■ Relatório STRIDE – Arquitetura: api_management_workflow

Descrição: Arquitetura "api_management_workflow" com os seguintes componentes identificados no diagrama: Microsoft Entra, Api Gateway, Developer Portal, Logic Apps, Azure Services, Saas Services, Rest Api, Soap Api.

■ Componente: Microsoft Entra

- Ameaça (Tampering): Configurações de identidade podem ser alteradas para permitir acesso indevido.
  Contramedida: Políticas de alteração aprovadas e alertas de auditoria.
- Ameaça (Denial of Service): Ataques de senha/lockout podem impedir logins legítimos.
  Contramedida: Proteção de IP/password spray e lockout inteligente.

■ Componente: Api Gateway

- Ameaça (Information Disclosure): Configuração incorreta pode expor rotas internas.
  Contramedida: Políticas de redação de respostas e revisão de CORS.
- Ameaça (Denial of Service): Ataques volumétricos podem exaurir throughput.
  Contramedida: Rate limiting, throttling e cache em memória.

■ Componente: Developer Portal

- Ameaça (Information Disclosure): Documentação sensível ou tokens de exemplo vazados.
  Contramedida: Autenticação para acesso a APIs privadas.
- Ameaça (Tampering): Usuários maliciosos podem tentar alterar Swagger ou exemplos.
  Contramedida: Controle de versão e revisão de pull-requests de documentação.

■ Componente: Logic Apps

- Ameaça (Tampering): Workflows podem ser modificados para executar lógica maliciosa.
  Contramedida: Versão e aprovação de CI/CD em pipelines.
- Ameaça (Elevation of Privilege): Conexões gerenciadas com permissões excessivas.
  Contramedida: Principle of least privilege em conexões e Managed Identity.

■ Componente: Azure Services

- Ameaça (Information Disclosure): Dados sensíveis expostos se controles de acesso falharem.
  Contramedida: RBAC, redes privadas (Private Endpoints) e TLS.
- Ameaça (Repudiation): Operações não rastreadas em serviços PaaS.
  Contramedida: Diagnostic logs para Storage, SQL, etc.

■ Componente: Saas Services

- Ameaça (Availability): Dependência de terceiros pode causar interrupções.
  Contramedida: Timeouts e circuit-breakers em Logic Apps.
- Ameaça (Information Disclosure): Dados trafegando para SaaS externos sem criptografia.
  Contramedida: TLS obrigatório e políticas DLP.

■ Componente: Rest Api

- Ameaça (Tampering): Manipulação de payloads/verbos não esperados.
  Contramedida: Validação de esquema JSON e cabeçalhos.
- Ameaça (Information Disclosure): Respostas detalhadas podem vazar stack trace.
  Contramedida: Sanitização de erros, Content-Security-Policy.

■ **Componente: Soap Api**

- Ameaça (Information Disclosure): WS-Security configurado incorretamente.
  Contramedida: Assinatura XML e encriptação.
- Ameaça (Repudiation): Sem logs de requisição SOAP.
  Contramedida: Logs detalhados de SOAP envelopes.