СБЕР 2В

Измерение эффективности функции кибербезопасности в компании



Иван Дмитриев
Директор по кибербезопасности
группы компаний Сбер2В

ОЦЕНКА

СБЕР 2В

Измеряем уровень: «шашечки или ехать?»



Спросить у CISO

Желаемый CISO уровень

Провести аудит

Необходимый кому-то уровень

Управление риском

Компания верит в необходимый уровень

Метрики

Необходимый и достаточный уровень

ОЦЕНКА

СБЕР 2В

Измеряем уровень КБ: «шашечки или ехать?»

Спросить у CISO

(Субъективная оценка)

- Доверие внутреннее
- Доверие клиента
- Объективность
- Реалистичность
- Скорость оценки

Желаемый CISO уровень

Провести аудит

(Претензия на объективную оценку показательного выступления)

- Доверие внутреннее
- Доверие клиента
- Объективность
- Реалистичность
- Скорость оценки

Необходимый кому-то уровень

Управление риском

(Все хотят, но никто не знает, как именно это сделать)

- Доверие внутреннее
- Доверие клиента
- Объективность
- Реалистичность
- Скорость оценки

Компания верит в необходимый уровень

Метрики

(«Стильно, модно, молодёжно»)

- Доверие внутреннее
- Доверие клиента
- Объективность
- Реалистичность
- Скорость оценки

Необходимый и достаточный уровень

СБЕР 2В

«А как у них?»: принципы КБ в Сбер2В

01
Спрашиваем у CISO

- Ежеквартальная отчётно-выборная конференция в составе комитета по безопасности

РЕЗУЛЬТАТ

- презентуем результаты
- строим планы
- обсуждаем выученные уроки

02
Проводим аудит

- Ежегодный аудит от акционера
- ISO 27001

РЕЗУЛЬТАТ

- примеряемся к лучшим практикам группы
- собираем практические кейсы в свою базу

03
Управляем рисками

- Применяем риск-ориентированный подход
- Не питаем иллюзий, что это панацея

РЕЗУЛЬТАТ

- совместно с бизнесом управляем риском
- применяем метрики для принятия решений

04
Используем метрики

- Еженедельные отчёты для топов и акционеров
- Оперативные дашборды для продактов
- BI для принятия решений на основе данных

РЕЗУЛЬТАТ

- принимаем решения на основе данных
- отчитываемся без встреч
- воспитываем культуру КБ

МЕТРИКИ

СБЕР 2В

Все ли подойдет?

ИНФРАСТРУКТУРА

- 0,18 — Среднее время реагирования на инцидент КБ — порог – не более 8 часов
- 17,4 — Среднее время решения инцидента КБ — порог – не более 120 часов
- нет — Время уведомления о высокоприоритетных инцидентах — порог – менее 3 часов
- 100% — Верифицированных сервисов на периметре — порог – не менее 100%
- 99,2% — Покрытие АВПО — порог – не менее 90%
- 100% — Покрытие EDR — порог – не менее 100%
- 100% — Покрытие AntiDDoS — порог – не менее 100%
- 100% — Покрытие 2FA для удаленных подключений — порог – не менее 100%
- 100% — Покрытие WAF — порог – не менее 100%
- нет — Среднее время устранения критических уязвимостей на периметре — порог – не более 5 часов
- нет — Среднее время устранения высоких уязвимостей на периметре — порог – не более 24 часов

КОМПЛАЕНС

- 100% — Актуальность данных в реестре РКН — порог – не менее 100%
- 100% — Актуальность политики в отношении обработки ПДн — порог – не менее 100%
- 100% — Покрытие процессов обработки ПДн актуальными регламентами — порог – не менее 100%
- 100% — Покрытие мониторингом индикаторов риска РКН — порог – не менее 100%
- 100% — Соответствие установленным срокам обработки обращений субъектов ПДн — порог – не менее 100%
- 100% — Соответствие установленным срокам обработки запросов регуляторов — порог – не менее 100%
- 0 — Некатегорированных объектов КИИ — порог – не более 0
- 0 — Информирований НКЦКИ с нарушением сроков (П-282) — порог – не более 0

ПРОДУКТЫ

- 100% — Релизов выведено в ПРОМ с согласованием КБ — порог – не менее 100%
- 100% — Покрытие релизов средствами SAST и SCA — порог – не менее 100%
- 0 — Релизов с критическими и высокими дефектами, обнаруженными SAST и SCA, выведено в ПРОМ — порог – не более 0
- 0 — Средний срок устранения дефектов — порог – не более 60 дней

