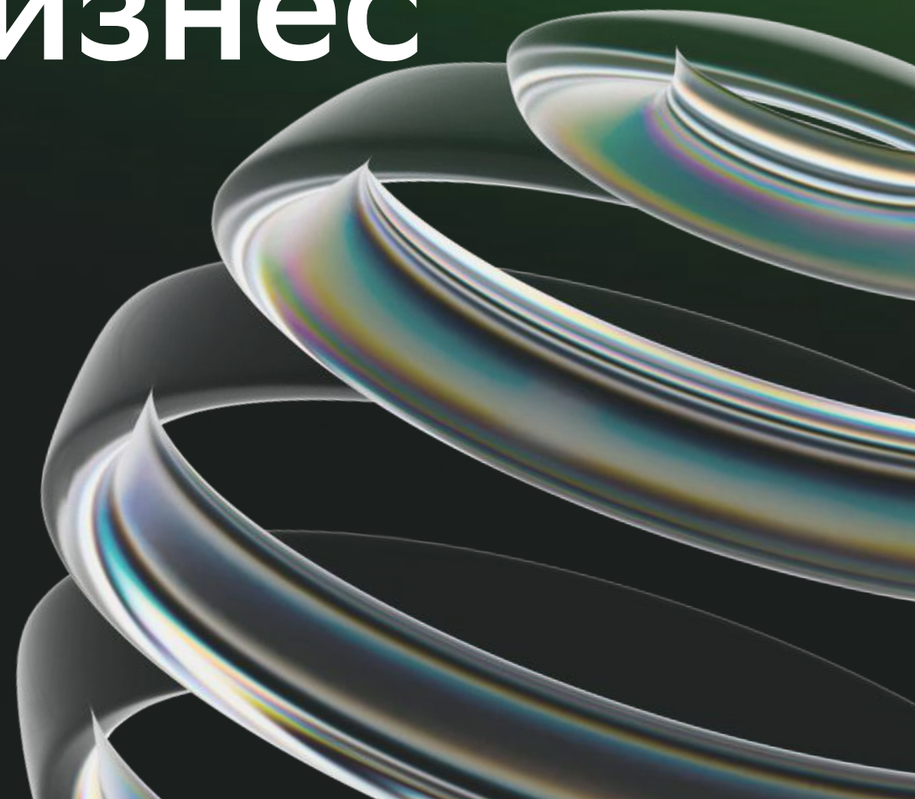
Домклик
СБЕР

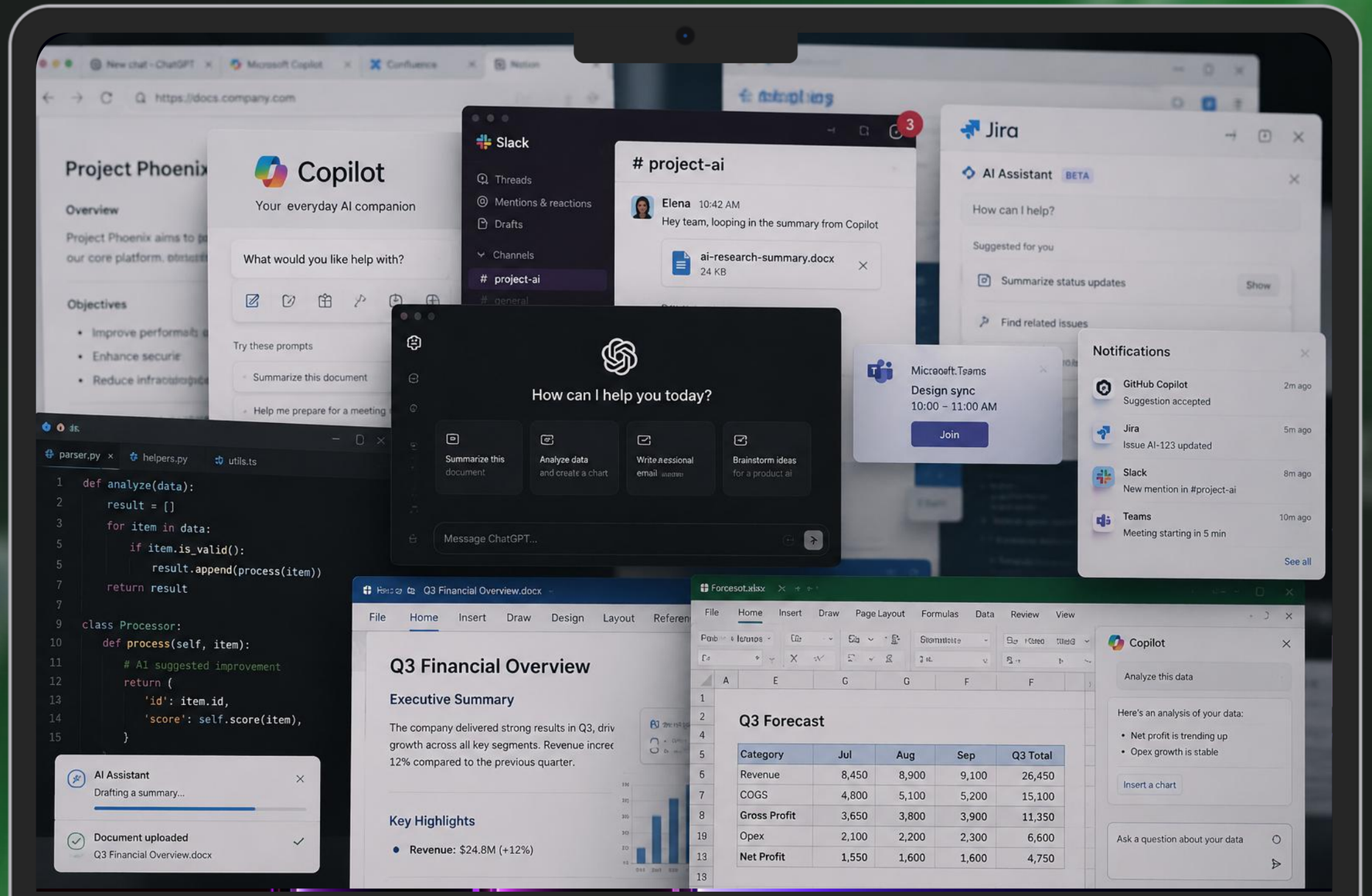
Shadow AI: пока CISO пишет политику, бизнес уже работает с ИИ

