SOC
FORUM
2023

Строим SOC «с нуля» в условиях ограниченного бюджета

SOC
FORUM
2023

Орлова Вера

ООО «Русагро технологии»

Несколько слов о группе компаний «Русагро»

Русагро – один из крупнейших агрохолдингов

SOC FORUM 2023

С 2021 года «Русагро Технологии» разрабатывают и внедряют ИТ-продукты для головной компании, помогая строить экосистему цифровых сервисов.

4 **Основных бизнес-направления**

- Сахар
- Сельское хозяйство
- Мясо
- Масла и жиры

Более 20 000 сотрудников

№2 Среди производителей масла России

№3 Среди производителей живка и сахара России

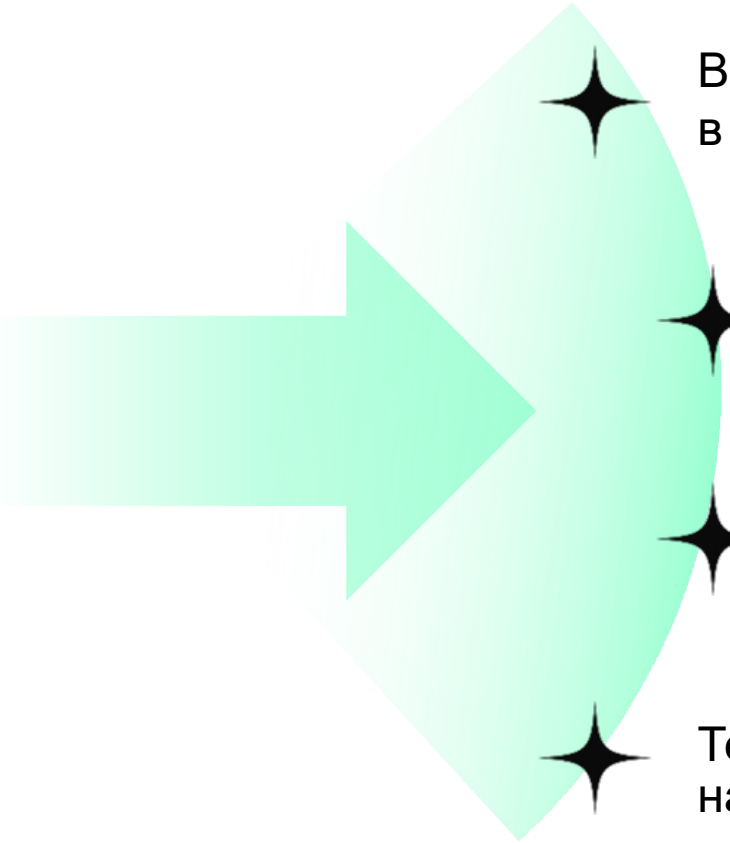
№4 По размеру земельного фонда России

Зачем нам SOC?

Зачем нам SOC?

SOC FORUM 2023

- Рост количества киберугроз
- Отсутствие понимание происходящего в ИТ-инфраструктуре
- Ускорение динамики изменений (рост бизнес-процессов, рост ИТ инфраструктуры, развитие приложений)



- Видеть наиболее критичные события в инфраструктуре
- Выявлять среди них потенциальные инциденты ИБ
- Осуществлять менеджмент инцидентов ИБ
- Тестировать инфраструктуру на наличие критичных уязвимостей

SOC «In House» vs MSSP

SOC FORUM 2023

6

Основных причин в пользу своего SOC

SOC “In House”

Преимущества

SOC FORUM 2023

Независимость

В случае MSSP при отказе от внешнего сервиса или необходимости перехода в другой SOC придется начинать всё «с нуля»

Инвестиции

Вложенные деньги инвестируются в развитие своей инфраструктуры и компетенций

Адаптация

Сервис и контент (сценарии выявления инцидентов и реагирования) адаптирован под нужды организации

Мотивация

Гибкие возможности для мотивации сотрудников SOC, что позволяет избежать формального отношения к отработке инцидентов

Знания инфраструктуры

Аналитики внутреннего SOC, с учетом более глубоких знаний инфраструктуры, имеют преимущество в скорости и корректности отработки инцидентов ИБ

Экономическая целесообразность

В долгосрочной перспективе внутренний SOC может быть даже дешевле коммерческого.

