e projetos de proteção de dados com **HSM, PAM, IAM e DLP**. Mais de 30 credenciais de fabricantes (Thales, Imperva, Trellix, Safetica), pós-graduanda em Cybersecurity pela FIAP e inglês fluente.

- Monitoramento SOC
- Resposta a incidentes
- Engenharia de detecção
- Threat hunting
- SIEM · EDR · NGFW · WAF
- Gestão de vulnerabilidades
- Proteção de dados e IAM
- Automação

EXPERIÊNCIA PROFISSIONAL

Neotel Segurança Digital

São Paulo, SP · Híbrido

- Analista de Cibersegurança Pleno · SOC / Blue Team

Jan/2024 – Atual

 - Responsável pelo ciclo completo de incidentes no SOC — detecção, triagem, investigação, contenção, erradicação e pós-incidente — em ambientes corporativos híbridos, seguindo o NIST SP 800-61.
 - Engenharia de detecção no **IBM QRadar**: criação e tuning de regras de correlação, casos de uso e dashboards mapeados ao **MITRE ATT&CK**, com redução contínua de falsos positivos.
 - Threat hunting orientado por hipóteses e inteligência de ameaças, com análise e bloqueio de IOCs no EDR, no firewall e no proxy.
 - Administração de firewalls **FortiGate 1800F**, **VMware NSX**, **Hillstone** e **Cisco Secure**, WAF F5, proxy Cisco e EDR **Trellix ePO**: políticas, revisão de regras, segmentação e resposta a ameaças.
 - Condução técnica de projetos de proteção de dados com **HSM, PAM, IAM e DLP**, da arquitetura à implantação e ao suporte.
 - Desenvolvimento de automações em Python e PowerShell integradas via API (QRadar, Trellix) para enriquecimento de alertas, coleta de evidências e monitoramento.
 - Elaboração de playbooks e de relatórios técnicos e executivos de incidentes; mentoria de analistas júnior.
- Analista de Cibersegurança Júnior · SOC

Jan/2021 – Dez/2023

 - Monitoramento de eventos de segurança no IBM QRadar, triagem de alertas em N1/N2, escalonamento e documentação de incidentes.
 - Análise de logs de firewall, proxy, EDR, Windows e Linux para investigar acessos suspeitos, malware e phishing.
 - Operação de firewalls, proxy e EDR: criação de regras, bloqueio de IOCs e tratamento de detecções.
 - Gestão de vulnerabilidades: varreduras, priorização por CVSS e acompanhamento das correções com os times responsáveis.
 - Monitoramento de disponibilidade com Zabbix e apoio à implantação de soluções Thales (HSM, CipherTrust, IAM) e Imperva (WAF, DDoS, DSF).

KrownCode

São Paulo, SP

Consultora de Cibersegurança

Fev/2023 – Atual

- Avaliações de postura de segurança e análise de riscos para clientes, com planos de remediação priorizados por impacto e criticidade.
- Hardening de servidores Linux e Windows, Active Directory e ambientes em nuvem com base em CIS Benchmarks e CIS Controls v8.
- Revisão de arquitetura de segurança: segmentação de rede, regras de firewall, WAF, MFA e gestão de acessos privilegiados.
- Estruturação de processos de resposta a incidentes, com playbooks e runbooks alinhados ao NIST e ao MITRE ATT&CK.
- Apoio à adequação à LGPD e à ISO/IEC 27001 (políticas, controles e evidências) e à segurança no ciclo de desenvolvimento (OWASP Top 10, SAST/DAST).

CET Companhia de Engenharia de Tráfego

São Paulo, SP

Estagiária de Cibersegurança

Jan/2020 – Dez/2020

- Apoio ao monitoramento de eventos de segurança e à análise de logs de servidores e estações de trabalho.
- Suporte à gestão de identidades e acessos no Active Directory e à aplicação de políticas de segurança.
- Inventário de ativos, verificação de patches e apoio à correção de vulnerabilidades.
- Suporte técnico a usuários, com orientação sobre phishing e boas práticas de segurança.