ТРЕБОВАНИЯ

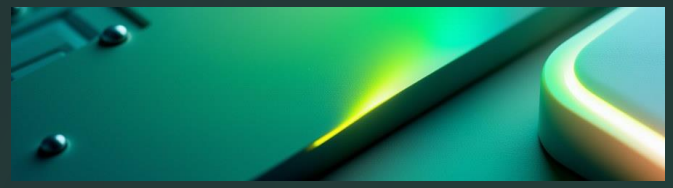
СБЕР 2В

Какими должны быть метрики?



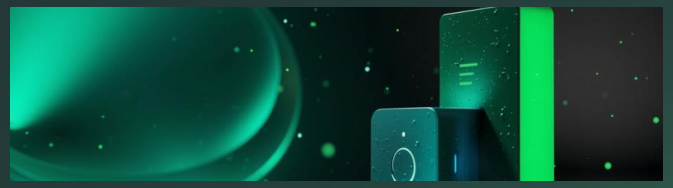
01 Управляемыми

Они поддаются прямому воздействию



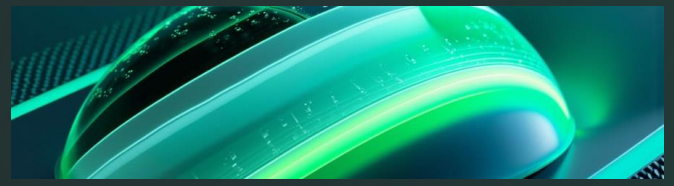
02 Релевантными

Связаны с целями и отражают достижение ключевых результатов



03 Определёнными

Позволяют получать однозначные результаты при повторных измерениях



04 Отзывчивыми

Должны своевременно реагировать на реальные изменения в процессах, позволять выявлять тренды и отклонения



05 Достоверными

Для метрики должны быть доступны точные и своевременные данные



06 Стабильными

Метрики должны отслеживать динамику, позволять сравнивать результаты за разные периоды без искажений

СБЕР 2В

Архитектура метрик

ЦЕЛЬ:

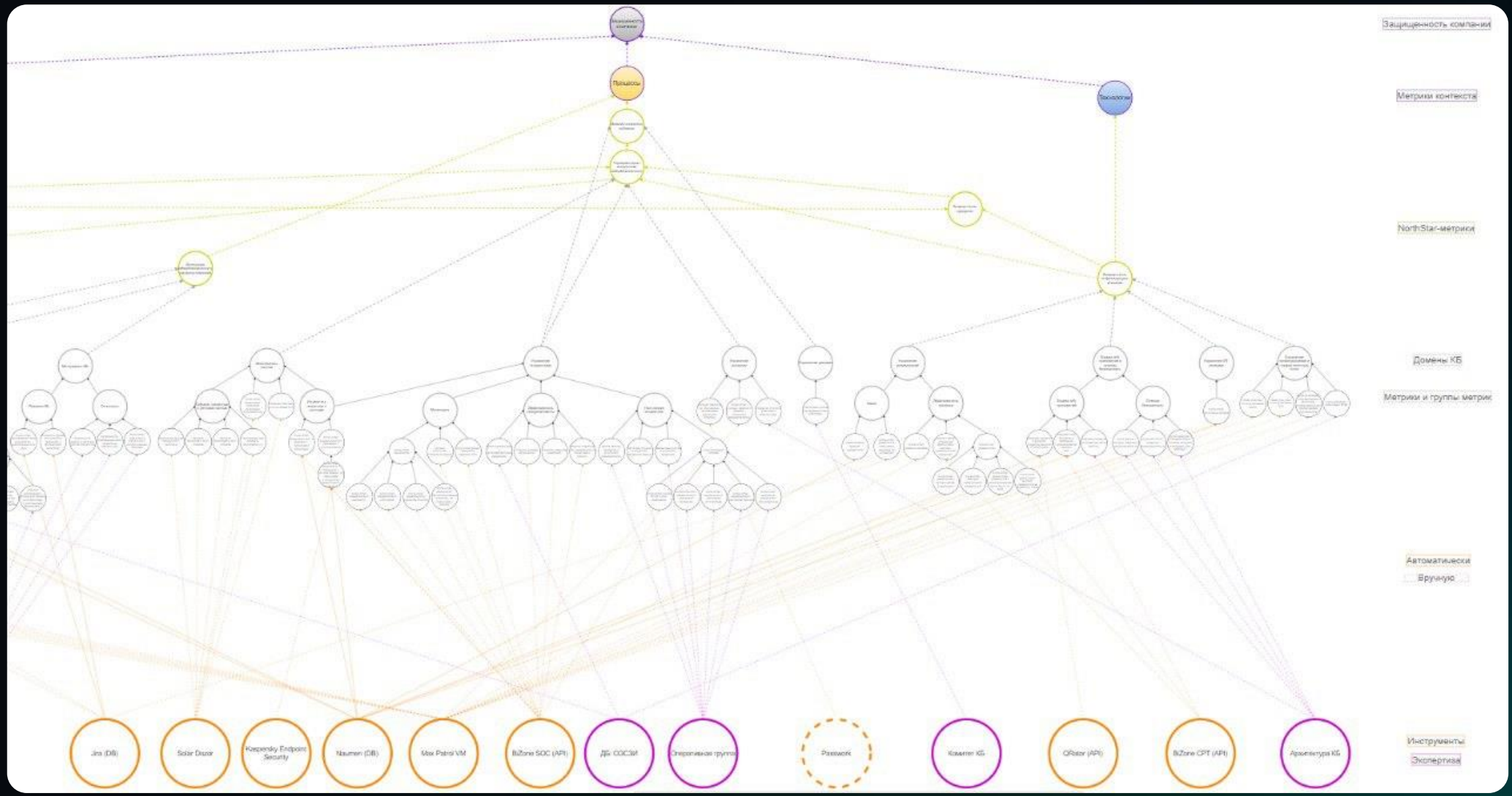
Определение и обеспечение уровня риска КБ, необходимого для устойчивого развития компании с помощью оценки и моделирования взаимосвязи различных групп метрик