Лагоденко Андрей,
CISO Домклик
Май’26



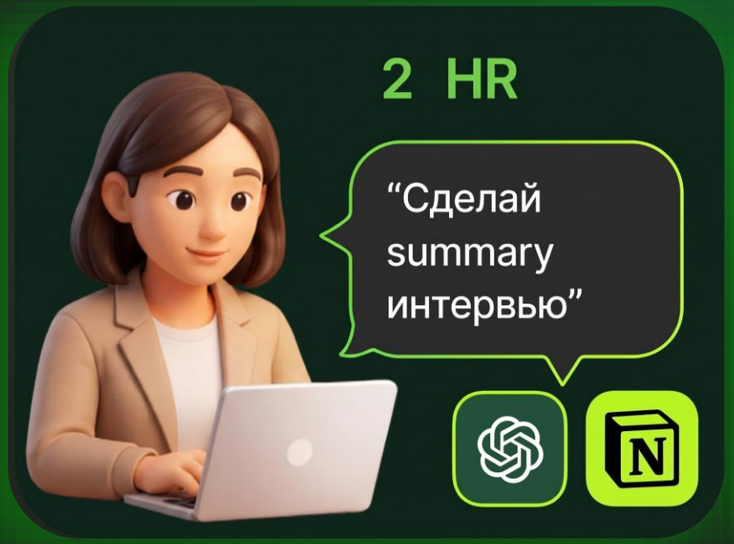
Shadow AI

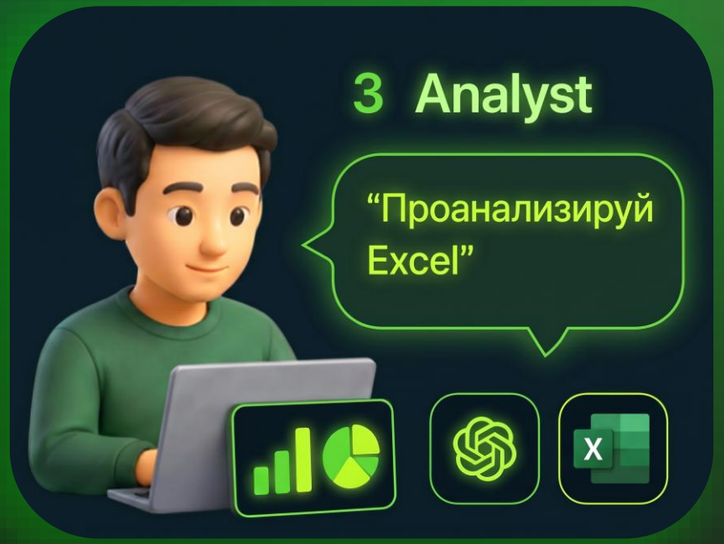
Домклик
СБЕР

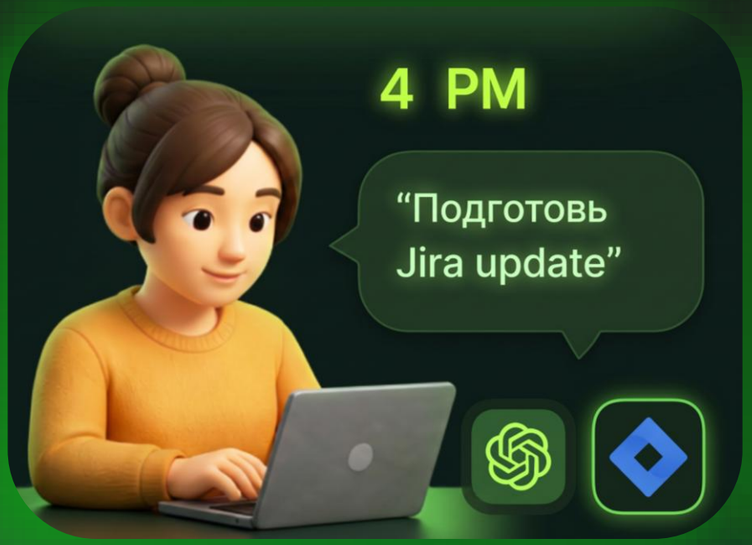


Выглядит как обычная работа

Домклик
СБЕР







А что же с потоками данных?