SOC «In House»

Эффект от внедрения

SOC FORUM 2023

Очевидное

- Не быть «на крючке» у MSSP-провайдеров
- Развитие собственной инфраструктуры
- Адаптированный корреляционный контент
- Знание инфраструктуры

Неочевидное

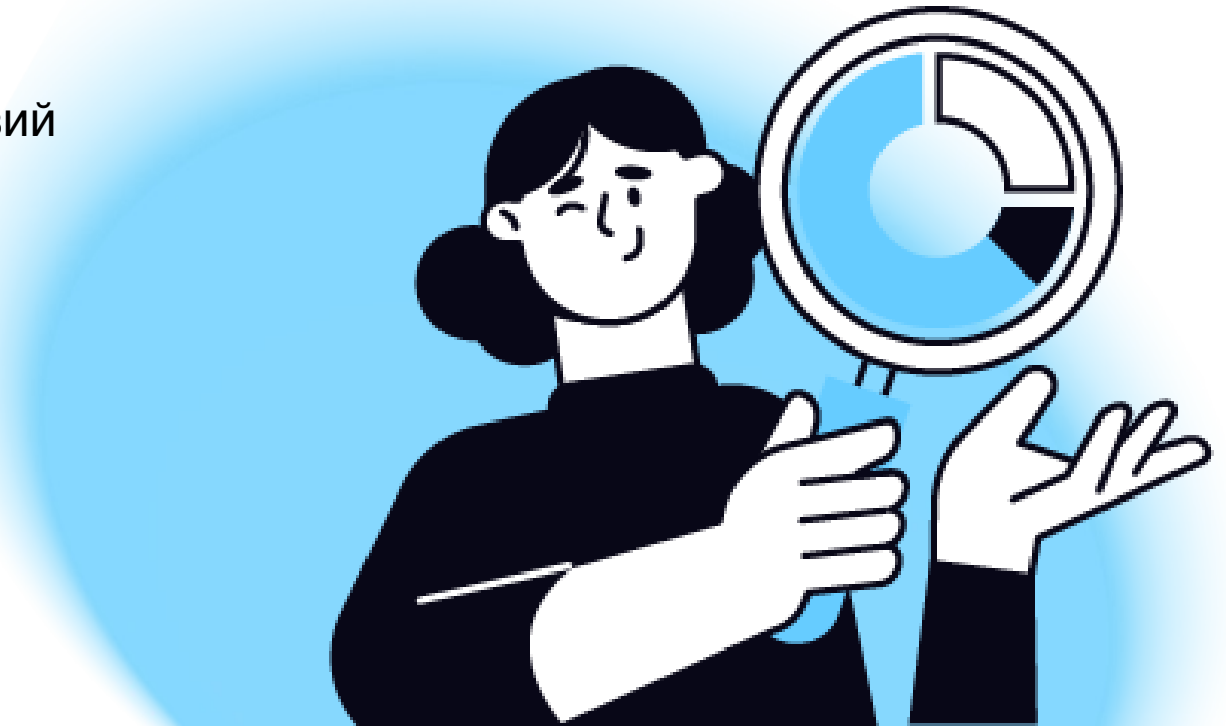
- Развитие инфраструктуры
- Развитие компетенций
- Возможность отработки нестандартных запросов
- Безопасность

Всё классно.
Но как сделать дешевле?

Что мы предприняли для снижения стоимости SOC?

SOC FORUM 2023

- Наняли сотрудников в регионах на удаленную работу
- Частично закрыли потребности в круглосуточном мониторинге за счет внешнего L3
- Отдали функцию по расследованию сложных инцидентов (L3) и Threat Hunting на аутсорсинг
- Передали часть функций по реагированию и расследованию инцидентов на других профильных сотрудников ИБ
- Подход поэтапного наращивания мощностей и расширения лицензий SIEM



На чем мы не экономим и вам не советуем!

SOC FORUM 2023

- Качественное программное обеспечение
- Внедрение специализированного ПО профессионалами
- Обучение сотрудников SOC. Киберучения.

