СБЕР КОРУС

От нуля к единице

Как мы совершили «прыжок» в зрелости кибербезопасности

Обо мне

Иван Дмитриев

Заместитель генерального директора
по информационной безопасности – директор
дирекции по безопасности

- 15 лет в ИБ
- MBA Стратегический менеджмент
- Сертифицированный аудитор

@idmitriev

Dmitriev.iv@esphere.ru

СБЕР КОРУС

СберКорус - разработчик цифровых продуктов и сервисов, которые создают комфортную среду для ведения и развития бизнеса

37
компаний из списка Forbes «200 крупнейших компаний России» работают с нами

1 млн+
клиентов пользуются нашими сервисами

6000
Элементов серверной инфрастуктуры

200+
Интеграций с информационными системами Банка и клиентов

Немного истории

Мы ваш недуг в подвиг обратим:

Решили строить процессы, а не копить артефакты

Май 2022

Инцидент кибербезопасности

Ноябрь 2023

Ликвидированы последствия инцидента. Подготовлена стратегия Безопасности

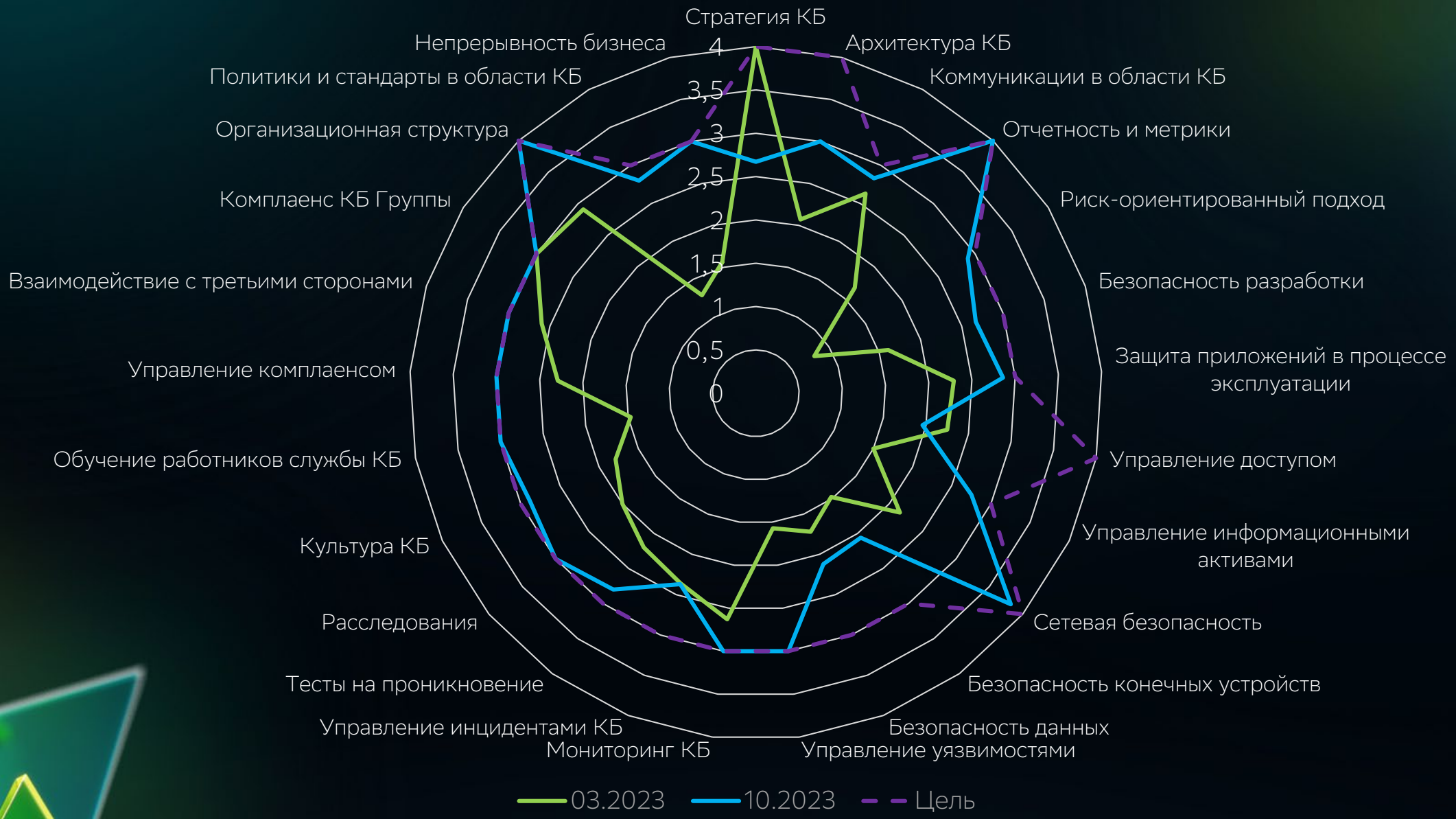
Февраль 2023

СберКорус признан «Фокусным» ДЗО. Стратегия Меняетс

Октябрь 2023

Выход в «Зеленую» зону уровня зрелости КБ. Очередная смена стратегии

СБЕР КОРУС

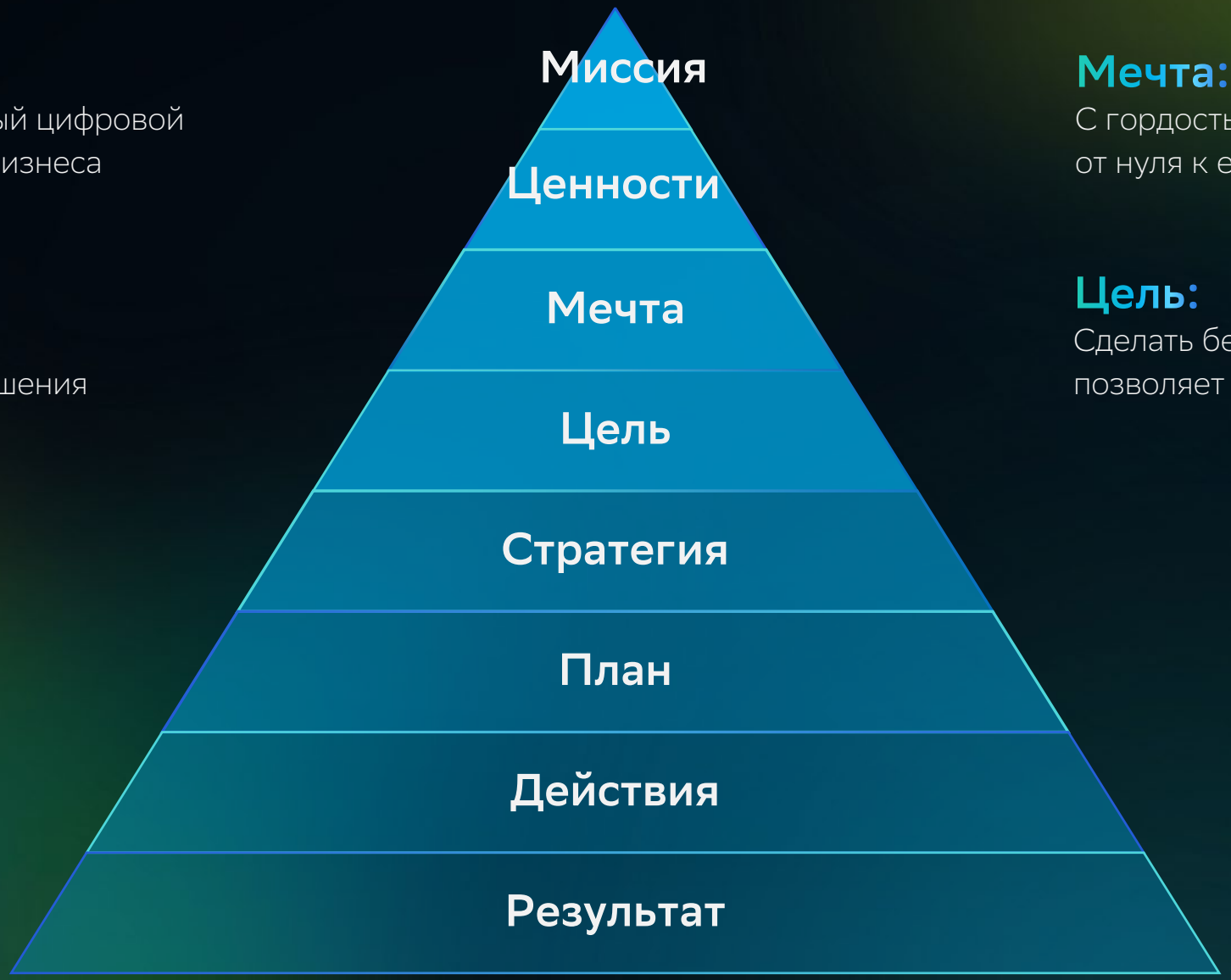

Стратегия КБ
Архитектура КБ
Коммуникации в области КБ
Отчетность и метрики
Риск-ориентированный подход
Безопасность разработки
Защита приложений в процессе эксплуатации
Управление доступом
Управление информационными активами
Сетевая безопасность
Безопасность конечных устройств
Безопасность данных
Управление уязвимостями
Мониторинг КБ
Управление инцидентами КБ
Тесты на проникновение
Расследования
Культура КБ
Обучение работников службы КБ
Управление комплаенсом