Домклик
СБЕР

1. ДАННЫЕ КОМПАНИИ

То, с чем мы работаем каждый день

- Документы
- Код
- Excel
- Звонки
- HR
- Jira

2. ДЕЙСТВИЯ СОТРУДНИКОВ

Повседневные запросы к ИИ


Сделай summary


Напиши SQL


Подготовь письмо


Проанализируй Excel

3. КУДА УХОДЯТ ДАННЫЕ

Внешние AI-ресурсы

Public AI Chats

ChatGPT, Claude, Gemini и другие

AI-enabled SaaS

Microsoft 365 Copilot, Notion AI, Slack AI, Jira AI и другие

Agents & Plugins

AI-агенты, плагины, интеграции, расширения браузера и IDE

Shadow AI побеждает за счет скорости

Домклик
СБЕР

Отчёт

2 часа → 20 минут

Анализ Excel

1 час → 10 минут

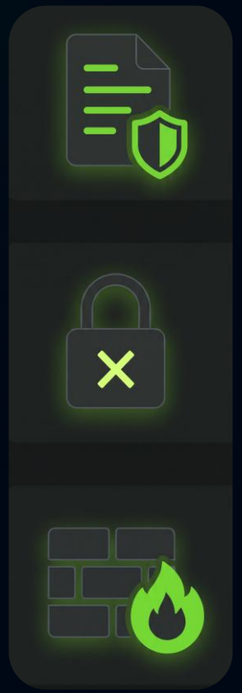
Ответ клиенту

30 минут → 5 минут

Запрет AI не контроль – а потеря видимости

Домклик
СБЕР

ЧТО ДЕЛАЕТ КОМПАНИЯ



AI policy

Access denied

Firewall block