Непрерывное развитие

SOC FORUM 2023

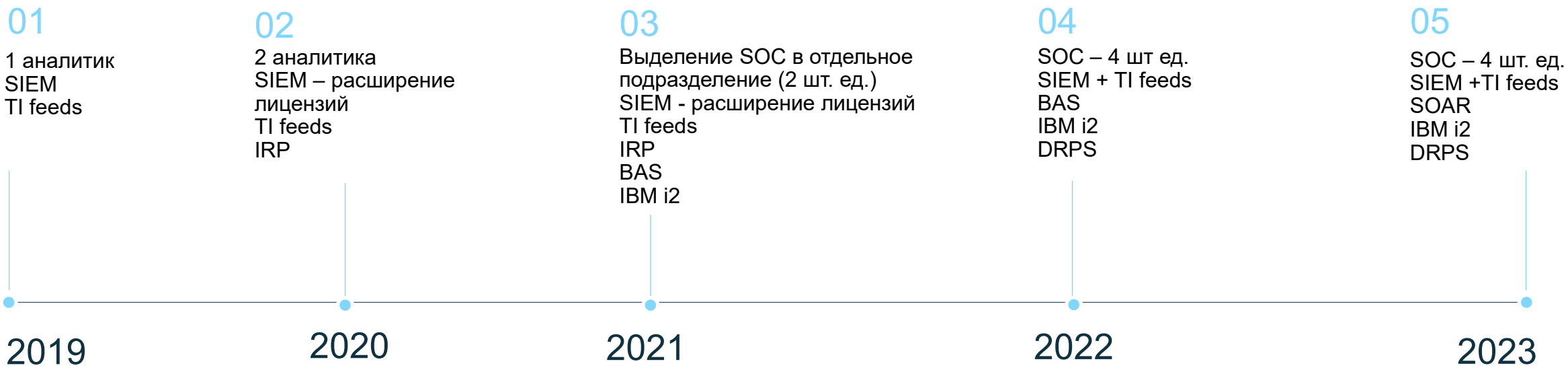
4

Года продуктивной работы SOC

Этапы развития SOC «Русагро»