Взаимодействие с третьими сторонами
Комплаенс КБ Группы
Организационная структура
Политики и стандарты в области КБ
Непрерывность бизнеса
4
3,5
3
2,5
2
1,5
1
0,5
0
03.2023
10.2023
Цель

СБЕР КОРУС

Пирамида результата

Миссия:
Мы создаем удобный цифровой мир для развития бизнеса

Ценности:
Клиент. Команда.
Непрерывные улучшения



Мечта:
С гордостью рассказать о прыжке от нуля к единице

Цель:
Сделать безопасность, которая позволяет бизнесу развиваться

СБЕР КОРУС

Стратегия и целеполагание (ЧТО?)

Минимальные риски для Банка и компаний экосистемы – Корус компания первого выбора для экосистемы.

Оптимизация расходов на безопасность.

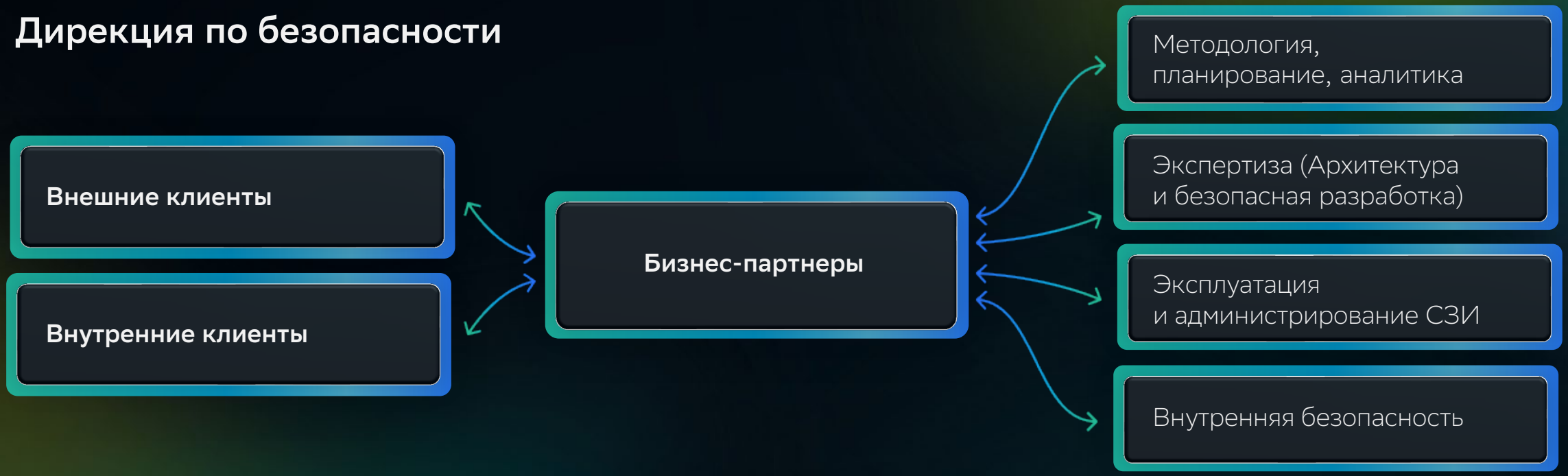
Нулевые потери от инцидентов

Безопасность продукта – конкурентное преимущество компании

СБЕР КОРУС

«Сначала КТО, затем ЧЕМ»

