📘 **Canvas: Deep Dive – Quản Lý Secrets bằng External Secrets trong GenAI Factory**

🎯 Mục tiêu Hardening: Bảo mật ở Cấp độ Sản xuất

Trong môi trường **Production-Grade**, việc quản lý bí mật (Secrets) không chỉ là lưu trữ khóa API mà là **bảo vệ tài sản chiến lược** — đặc biệt khi các khóa API LLM (như OpenAI, Anthropic) có chi phí rất cao và ảnh hưởng trực tiếp đến an toàn tài chính của hệ thống.

Mục tiêu: **Loại bỏ hoàn toàn việc dùng Kubernetes Secrets cơ bản** (vốn chỉ là Base64) và thay thế bằng **External Secrets**, kết nối trực tiếp với các dịch vụ quản lý bí mật chuyên nghiệp như HashiCorp Vault, AWS Secrets Manager, Azure Key Vault.

I. ⚠️ Vấn Đề của Kubernetes Secrets Cơ Bản

Trong thiết kế ban đầu, các file như `api-keys-secret.yaml` được dùng để chứa khóa API.

Vấn đề: Kubernetes Secrets chỉ mã hóa Base64, **không phải mã hóa thực sự (encryption)**.
Bất kỳ ai có quyền truy cập vào file YAML hoặc cơ sở dữ liệu etcd đều có thể dễ dàng giải mã khóa API.

➡️ Điều này **vi phạm nguyên tắc bảo mật cơ bản**: > ❌ *"Không lưu trữ bí mật trong Git."*

II. ✅ Giải Pháp: External Secrets Operator (ESO)

External Secrets Operator (ESO) là một Controller trong Kubernetes, hoạt động như **cầu nối giữa Kubernetes và Secret Manager bên ngoài**.

Cấu phần	Vai trò	Tầm quan trọng (Hardening Value)
Secret Manager	Kho lưu trữ bí mật an toàn cao (HashiCorp Vault, AWS Secrets Manager, Azure Key Vault).	Lưu trữ an toàn, được mã hóa và kiểm toán (audit) đầy đủ.
External Secrets Operator	Controller trung gian chạy trong cụm Kubernetes.	Đảm nhận việc xác thực, truy xuất và đồng bộ hóa bí mật từ Secret Manager.

Cấu phần	Vai trò	Tầm quan trọng (Hardening Value)
Kubernetes Secret	Kết quả tạm thời được tạo ra bởi ESO.	Cung cấp bí mật cho ứng dụng (Pod) thông qua cơ chế injection.

💡 **Hardening Value:** Không lưu trữ bí mật trong Git. Kubernetes chỉ nắm giữ metadata, không bao giờ thấy giá trị thực của key.

III. ⚙️ Cơ Chế Hoạt Động trong `infra/`

📦 A. Manifest Cũ (Không An Toàn)

```yaml
# infra/k8s/secrets/api-keys-secret.yaml (CŨ)
apiVersion: v1
kind: Secret
metadata:
  name: genai-api-keys
type: Opaque
data:
  OPENAI_API_KEY: Wg9rR21... # Base64 encoded key
```

❌ **Nhược điểm:** Lưu khóa API trực tiếp trong Git, chỉ được Base64-encode.

🧩 B. Manifest Mới (Hardened - Dùng External Secrets)

```yaml
# infra/k8s/secrets/external-secret.yaml (MỚI)
apiVersion: external-secrets.io/v1beta1
kind: ExternalSecret
metadata:
  name: genai-external-api-keys
spec:
  refreshInterval: "1h" # Tự động cập nhật mỗi giờ
  secretStoreRef:
    name: aws-secret-store
    kind: SecretStore
  target:
    name: genai-api-keys-sync
    creationPolicy: Owner
  data:
  - secretKey: OPENAI_API_KEY
    remoteRef:
      key: /production/genai-factory/openai-key
      property: api_key
```

✅ **Ưu điểm:** - File YAML trong Git **chỉ chứa metadata**, không chứa giá trị thực. - Ứng dụng vẫn đọc từ `K8s Secret` chuẩn (`genai-api-keys-sync`), nhưng **Secret này được đồng bộ hóa tự động từ Secret Manager**.

IV. 🧠 Kết Quả Hardening & Giá Trị Bảo Mật

Nguyên tắc	Cách Được Đảm Bảo
Least Privilege (Quyền hạn tối thiểu)	Chỉ ESO có quyền truy cập đọc bí mật. Các Pod chỉ đọc giá trị đã được đồng bộ hóa.
Auditability (Khả năng kiểm toán)	Mọi truy cập vào key đều được ghi lại trong Secret Manager (Vault/AWS).
No Static Secrets in Git	Không có khóa API thực tế được lưu trong repo.
Auto Rotation & Refresh	Bí mật được tự động cập nhật định kỳ, tránh rò rỉ lâu dài.

🚀 Kết luận

Sử dụng **External Secrets** trong lớp `infra/` là bước chuyển **từ Dev sang Production thật sự**:

✅ An toàn tuyệt đối cho khóa API LLM.
✅ Tuân thủ chuẩn bảo mật doanh nghiệp (SOC2, ISO27001).
✅ Đảm bảo khả năng kiểm toán và mở rộng an toàn trên Cloud.

> **Tóm lại:** External Secrets là lớp bảo mật nền tảng giúp GenAI Factory đạt chuẩn sản xuất thực thụ — bảo vệ tài sản quan trọng nhất: *bạn và dữ liệu của bạn*.