GABRIEL LIRA

SOC ANALYST · DETECÇÃO & RESPOSTA A INCIDENTES

BRASÍLIA, DF | +55 61 9916-5502 | LINKEDIN.COM/IN/LIRAGBR | LIRAGBR.GITHUB.IO

HISTÓRICO PROFISSIONAL

Profissional de Segurança da Informação atuante em operações defensivas (Blue Team) e resposta a incidentes, com vivência prática em ambientes corporativos críticos. Experiência consolidada no monitoramento contínuo de ameaças e detecção de anomalias operando plataformas de ponta como Darktrace (NDR) e CrowdStrike Falcon (EDR), além de ferramentas SIEM como Wazuh e Splunk. Proficiente na triagem de alertas, threat hunting e gestão de incidentes cibernéticos baseando-se no framework MITRE ATT&CK e nas diretrizes da norma NIST SP 800-61

FORMAÇÃO ACADÊMICA

PÓS-GRADUAÇÃO LATO SENSU EM SEGURANÇA CIBERNÉTICA

Centro Universitário de Brasília (CEUB) – 2025 / 2026.

TECNÓLOGO EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

Centro Universitário de Brasília (CEUB) – 2023 / 2025.

EXPERIÊNCIA

GARAGE TECH | SOC ANALYST

Brasília, DF, jun, 2026 – presente

Atuação direta no Security Operations Center (SOC) gerenciando a segurança de ambientes corporativos por meio do monitoramento contínuo e detecção avançada de ameaças. Responsável por operar a solução Darktrace para análise profunda de tráfego e detecção de anomalias de rede (NDR), atuando de forma integrada com o CrowdStrike Falcon para a proteção e contenção ativa de incidentes em endpoints (EDR). O fluxo de trabalho operacional envolve a gestão rigorosa de incidentes na plataforma DeskManager (ITSM), assegurando o cumprimento de SLAs. O escopo diário de atuação engloba a triagem de alertas complexos, correlação de eventos e investigação de comportamentos suspeitos, fundamentando o mapeamento de táticas e técnicas de invasão através do framework MITRE ATT&CK. Conduz o ciclo completo de resposta a incidentes em rigorosa conformidade com o framework NIST SP 800-61, fornecendo relatórios técnicos detalhados e coleta estruturada de evidências para o aprimoramento contínuo das regras de segurança defensiva

COMPETÊNCIAS TÉCNICAS

- **Segurança Defensiva e Operações:** Monitoramento de Rede, Resposta a Incidentes, Threat Hunting, Correlação de Eventos, Frameworks MITRE ATT&CK e NIST SP 800-61.
- **Plataformas e Ferramentas de Análise:** Darktrace (NDR), CrowdStrike Falcon (EDR), Wazuh e Splunk (SIEM), Wireshark, TShark, Nmap, Burp Suite e DeskManager (ITSM)
- **Redes & Infraestrutura:** TCP/IP, DNS, HTTP/HTTPS, STUN/WebRTC, Firewall, Linux (Kali, Parrot, Ubuntu Server), Windows Server.
- **Idiomas:** Português (nativo), inglês (leitura e escrita avançadas).