ЧТО ПРОИСХОДИТ РЕАЛЬНО

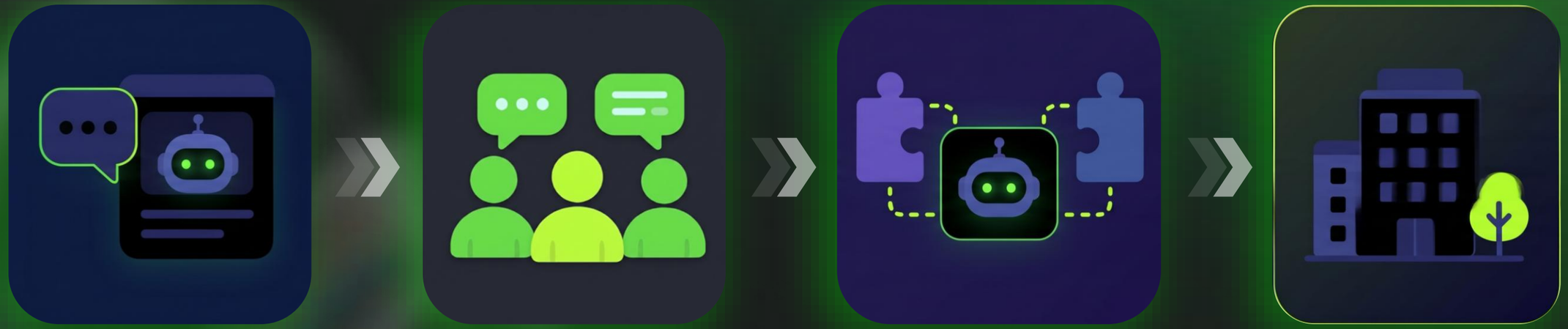
Личный телефон

Личный аккаунт

Браузер AI

Shadow AI прорастает в бизнес

Домклик
СБЕР



Личное использование AI

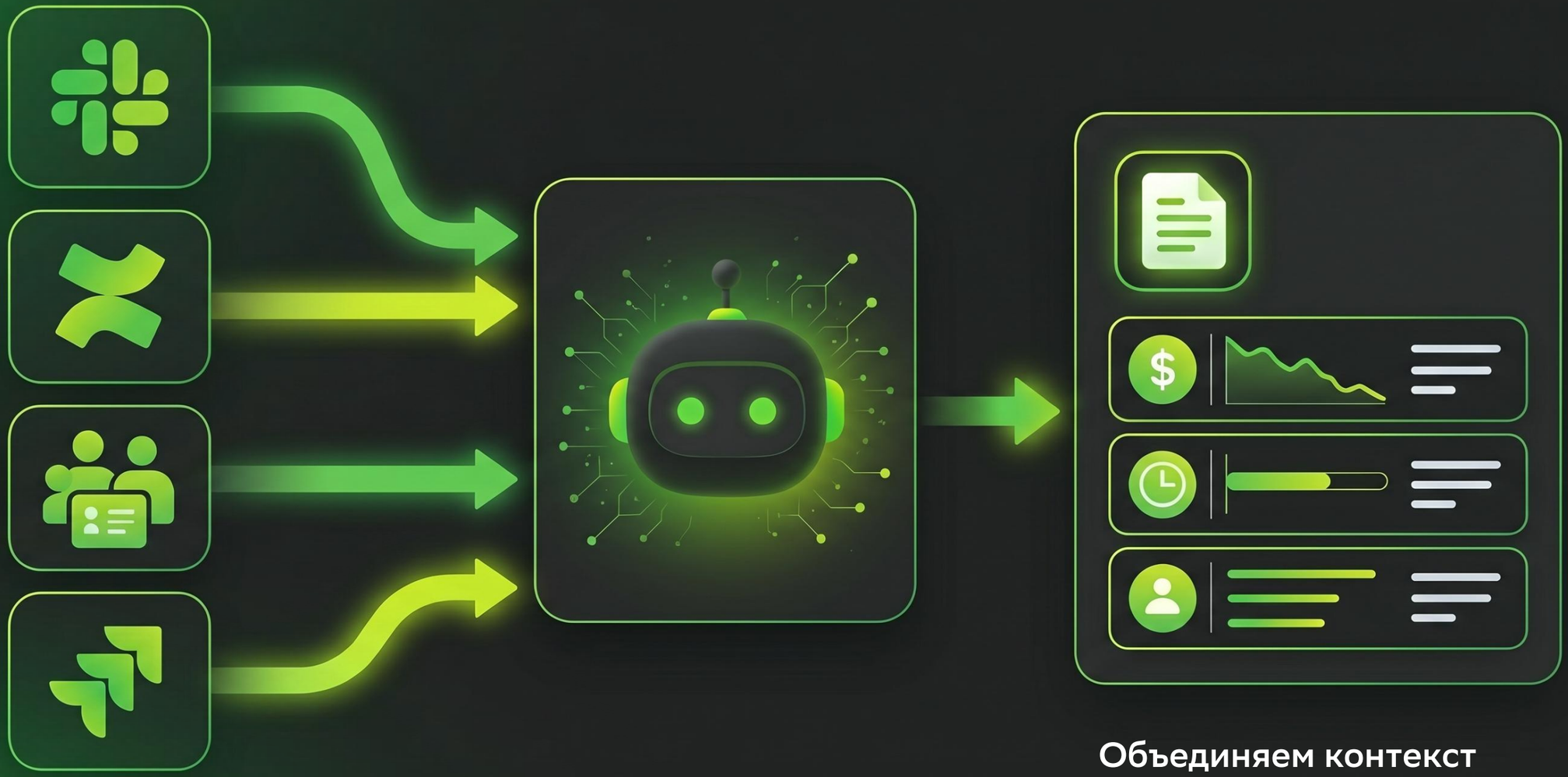
Делимся с командой

С интеграциями еще удобней

Часть бизнес-процесса

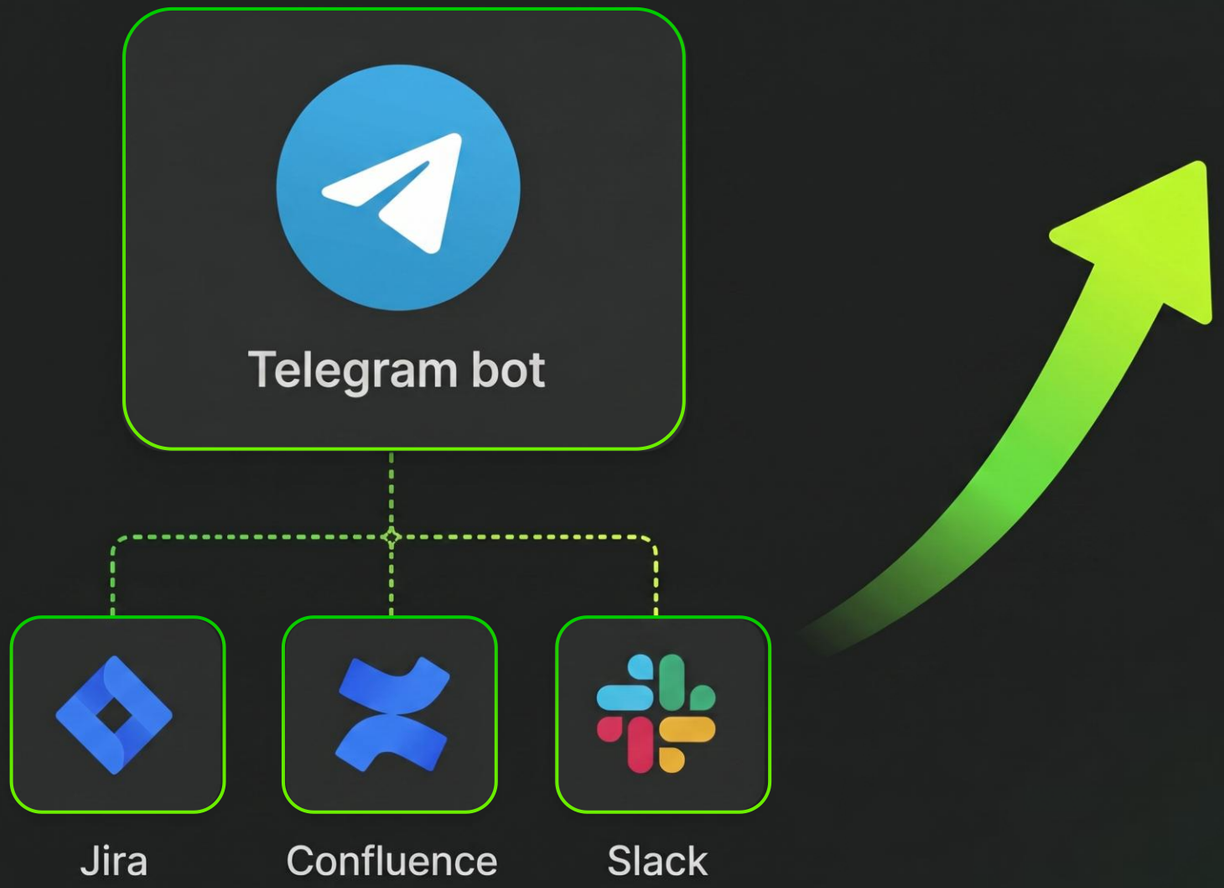
КЕЙС #1 Саммаризация

Домклик
СБЕР



Объединяем контекст
(раскрывая конфиденциальные данные)

Кейс #2. Телеграм-бот



- Личные устройства
- Нет IAM
- Нет логов

Главная ошибка

Домклик
СБЕР

политики
ревью
риски
согласования
AI-платформа
AI шлюз
процессы
Реестр моделей
регламенты
red teaming
compliance
архитектура

Понять, где уже используют?

Дать согласованный AI

Ввести простые правила

Как реально найти Shadow AI

Домклик
СБЕР

Браузер и расширения

ГДЕ СМОТРЕТЬ
Proxy / EDR / NGFW / Logs

ЧТО ИСКАТЬ
ChatGPT, Claude, Gemini, etc.

Teams / Slack / Telegram

ГДЕ СМОТРЕТЬ
Чаты, боты, каналы

ЧТО ИСКАТЬ
LLM-, summary-, search- боты

Загрузка данных во внешние AI

ГДЕ СМОТРЕТЬ
Proxy / DLP / Logs

ЧТО ИСКАТЬ
Документы, Excel, Code

Интервью с командами

Что спрашивать
где AI уже экономит время?
без каких AI инструментов неудобно?
что используют “временно”?
где хотелось бы начать использовать?

Как дать сотрудникам согласованный AI

Домклик
СБЕР

Подход	Где применять	Что учесть
Корпоративные аккаунты у коммерческих AI	**Быстрый старт и хороший UX**	Логирование, SSO, использование данных для дообучения
On-prem модели	**Чувствительные данные, RAG**	Качество моделей, GPU/Инфраструктура, TCO
AI Gateway	**Контролировать разные AI-сервисов**	Логирование, контроль файлов

