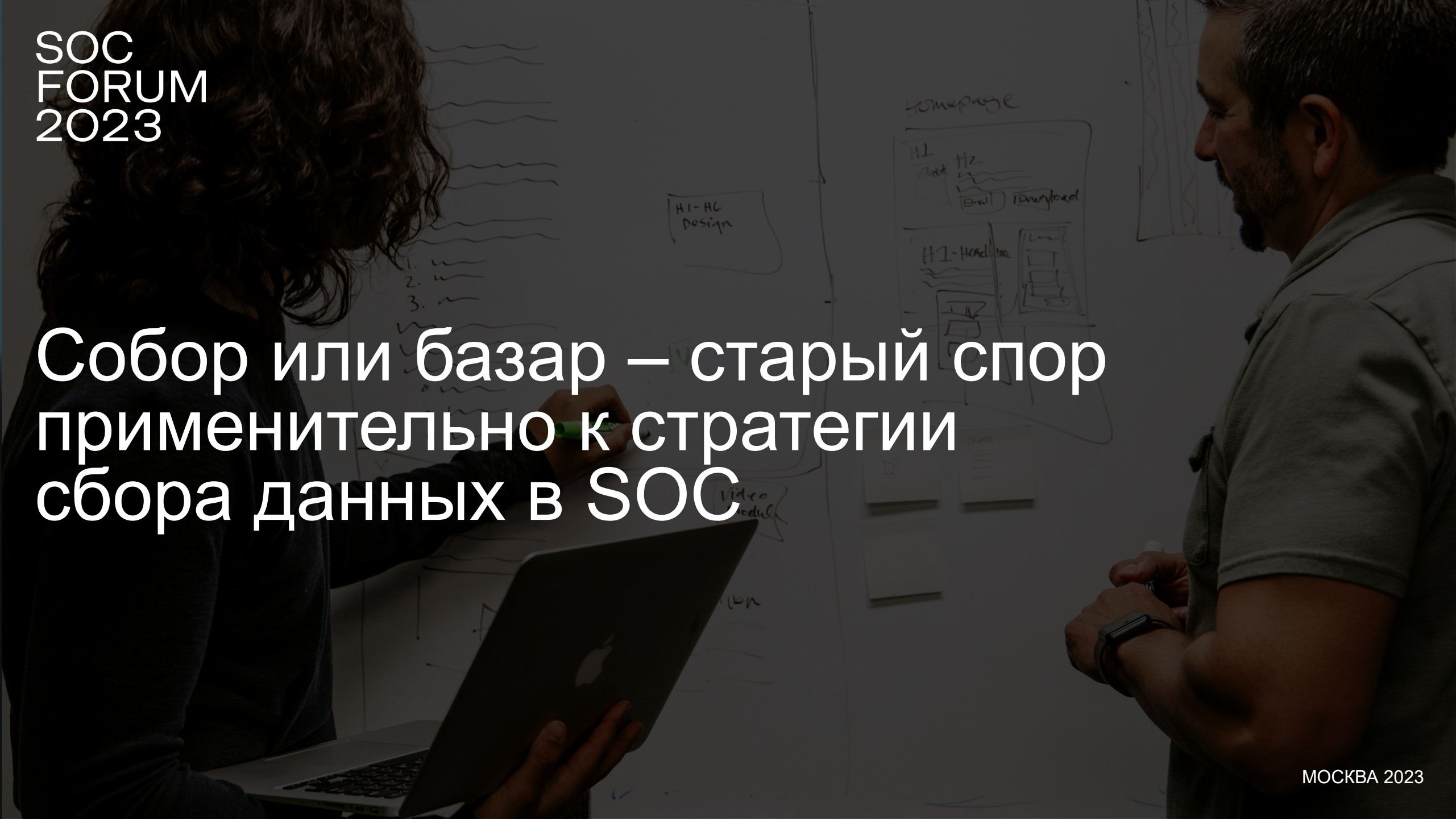
SOC
FORUM
2023



Собор или базар – старый спор применительно к стратегии сбора данных в SOC

МОСКВА 2023

SOC
FORUM
2023

РУСЛАН ИВАНОВ

Независимый эксперт

Собор или базар* ?

какую стратегию сбора данных в территориально распределенной организации выбрать

- Эрик Рэймонд
  http://www.catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/

О чем мы НЕ будем сегодня говорить?

