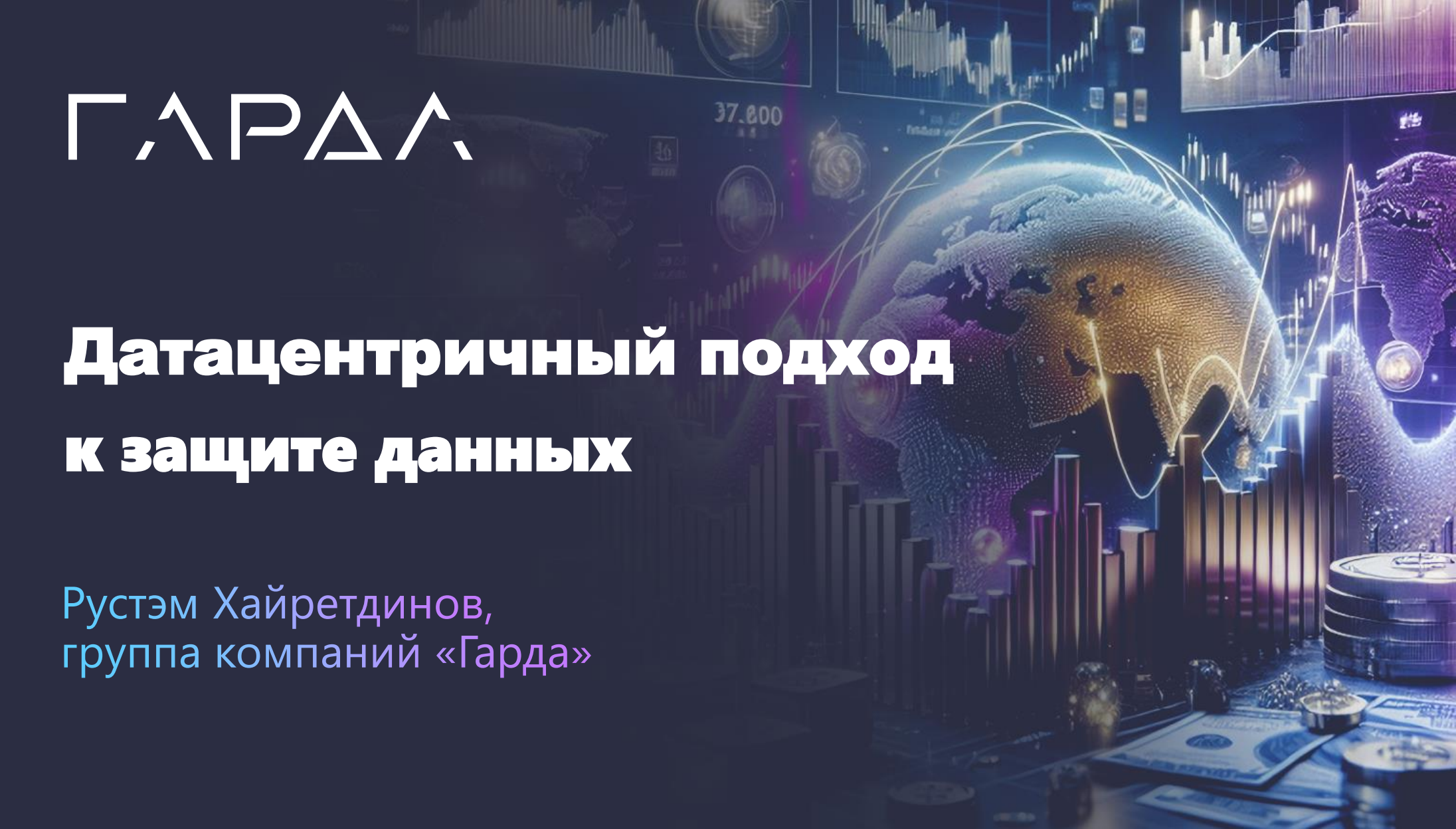
ГАРДА

# Датацентричный подход к защите данных

Рустэм Хайретдинов,
группа компаний «Гарда»



# Новое в противостоянии в киберпространстве

- Цель — не заработок, а уничтожение + PR
- В 100% инцидентов есть внутренний «соучастник»
  - Социнженерия (фишинг, ‘приказы’ начальника и т.п.)
  - Халатность (неправильные настройки, слабые пароли)
  - Слабый подрядчик (экономия на безопасности)
  - Шантаж (угрозы самому и родственникам, хищение средств)
  - Подкуп (обещание денег, выезда, гражданства)
- Сегодня лучший хакер в HackerOne – ИИ-агент Xbow
- «Цифровое смирение» всех рано или поздно взломаю

# Реакция на новый контекст:

## защищать не только инфраструктуру, но и данные

- Знать где находятся данные (СУБД, приложения, файлы, трафик)
- Знать кто и зачем имеет к ним доступ
- Управление доступом, ролевая модель
- Контроль запросов **и ответов**
- Сегментация данных
- Маскирование, обезличивание, токенизация, шифрование
- Пассивный подход «мы всё пишем» не защищает
- План Б - быстрое восстановление

# Специфика защиты данных

- Из коробки можно увидеть только экстремальные аномалии
- Надо знать где находятся и как «живут» данные
- Надо понимать бизнес-контекст оборота данных
- Надо подстраиваться под приложения и открытые API
- Надо понимать ролевые модели всех участников доступа к данным, включая внешних

ГАРДА

# Задавайте вопросы

Рустэм Хайретдинов,
заместитель генерального директора
группы компаний «Гарда»
+7 (903) 961-7312
r.khairetdinov@gardatech.ru