Правила, которые люди **реально** читают

Домклик
СБЕР

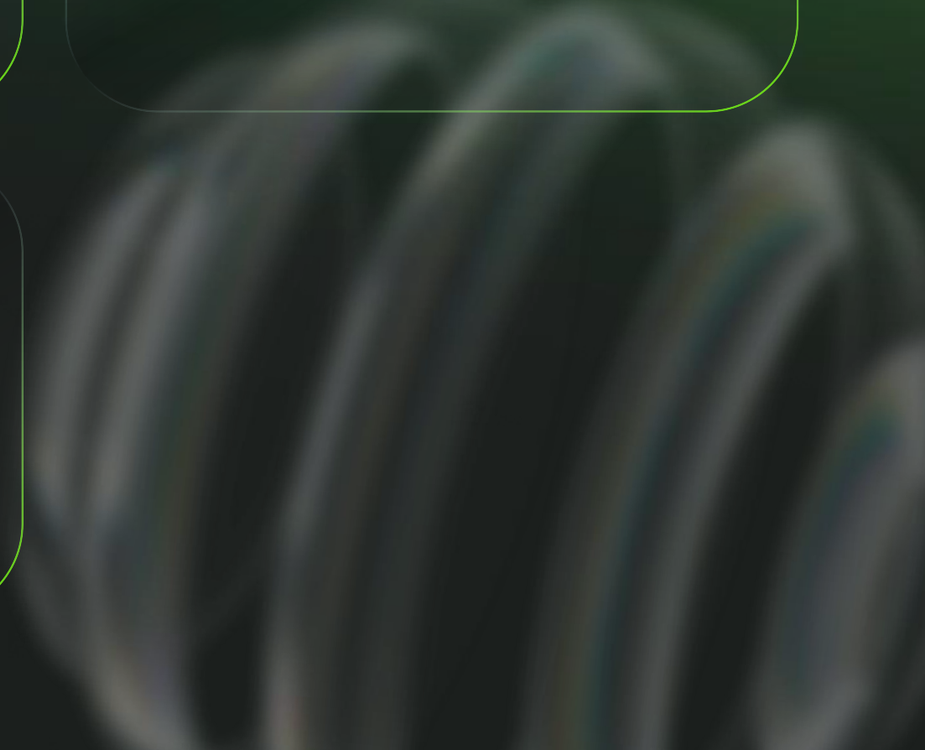
Не отправлять
секреты и креды

Не загружать
персональные данные
(особенно клиентские)

Всегда проверять
ответ модели, прежде чем использовать

Внешний AI для **неконфиденциальных** данных

В работе использовать только **согласованный AI**



Не все AI-риски одинаково опасны

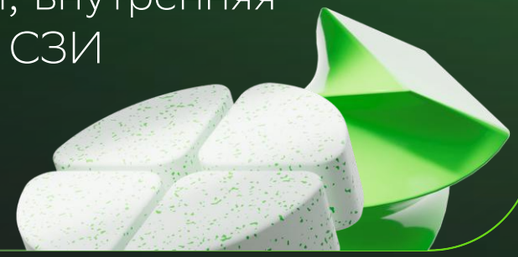
Домклик
СБЕР

Клиентские данные

Персональные данные,
договоры, обращения

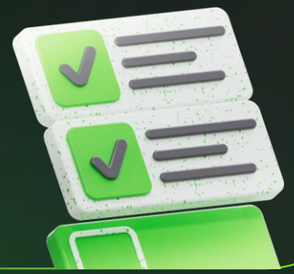
ИТ/ИБ-архитектура

Репозитории, скрипты, внутренняя
логика, архитектура и СЗИ



Доступ к внутренним данным

Jira, Confluence, Slack, CRM,
базы знаний



Агенты

Боты, автоматизация, агенты
и мультиагентные системы

Управляемость в повторяемости

Обнаружить, где используют

Дать согласованный AI

Ограничить опасные сценарии

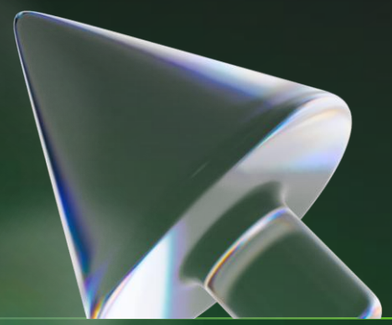
Логировать и наблюдать

Обновлять правила

Вместо выводов

Домклик
СБЕР

AI с нами надолго



Заборы не помогут

Управляемость возможна