циан

июнь 2025

Deep Sick. Как быть продуктивной компанией в новом AI мире, и не болеть утечками

Александр Смирнов
Senior Application Security Engineer.
Циан

циан

Тренды AI

Постоянно появляются новые провайдеры LLM

Автоматизация бизнес процессов

AI Агенты

циан

Почему ИБ тут актуальна?

- Утечка DeepSeek
- No/Low code со встроенными агентами
- AI агенты принимают решения на основе вывода LLM
- Промт инъекции
- Высокая стоимость API

циан

Решение Циан

Единый шлюз для запросов во внешние LLM

Какие контроли безопасности для этого реализовали?
Какие бенефиты получили? Как используем?

циан

gpt-gateway

Секреты хранятся в Vault

Несколько провайдеров LLM

Таймауты и ретраи

Управление промптами

Межсервисная аутентификация

Управление лимитами запросов, квотирование

Детект и маскирование конфиденциальных данных

циан

Logging

Kafka. Access Control List

Логи доезжают до SIEM

Алерты

Статистика запросов

циан

Process

Политика использования

Предупреждаем о рисках

Ревью каждой интеграции

циан

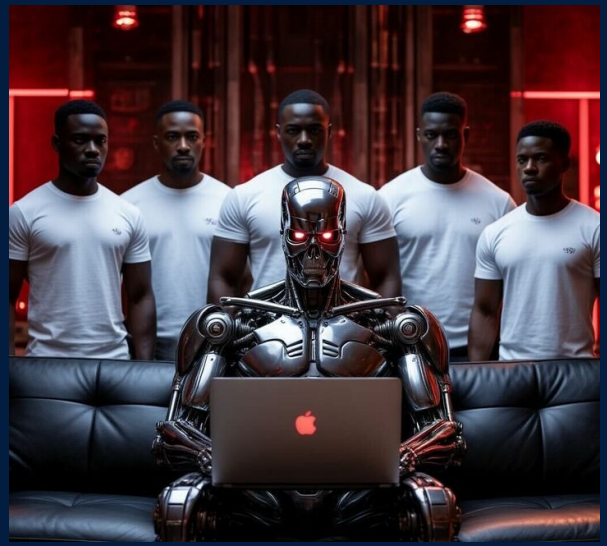
Применение в разработке. Кейсы

Продуктовые фичи

Корпоративный чат бот

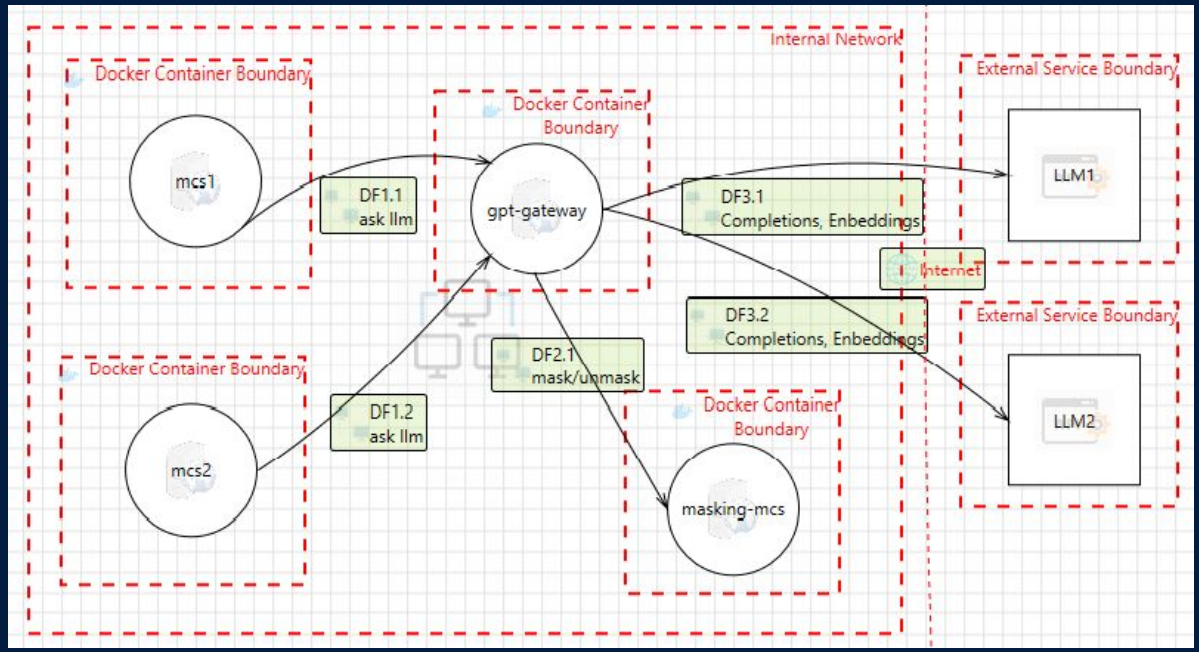
Хелп по документации

Ревью кода по заданным правилам



циан

Применение в разработке



циан

Заключение

Единый шлюз — это рабочий способ сделать взаимодействие с внешними LLM безопасным, расширяемым и отказоустойчивым

циан

Roadmap

1. GPT gateway

Микросервис
Межсервисная аутентификация
Управление промптами
Логирование

2. Masking

Маскирование данных

3. Формируем политику

Политика использования внешних LLM в компании

4. Используем в корп решениях

Продуктовые фичи
Корпоративный чат бот
Ассистенты ревью кода

5. Собираем аналитику

Статистика использования внешних LLM в компании

циан

Спасибо за внимание

Телеграм: @memory_stream

Почта: alessander.smirnov@gmail.com