ROADMAP DE BOAS PRÁTICAS PARA SEGURANÇA DA API DO KUBERNETES

1. **Introdução**
- Visão geral
- Aplicação de boas práticas em segurança da API do Kubernetes

2. Autenticação e Autorização

- Implementar autenticação forte (Token, TLS 1.3)
- Configuração de RBAC
- Princípio do menor privilégio

3. Proteção de Secrets

- Armazenamento seguro
- Criptografia em repouso (etcd)
- Acesso restrito via RBAC

4. Proteção TLS e HTTPS

- Exigência de TLS 1.3
- Certificados válidos (Let's Encrypt, auto-assinado)
- Validação e rotação de certificados

5. Controle de Acesso à API

- Bloqueio de exposição direta
- Uso de VPN, firewalls e Ingress com TLS
- Restrições por IP
- Rate limiting

6. Ferramentas e Auditoria

- Falco, Kubeaudit, cert-manager
- Postman com token JWT para testes controlados

7. Pontos de Atenção

- Ausência de MFA
- Controle por IP
- Limitação de requisições

8. Conclusão

- Segurança como processo contínuo
- Revisão
- Atualização constante