ПРАКТИКА

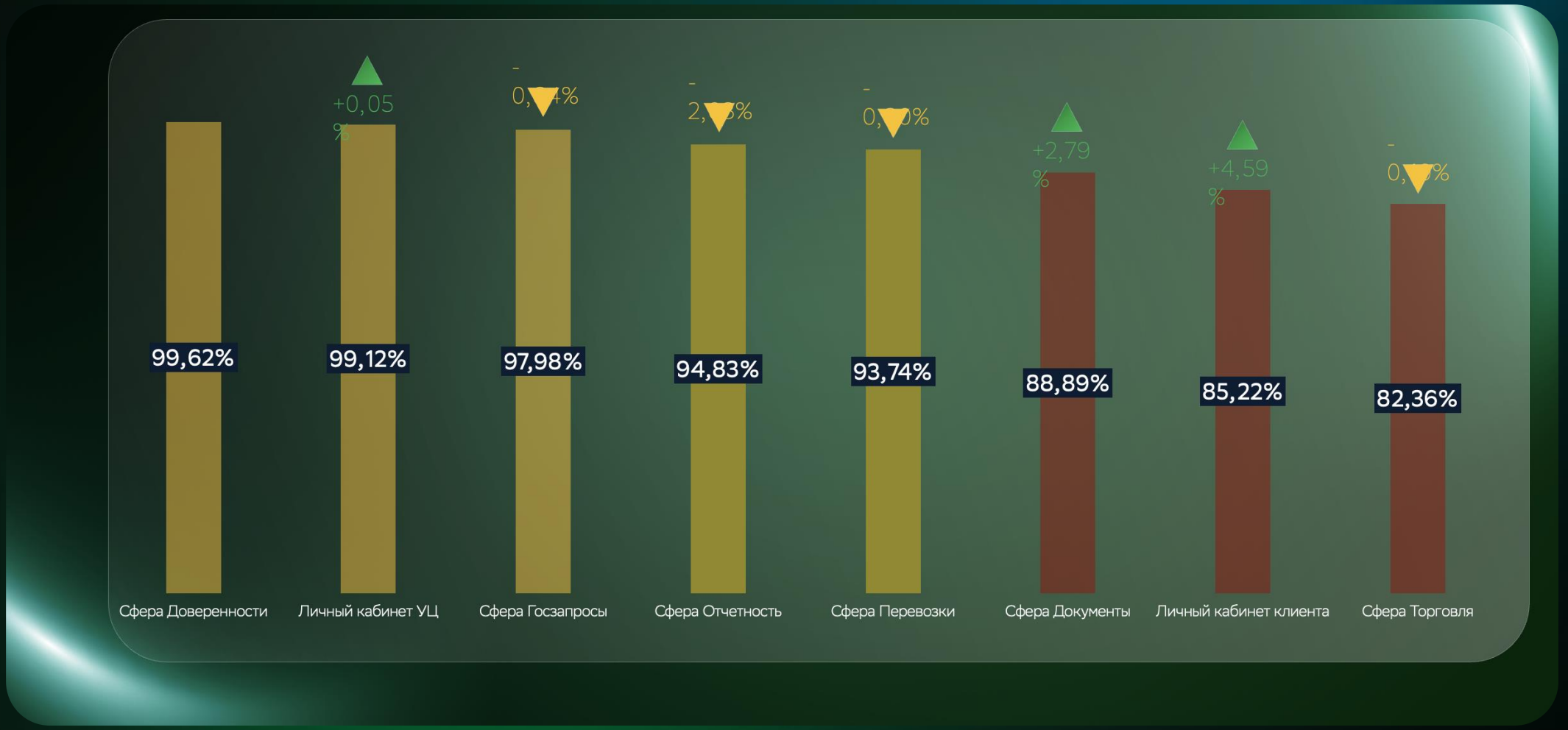
СБЕР 2В

Реальность бизнеса



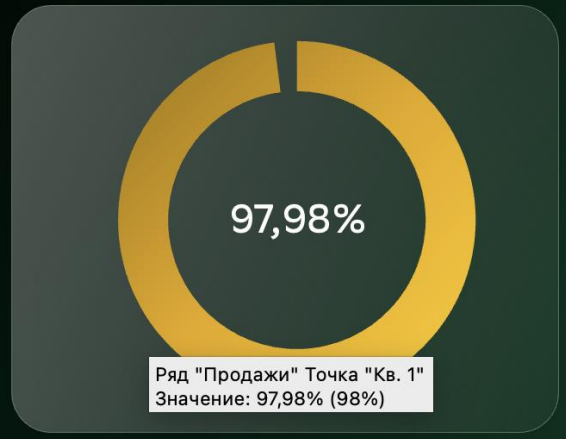
СБЕР 2В

Пример: RUN-метрики в CEO

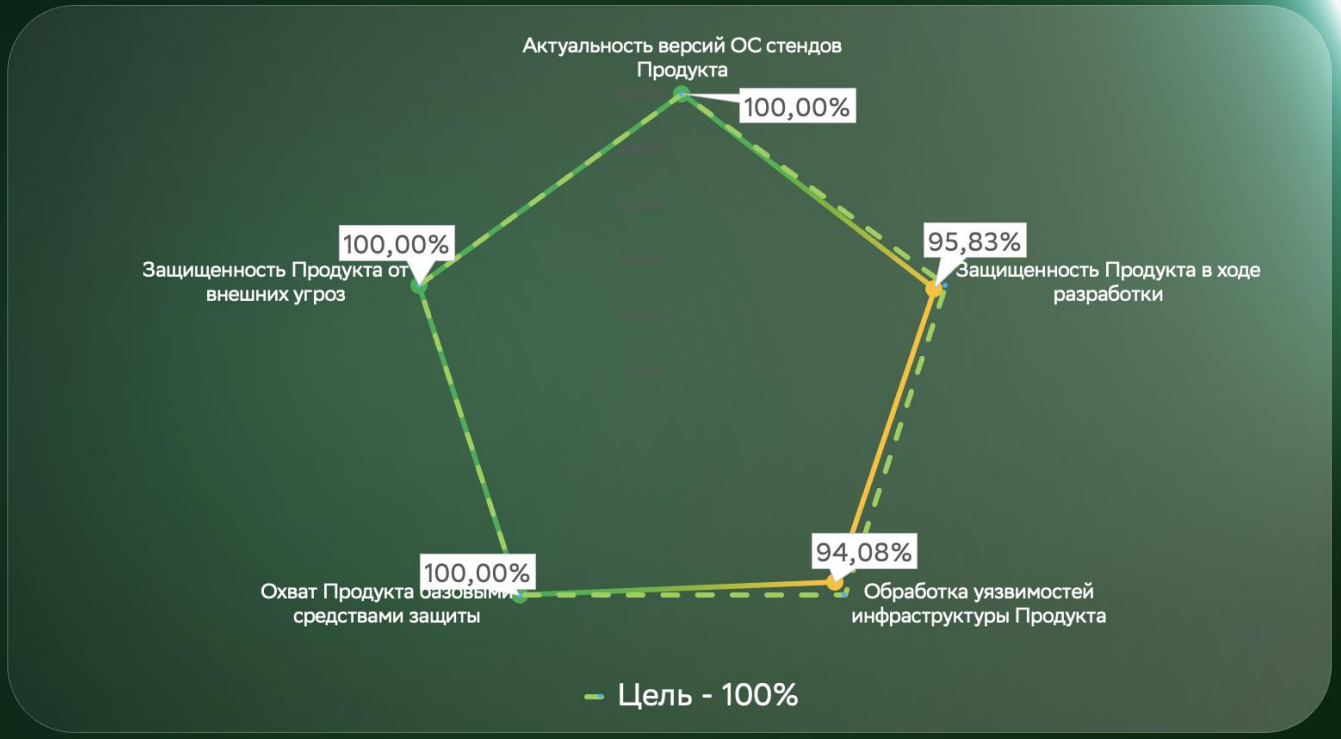


СБЕР 2В

Пример. Run-метрики в Бизнес





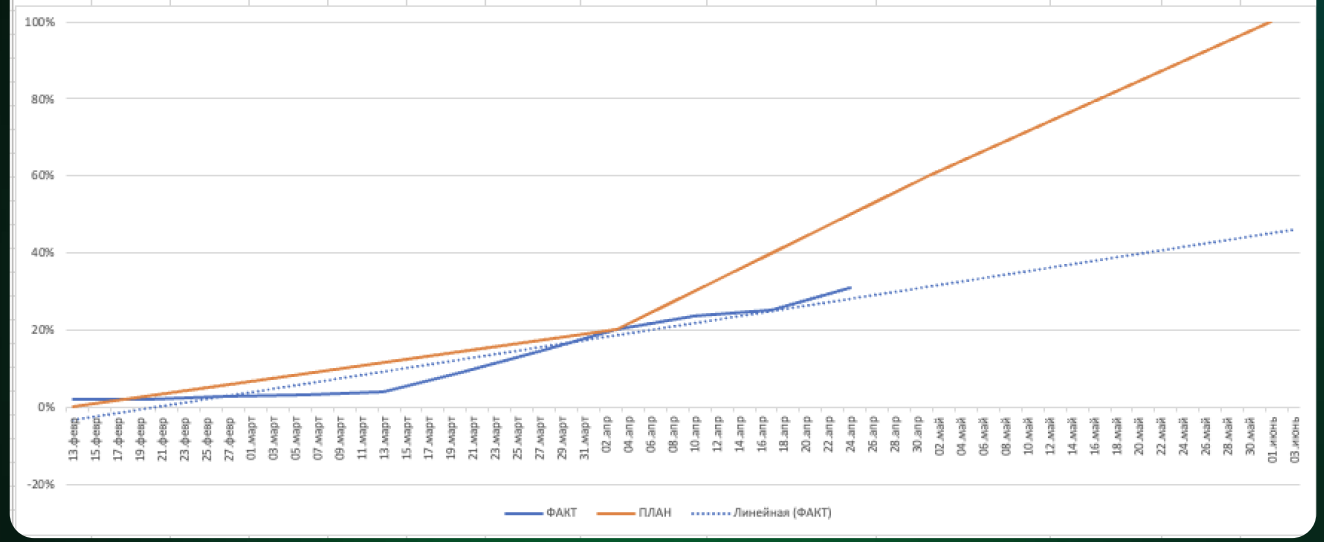


Актуальные данные ищи в FineBI