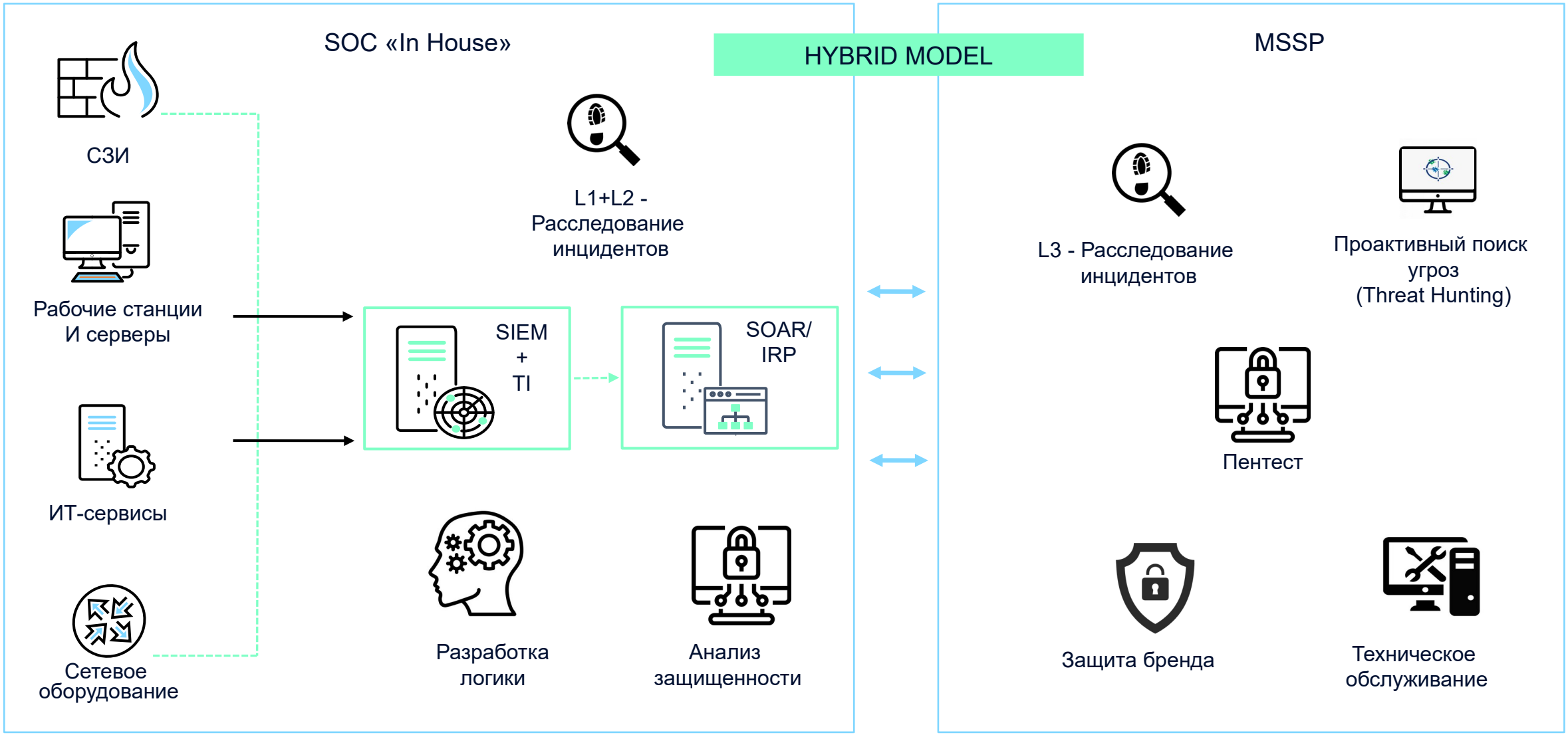
SOC FORUM 2023

Технологический стек



Принцип – взять лучшее из каждой модели

SOC FORUM 2023



SOC «Русагро» сегодня

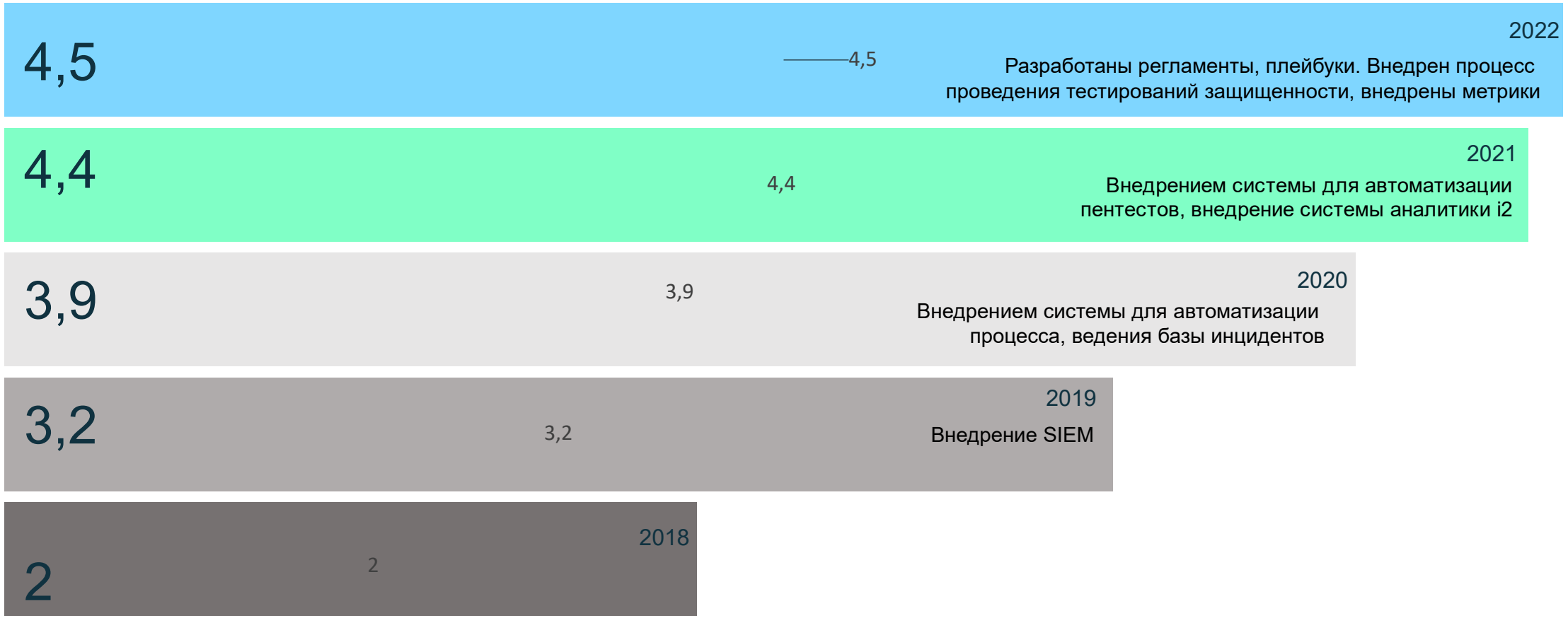
SOC FORUM 2023

- Выстроенный и работающий процесс управления инцидентами ИБ
- Разработанные сопутствующие регламенты и документы
- Развитые компетенции специалистов, позволяющие самостоятельно расследовать инциденты ИБ на уровне не ниже L3, подключать источники и формировать правила корреляции
- Threat Hunting
- Опыт выстраивания процесса тестирования защищенности (BAS-решение + внешний подрядчик)
- Выстроен процесс взаимодействия с ТОП-менеджментов по вопросам инцидентов ИБ
- Выстроен процесс отработки запросов от ИТ и бизнеса (регулярные обращения с различными запросами, помимо инцидентов ИБ)
- Внедрены метрики эффективности процессов SOC

Оценка зрелости процессов управления инцидентами по модели CMMI*

SOC FORUM 2023

Динамика изменения показателей зрелости



* - Цель **модели CMMI** заключается в оценке зрелости процессов организации и предоставлении рекомендаций по улучшению процессов

Статистика и ключевые показатели SOC сегодня

SOC FORUM 2023

4000

Подозрений на инцидент ИБ
за год обрабатывается SOC

70

Подтвержденных инцидента выявлено
SOC в 1м квартале 2023 года

96%

Подозрений закрываются на стороне SOC,
остальные 4% направляются на дальнейшую
проработку

1100

Источников отправляют логи в SIEM
Охват мониторингом:
97% - обеспечивающая инфраструктура,
80% - СЗИ,
