Larissa Castro Correa

Analista de Cibersegurança | SOC Analyst

larissalarissa.c16@outlook.com
São Paulo, SP — Brasil
linkedin.com/in/larissa-castro-correa

RESUMO PROFISSIONAL

Profissional de Cibersegurança com quase 4 anos de experiência em operações de SOC, atuando em monitoramento contínuo, triagem de alertas, resposta a incidentes e administração avançada de ferramentas de segurança (Wazuh, CrowdStrike Falcon, Check Point, Guardicore, TheHive) para múltiplos clientes corporativos. Experiência com treinamento de equipe, documentação técnica formal e campanhas de conscientização.

EXPERIÊNCIA PROFISSIONAL

Analista de Segurança Cibernética

jul/2022 – mar/2026

eSecurity — Serviços em Segurança Cibernética

- Monitoramento contínuo e triagem de alertas com escalação conforme criticidade
- Resposta a incidentes seguindo playbooks e runbooks, incluindo contenção e documentação formal
- Administração avançada de Wazuh SIEM: instalação, configuração, decoders, regras personalizadas, integrações, gerenciamento de agentes via API, monitoramento de Docker e auditoria de logs
- CrowdStrike Falcon: monitoramento EDR e homologação de software via sandbox
- Homologação manual de software em VM: análise de comportamento de rede e conexões suspeitas
- Firewall Check Point: criação de regras e gerenciamento de alertas IPS
- POC de ModSecurity (WAF) para implementação
- Guardicore (Akamai): operação de microsegmentação
- Microsoft Azure e Defender; análise de e-mails (phishing, spam, headers maliciosos)
- Documentação e gestão de incidentes via TheHive; monitoramento com Graylog
- Hardening de ambientes Microsoft
- Campanhas de conscientização e apresentações técnicas sobre ataques e protocolos
- Treinamento de analistas juniores em ferramentas, triagem de alertas e documentação

Analista de Suporte Pleno

2020 – 2022

Telemática Sistemas Inteligentes

- Gestão e análise de chamados via ServiceNow para um dos maiores contratos da empresa
- Consultas avançadas em banco de dados Oracle (SELECT, UPDATE, INSERT) para investigação e resolução de incidentes
- Geração de relatórios de BI (QlikView) e controle de indicadores da operação
- Contato direto com cliente para validação de testes e levantamento de informações

Operações Externas

ago/2019 – nov/2020

Banco Bradesco

- Elaboração de relatórios e análise de dados para controle de metas operacionais
- Apoio ao departamento de TI em controles de sistema e implementação de melhorias
- Verificação de protocolos de atendimento e auditoria de qualidade

FORMAÇÃO ACADÊMICA

Bacharelado em Ciências da Computação

UNINOVE — Universidade Nove de Julho — Concluído

CERTIFICAÇÕES

CompTIA Security+ CE — CompTIA — jul/2024 — jul/2027

NDE — Network Defense Essentials — Acadi-TI — out/2023

Linux Essentials — 4Linux — set/2022

Linux Fundamentals — 4Linux — set/2022

Kali Linux for Beginners — eSecurity — Cyber Security — ago/2022

Monitoramento de Ataques Cibernéticos com Wazuh — Victor Oliveira — Em andamento

COMPETÊNCIAS TÉCNICAS

SIEM: Wazuh (avançado — instalação, decoders, regras, integrações, API), Graylog

EDR: CrowdStrike Falcon, Microsoft Defender

Firewall / IPS: Check Point (regras, alertas IPS), ModSecurity WAF (POC)

Microsegmentação: Guardicore (Akamai)

Gestão de Incidentes: TheHive, OTRS

Cloud: Microsoft Azure, Microsoft Defender

ITSM: ServiceNow

Análise: Phishing, malware, artefatos maliciosos, logs, vulnerabilidades

Hardening: Políticas de hardening Microsoft

Sistemas Operacionais: Linux (Kali, Ubuntu, Rocky), Windows, Windows Server

Banco de Dados: Oracle (SQL avançado)

Containers: Monitoramento Docker com Wazuh

Frameworks: MITRE ATT&CK (TTPs), OWASP Top 10, NIST, Kill Chain

Threat Detection: Threat hunting, análise de IOCs, correlação de eventos, detecção de anomalias

Documentação: Relatórios técnicos, playbooks, runbooks, procedimentos operacionais

PLATAFORMAS DE TREINAMENTO

TryHackMe · LetsDefend · eSecurity Academy

IDIOMAS

Português — Nativo

Inglês — Técnico (leitura e escrita)