SOC FORUM 2023

Мы не будем обсуждать, что и как собирать

Наша цель – выбрать стратегию сбора, обработки и хранения данных телеметрии в территориально распределенной организации на основе анализа технических и экономических параметров

LOG SOURCES	VOLUME[11]	IOC MATCHING	THREAT HUNTING	AUDIT TRIAL[9]	APT DETECTION[10]
Antivirus	Low	-	++[3]	+	+++
Windows&Sysmon	Medium[8]	++[1]	+++[4]	++	++
Proxy	Medium	++[2]	+[5]	++	+
NIDS / NSM[7]	Medium	+	+	+	+
DNS	High	++[2]	+[5]	+	+
Mall[6]	Medium	+	-	+	-
Firewall	High	+[2]	-	++	-
Linux (auditd)	Medium	-	+	+	-

Приоритет

ВЫСОКИЙ

НИЗКИЙ

1. Hash-MD5, SHA1, SHA256
2. C2 IP-адреса и домены
3. Antivirus Event Analysis Cheat Sheet, @cyb3rops
4. Sigma правила
5. Подозрительные TLD и UserAgent
6. Эффективен при использовании T1 feeds
7. Suricata/Zeek или коммерческие Anti-APT, NTA
8. Напрямую зависит от политики (MS baseline and sysmon-modular)
9. Польза в реконструкции инцидентов
10. Польза в реконструкции продвинутых TTP
11. Напрямую зависит от политик и фильтров

*Источник: Twitter эксперта по кибербезопасности Флориана Рота (Florian Roth) в переводе Данилы Луцива, Security Vision.

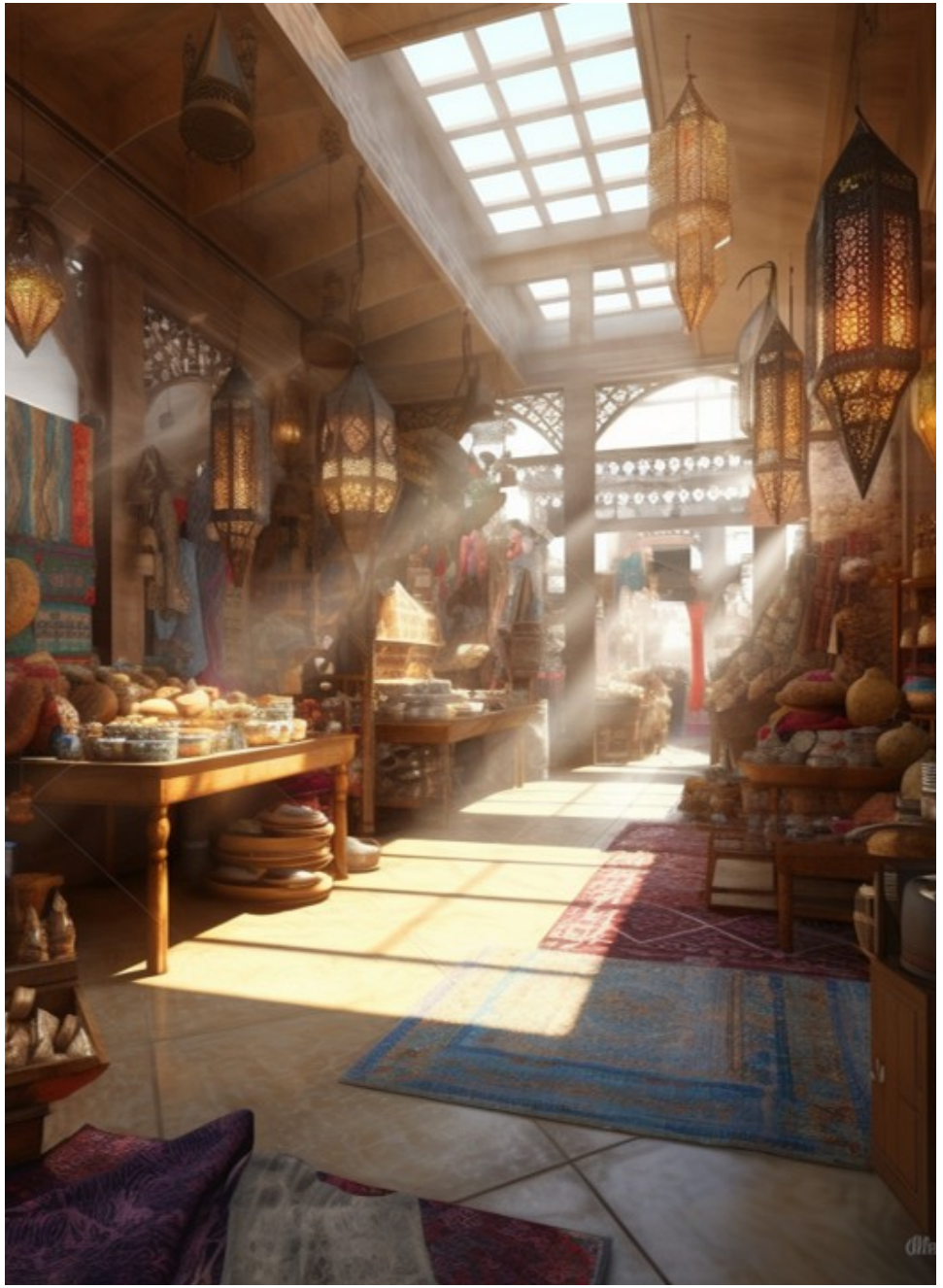
Централизованная модель сбора «Собор»