78% - Шлюзы (Proxy, терминальные, VPN)

400

Работающих правил корреляции

85%

Направленных на проработку подозрений
закрываются как подтвержденный
инцидент ИБ

Практические кейсы SOC

SOC FORUM 2023

Реальные кейсы, в которых:
- мы убедились в эффективности нашего подхода с аутсорсингом L3
- SOC оказался полезен инфраструктуре

1. Атака на цепочку поставок

Что произошло:
- ИТ-контрагент, взломанный 2-3 дня назад;
- Около 70 УЗ в домене ГК Русагро, в т.ч. администраторские;

Что предприняли:
- Подключена L3 подрядчика;
- Разделены задачи по аналитике и реагированию;

Итог:
- Общее время выполнения задачи сокращено в три раза;
- Проведены все необходимые работы, направленные на обеспечение безопасности УЗ подрядчика

2. Ошибки администрирования

Что произошло:
- Выявлено массовое изменение 587 УЗ подрядчиков в части срока их действия

Что предприняли:
- Проведена аналитика по причинам блокировки
- Выявлена корневая причина

Итог:
- Выставлены корректные сроки действия УЗ подрядчиков;
- Предотвращен потенциальный простой сотрудников подрядных организаций и сопутствующие издержки

За 4 года SOC выявлял:

- Компрометации УЗ
- Недокументированные возможности ПО
- Невылеченные вирусные заражения
- Атаки вследствие некорректных настроек оборудования
- Атаки с использовнием социальной инженерии (фишинг, спуфинг)
- Утечки конфиденциальных данных
- СПАМ-рассылки с ящиков сотрудников

и прочее…

SOC FORUM 2023

32% экономии

Стоимость сопровождения внутреннего SOC “Русагро” (в год)