СБЕР 2В

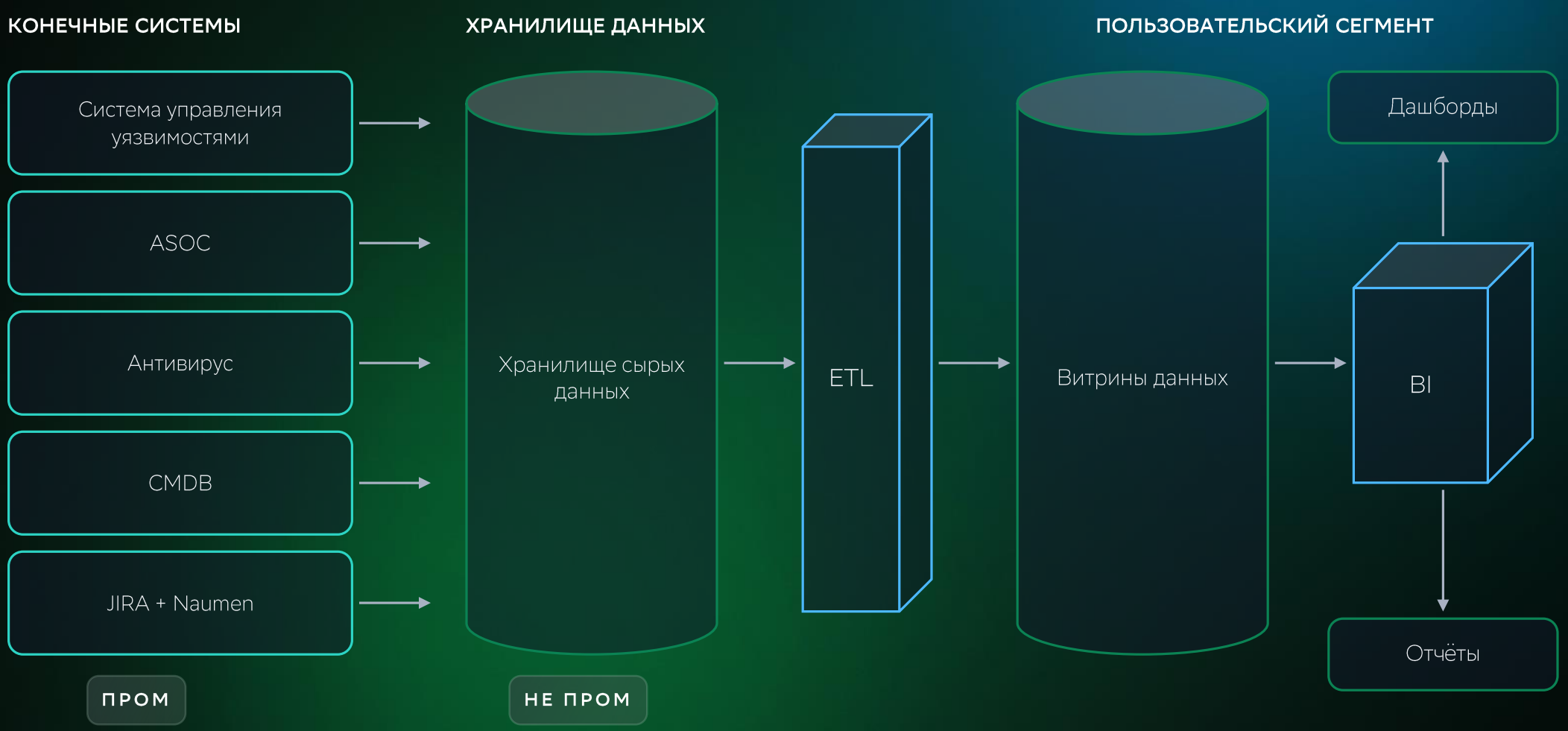
Пример: Как начать мерить Change

Дата	Всего доменов	As is	За VPN	За WL	Удалено	В публичном доступе	Отправлена заявка в BI.Zone	Подготовлен профиль	Тестирование	Переведен за WAF	ФАКТ	ПЛАН
13.февр	368	0	0	0	0	368	60	2	15	7	2%	0%
20.февр	368	0	0	0	0	368	0	4	73	7	2%	
27.февр	368	0	0	0	0	368	0	4	69	11	3%	
06.март	368	0	0	0	0	368	6	2	70	12	3%	
13.март	368	0	0	0	0	368	0	4	71	15	4%	
20.март	368	0	0	0	0	368	0	4	53	33	9%	
27.март	368	0	0	0	1	367	7	3	34	53	14%	
03.апр	368	0	0	0	5	363	0	0	29	73	20%	20%
10.апр	368	0	0	0	20	348	0	0	20	82	24%	
17.апр	368	0	0	0	23	345	1	0	15	87	25%	
24.апр	368	26	0	0	56	286	7	0	37	89	31%	
01.май												60%
08.май												
15.май												
22.май												
29.май												
01.июнь												100%



СБЕР 2В

Техническая архитектура системы аналитики



СБЕР 2В

Готов ответить на вопросы



Иван Дмитриев
Директор по кибербезопасности
группы компаний Сбер2В