Дирекция по безопасности

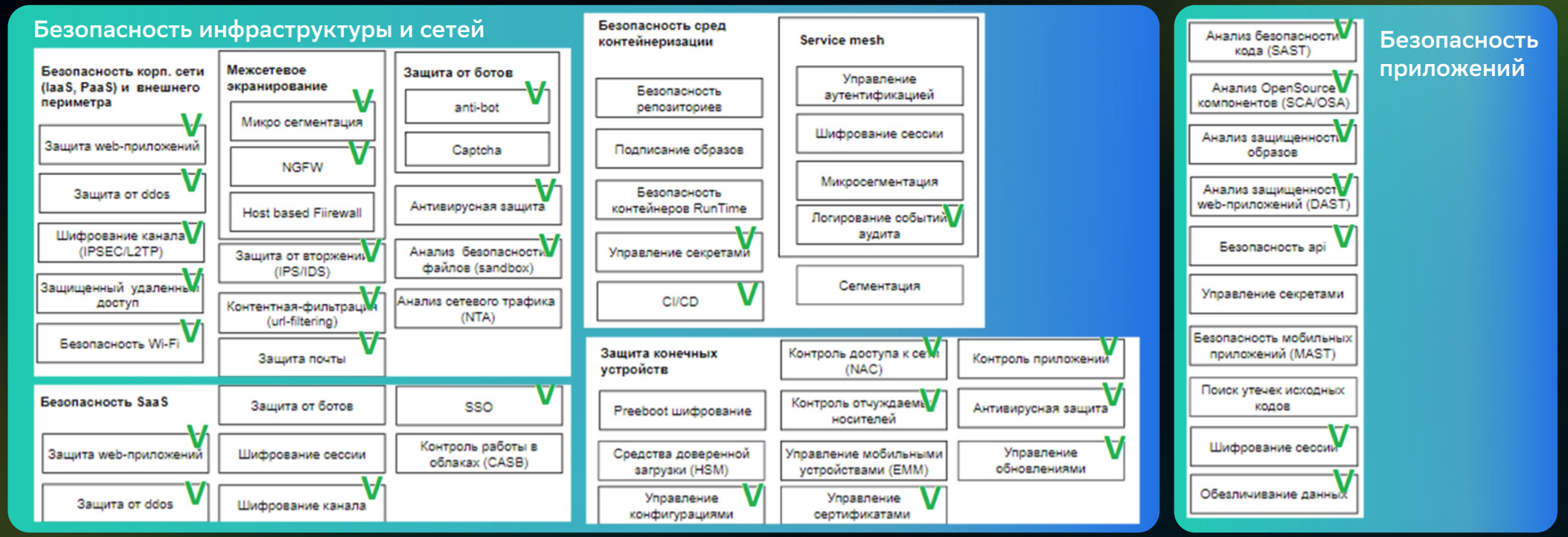


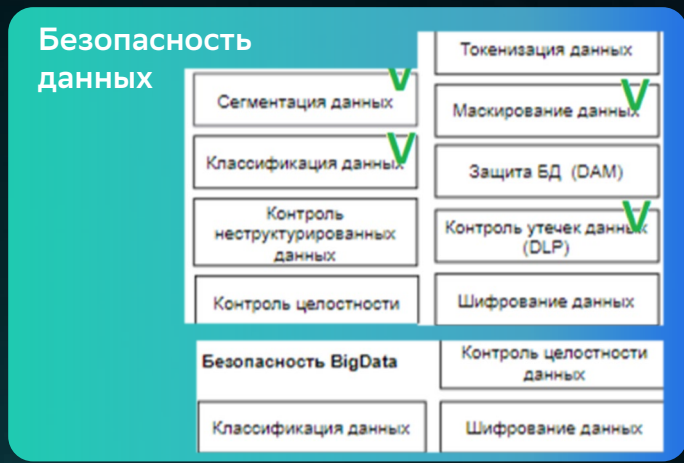
Основные принципы

1. Несоответствие профилю позиции по софт-скиллам и ценностям критично
2. Прозрачная мотивация и целеполагание
3. Специализация со взаимозамещением
4. Лидеры направлений
5. Делегирование
6. Обратная связь и поощрение чемпионов

СБЕР КОРУС

ЧЕМ?