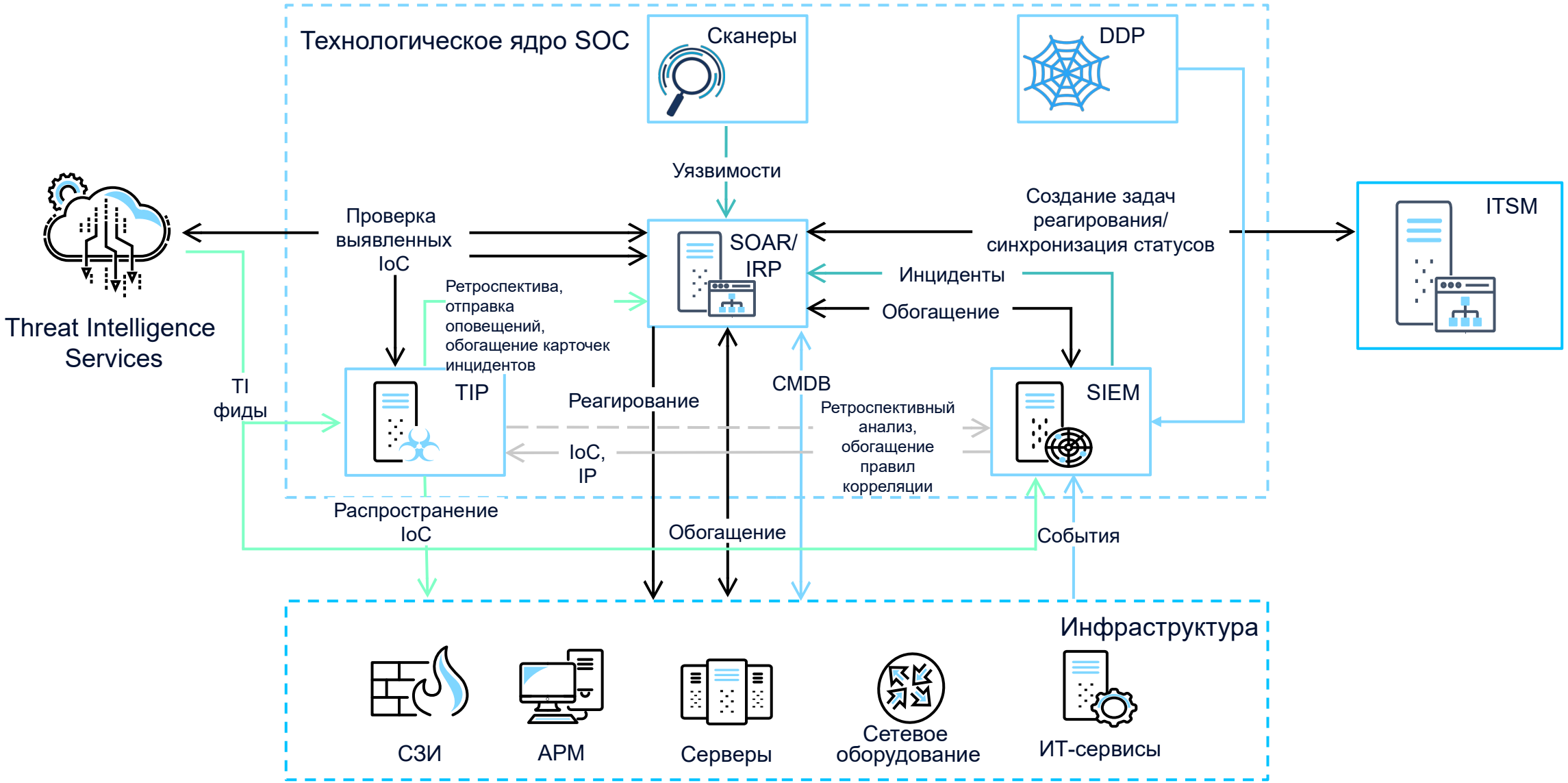
Стоимость внешнего сервиса SOC (MSSP) (в год)

- Экономическая выгода при сопровождении собственного SOC относительно MSSP
- Экономия при обслуживании 24*7 с частичным закрытием потребности за счет внешних L3 и технического обслуживания (при штате 6 чел.+ руководитель)

Что дальше?

