# **Plano de Negócios Resumido**

**Projeto: Ingestão de Logs + Detecção de Anomalias em Logs**

## **1. Visão Geral**

O projeto propõe uma solução inovadora para ingestão, padronização e análise de logs em tempo real, com foco na **detecção automática de anomalias** que possam representar falhas, ataques ou tentativas de invasão. O sistema combina técnicas de **Machine Learning** (Isolation Forest, Local Outlier Factor) e regras heurísticas para fornecer alertas imediatos e painéis de monitoramento intuitivos.

## **2. Problema**

Empresas e órgãos públicos enfrentam desafios crescentes no **monitoramento de logs**, devido ao grande volume de dados gerados diariamente. A análise manual é **demorada, suscetível a falhas humanas** e muitas vezes reativa, só identificando problemas após a indisponibilidade de serviços.

## **3. Solução**

Nosso sistema oferece:

* **Pipeline de ingestão** de logs em tempo real.
* **Modelos de detecção de anomalias** baseados em IA.
* **Painel interativo em Streamlit**, com dashboards de requisições por IP, métodos HTTP e visualização de anomalias.
* **Alertas em tempo real**, reduzindo o tempo de resposta a incidentes.

## **4. Público-Alvo**

* Equipes de **NOC, SRE e DevOps**.
* **PMEs** com infraestrutura de TI crítica.
* **Órgãos públicos** que precisam monitorar sistemas sensíveis.
* **ISPs e provedores de serviços** que buscam maior confiabilidade.

## 

## **5. Diferenciais**

* Execução **on-premise**, garantindo **privacidade e segurança dos dados**.
* Uso de **IA explicável** com logs detalhados para validação dos alertas.
* Arquitetura modular, fácil de expandir para novos modelos ou fontes de log.
* Solução **de baixo custo** comparada a ferramentas proprietárias.

## **6. Modelo de Negócio**

* **Licenciamento on-premise** com manutenção anual.
* **Consultoria e personalização** para ambientes específicos.
* **Versão SaaS futura** para empresas que preferem solução gerenciada.

## **7. Viabilidade Técnica**

* Desenvolvido em **Python (pandas, numpy, scikit-learn, streamlit)**.
* Integrações previstas com **Grafana e Firebase**.
* Código versionado no **Forge URI com boas práticas de engenharia**.
* Produto Mínimo Viável já validado em cenários simulados.

## **8. Roadmap de Evolução**

* Aprimoramento dos modelos com técnicas de **Deep Learning**.
* **Escalabilidade distribuída** para grandes volumes de dados.
* Dashboards personalizáveis para diferentes perfis de usuário.
* **Ações corretivas automatizadas** em incidentes críticos.

## **9. Conclusão**

A solução oferece um **ganho significativo em confiabilidade, proatividade e redução de custos operacionais**, sendo uma ferramenta estratégica para diferentes setores. Com o MVP validado, há potencial real de evolução para um produto **robusto, escalável e comercialmente viável**.