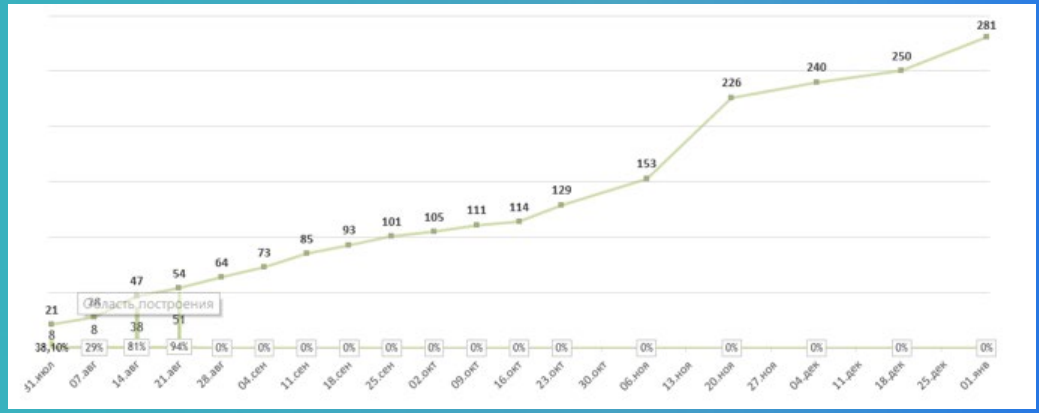




СБЕР КОРУС

План и действия (КАК?)

Вопрос 2. Для основных процессов КБ определены метрики.	ДА	Да, в компании определен ряд фокусных метрик по КБ. Отчетность по данным метрикам предоставляется CEO и CEO-1, а также BP Банка еженедельно.



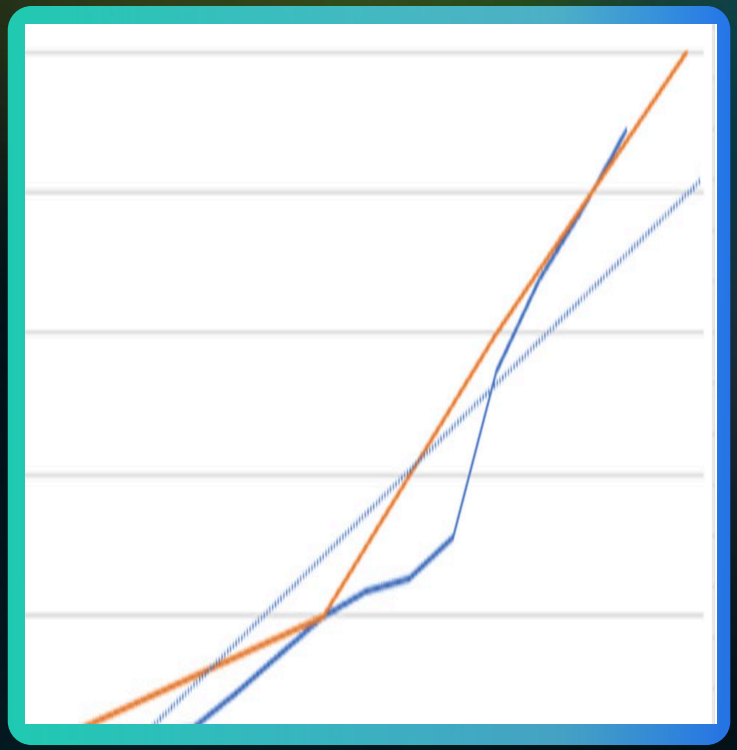
Основные принципы

1. Контроль != ответственность и авторитарные указания
2. Разделение ЛНА, рабочих документов и гайдов
3. Смежники справа-слева тоже команда, они имеют доступ ко всей информации и тоже профессионалы
4. Взаимная подотчетность
5. Непрерывные измерения
6. Открытость в признании факапов

СБЕР КОРУС

Пример измеримости достижения результата

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
368	0	0	0	0	368	60	2	15	7	2%	0%
368	0	0	0	0	368	0	4	73	7	2%	
368	0	0	0	0	368	0	4	69	11	3%	
368	0	0	0	0	368	6	2	70	12	3%	
368	0	0	0	0	368	0	4	71	15	4%	
368	0	0	0	0	368	0	4	53	33	9%	
368	0	0	0	1	367	7	3	34	53	14%	
368	0	0	0	5	363	0	0	29	73	20%	20%
368	0	0	0	20	348	0	0	20	82	24%	
368	0	0	0	23	345	1	0	15	87	25%	
368	26	0	0	56	286	7	0	37	89	31%	
372	31	0	0	136	205	16	0	23	112	55%	60%
373	34	0	0	155	184	14	0	13	124	67%	
373	34	0	18	156	165	12	0	10	128	78%	
373	34	0	33	153	153	0	0	12	136	89%	
											100 %



СБЕР КОРУС

СБЕР КОРУС

Q&A

Иван Дмитриев

Заместитель генерального директора
по информационной безопасности

@idmitriev