Планы на развитие

SOC FORUM 2023



Дважды-опыт внедрения SOAR

Внедряем SOAR Русагро

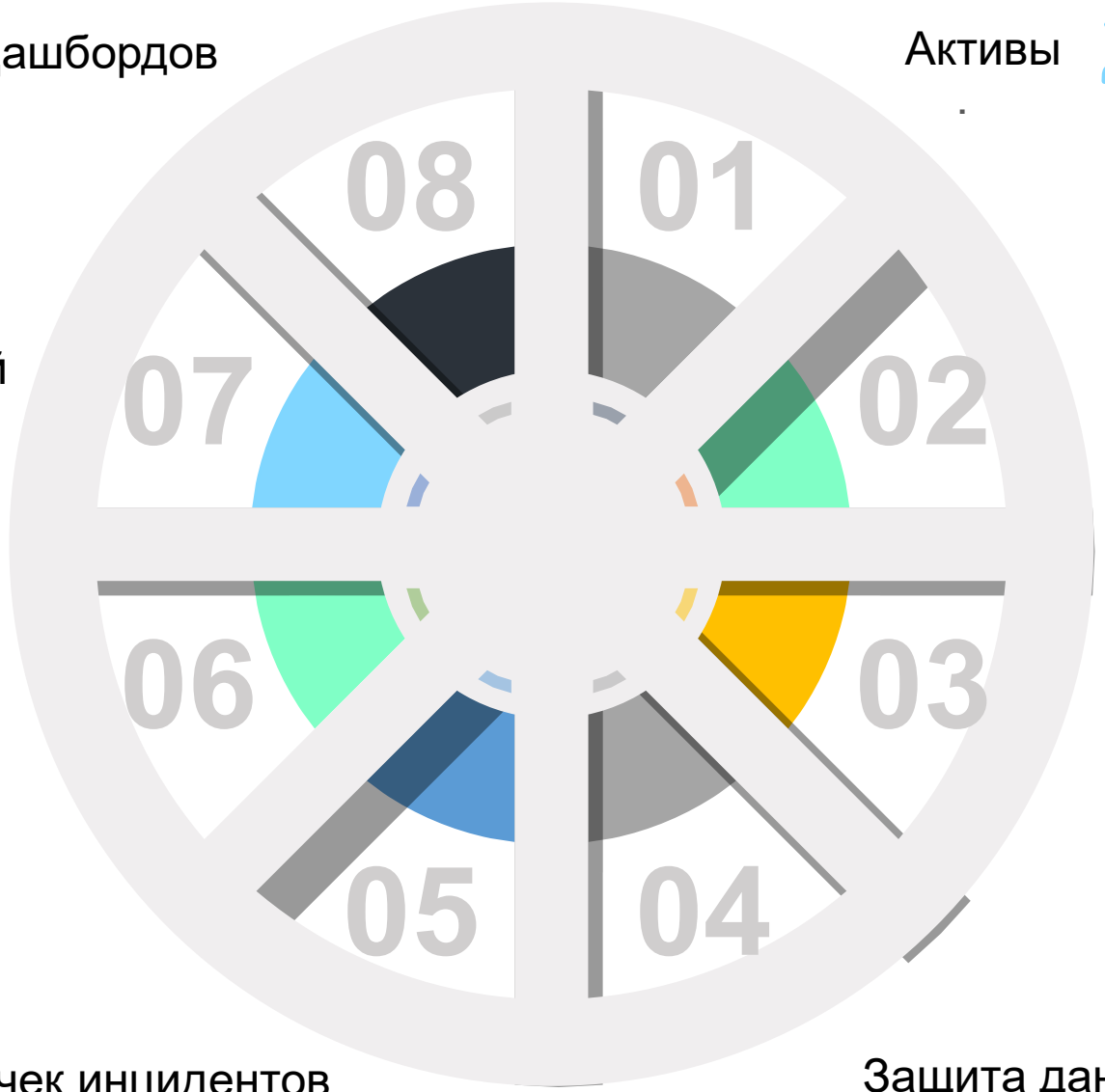
SOC FORUM 2023

18 Отчетов и Дашбордов

18 Интеграций

15 Playbooks

15 типов карточек инцидентов



Активы

SLA

5+ скриптов реагирования

Защита данных

Дважды-опыт внедрения SOAR

Работа над ошибками

SOC FORUM 2023

Сбор активов

Автоматизированный сбор и идентификация активов существенно сокращает время на понимание уровня критичности инцидента ИБ. Как правило, это дополнительный модуль, за который имеет смысл заплатить.

Избыточная информация в карточке инцидента

Слишком подробное заполнение карточки увеличивает время на обработку инцидента, не приносит существенной пользы, вызывает негатив у аналитиков.

Продуманная защита SOAR-системы

Подтверждение второй рукой операций по реагированию, двухфакторная аутентификация, защита базы данных.

Частичная автоматизация реагирования

Существенно сокращает время на отработку инцидента, снижая воздействие человеческого фактора.