COMPETÊNCIAS TÉCNICAS

SIEM e detecção	IBM QRadar (AQL) · Splunk (SPL) · Microsoft Sentinel (KQL) · Wazuh · Elastic · regras de correlação e casos de uso · Sigma · tuning de falsos positivos
Threat hunting e CTI	MITRE ATT&CK · Cyber Kill Chain · Pyramid of Pain · IOCs e IOAs · MISP · VirusTotal · AbuseIPDB · Shodan · YARA
Resposta a incidentes e forense	NIST SP 800-61 · playbooks e runbooks · triagem de malware · análise de phishing e cabeçalhos de e-mail · Sysmon e Windows Event Logs · Velociraptor · KAPE · Volatility · cadeia de custódia
Endpoint (EDR/XDR)	Trellix ePO e EDR · Microsoft Defender for Endpoint · CrowdStrike Falcon · SentinelOne
Segurança de redes	FortiGate · VMware NSX · Hillstone · Cisco Secure Firewall · proxy Cisco · IDS/IPS (Suricata, Snort) · VPN · segmentação e Zero Trust · Wireshark · tcpdump
Aplicações e APIs	F5 Advanced WAF · Imperva WAF Gateway e API Security · proteção contra DDoS · OWASP Top 10 · Burp Suite
Dados, identidade e criptografia	Thales Luna HSM e Payment HSM · CipherTrust (CDSP) · SafeNet Trusted Access (MFA/SSO) · PAM · IAM · Active Directory e Entra ID · DLP (Safetica) · Imperva DSF · PKI
Vulnerabilidades e hardening	Tenable Nessus · Qualys · OpenVAS · Nmap · CVSS e EPSS · gestão de patches · CIS Benchmarks
Cloud	AWS (CloudTrail, GuardDuty, Security Hub) · Microsoft Azure e Microsoft 365 (Defender, Entra ID, Purview)
Automação e SOAR	Python · PowerShell · Bash · APIs REST · SOAR (Cortex XSOAR, Shuffle) · expressões regulares
Sistemas e monitoração	Linux · Windows Server 2016/2022 · Active Directory e GPO · Zabbix
Governança e conformidade	ISO/IEC 27001 e 27002 · NIST CSF 2.0 · CIS Controls v8 · LGPD · PCI DSS · gestão de riscos
Comportamentais	Comunicação técnica com clientes e gestores · documentação clara · calma sob pressão em incidentes · mentoria · trabalho em equipe

CERTIFICAÇÕES

Thales	SafeNet Trusted Access Professional Engineer · jan/2025, válida até jan/2027 · ID 130728457 TPA: CipherTrust Data Security Platform (CDSP), General Purpose HSM, Payment HSM, High Speed Encryption, Workforce IAM e Customer IAM · dez/2024 Accelerate Pre-Sales Technical Professional (PTP)
Imperva	WAAP: WAF Gateway, API Security e Foundation · dez/2024 Data Security Fabric (DSF) · Network Protection · DDoS for Networks
Safetica	Safetica Certified Associate · jun/2026
Trellix	Trellix API Essentials · jun/2024
Cursos (Udemy)	Preparatório EXIN ISFS – Information Security Foundation (ISO/IEC 27001) · Governança de TI · Administração de Sistemas GNU/Linux · Windows Server 2016 e 2022

Lista completa, com mais de 30 credenciais e links de verificação, no LinkedIn.

FORMAÇÃO ACADÊMICA

Pós-graduação em Cybersecurity — FIAP	Em andamento	Fev/2026 – Atual
Tecnólogo em Análise e Desenvolvimento de Sistemas — Universidade Santo Amaro (UNISA)		Fev/2023 – Dez/2024

IDIOMAS

Português	Nativo
Inglês	Fluente
Espanhol	Básico

INFORMAÇÕES ADICIONAIS

- Disponível para trabalho híbrido ou remoto.
- Participação em eventos técnicos e de diversidade, como o Ada Lovelace Day.
- Projetos e laboratórios em yfreitas.krowncode.tech.