Непрерывное развитие

SOC FORUM 2023

3

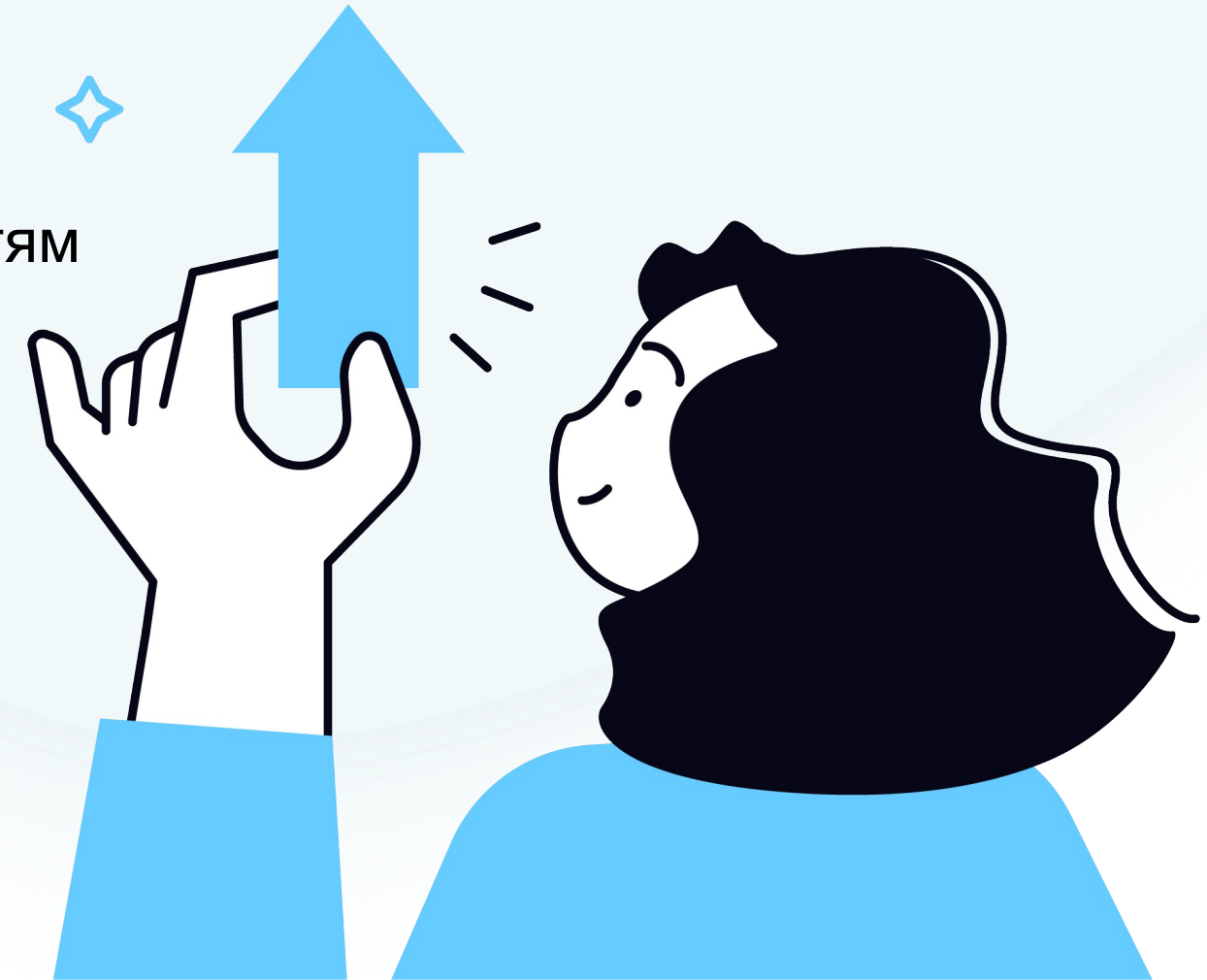
Основных вывода

SOC FORUM 2023

Лучшая инвестиция –
это инвестиция в себя!

Есть слона нужно по частям

Ищите баланс!



СПАСИБО
ЗА ВНИМАНИЕ!

Орлова Вера

ООО «Русагро технологии»
VA.Orlova@rusagro.tech