SOC FORUM 2023

- ПОЛНОСТЬЮ ЦЕНТРАЛИЗОВАННЫЕ СБОР И ОБРАБОТКА
- ВЫСОКИЕ ТРЕБОВАНИЯ К НАДЕЖНОСТИ И ХАРАКТЕРИСТИКАМ КАНАЛОВ
- ВСЕ ХРАНЕНИЕ (И ГОРЯЧЕЕ, И ХОЛОДНОЕ) В ЦЕНТРЕ
- ПРЕДСКАЗУЕМАЯ РАБОТА В СЛУЧАЕ АВАРИЙ
- НА ПЕРВЫЙ ВЗГЛЯД ДЕШЕВЛЕ РАСПРЕДЕЛЕННОЙ МОДЕЛИ

Распределенная модель сбора «Базар»

- РАСПРЕДЕЛЕННЫЙ СБОР И ОБРАБОТКА
- ТРЕБОВАНИЯ К КАНАЛАМ МЕНЬШЕ
- НЕОБХОДИМО ОБОРУДОВАНИЕ В ПРОМЕЖУТОЧНЫХ УЗЛАХ
- РАСПРЕДЕЛЕННОЕ ХРАНЕНИЕ
- НЕОЧЕВИДНОЕ ПОВЕДЕНИЕ ПРИ СБОЯХ
- НА ПЕРВЫЙ ВЗГЛЯД ДОРОЖЕ ЦЕНТРАЛИЗОВАННОЙ МОДЕЛИ



Почему вообще встает вопрос сравнения этих стратегий?

SOC FORUM 2023

На самом деле выбор стратегии не так прост, как кажется, особенно если рассматривать все в комплексе:

По первоначальным вложениям централизованная стратегия на первый взгляд дешевле

На длинной дистанции ответ не всегда очевиден

Почему вообще встает вопрос сравнения этих стратегий?

SOC FORUM 2023

«Правильного» ответа нет, и он может меняться со временем:

Может зависеть от оргструктуры компании

Точно зависит от распределения наблюдаемых объектов

Может зависеть от местоположения наблюдающих субъектов

Зависит от требований к отказоустойчивости и сохранности собираемой телеметрии в случае аварий

Деньги, деньги, дребеденьги – остальное суета!

ДЛЯ НЕБОЛЬШИХ КОМПАНИЙ

централизованная схема сбора является обычно самой выгодной с экономической точки зрения

ДЛЯ КОМПАНИЙ ПОБОЛЬШЕ

до 30–40 тысяч EPS в сумме на весь мониторинг

скорее всего, будет принято решение о централизованном сборе, т. к. точка перегиба с точки зрения экономики решения не достигнута

ДЛЯ КОМПАНИЙ ФЕДЕРАЛЬНОГО УРОВНЯ

сотни тысяч EPS

ответ совсем неоднозначен и зависит от множества вводных

Закон больших чисел (ЗБЧ) в теории вероятностей для ИБ

SOC FORUM 2023

> Чем больше объем выборки / чем чаще проводятся измерения какого-либо параметра, тем выше вероятность, что результаты окажутся близки к ожидаемым (или к неким средним значениям)*.

* Важно помнить, что закон применим только тогда, когда рассматривается большое количество испытаний

SOC
FORUM
2023

Что мы делаем

мы проектируем систему исходя
из анализа средних значений
за какой-то значимый промежуток
времени

Встреча с «черным лебедем»

SOC FORUM 2023

Итак, в нашей системе сбора и анализа событий произошла встреча с «черным лебедем»

Встреча с «черным лебедем»

SOC FORUM 2023

Итак, в нашей системе сбора и анализа событий произошла встреча с «черным лебедем»

БЕЛЫЙ ЛЕБЕДЬ, ВСЕ НОРМАЛЬНО

с точки зрения количества событий не поменялось ничего, и неважно, какая стратегия сбора

Встреча с «черным лебедем»

SOC FORUM 2023

Итак, в нашей системе сбора и анализа событий произошла встреча с «черным лебедем»

БЕЛЫЙ ЛЕБЕДЬ, ВСЕ НОРМАЛЬНО

с точки зрения количества событий не поменялось ничего, и неважно, какая стратегия сбора

Встреча с «черным лебедем»

SOC FORUM 2023

Итак, в нашей системе сбора и анализа событий произошла встреча с «черным лебедем»

БЕЛЫЙ ЛЕБЕДЬ, ВСЕ НОРМАЛЬНО

с точки зрения количества событий не поменялось ничего, и неважно, какая стратегия сбора

ВСТРЕЧА С ТИПИЧНЫМ «ЧЕРНЫМ ЛЕБЕДЕМ»

резко возросло количество событий или часть событий по каким-то причинам стала недоступна или утеряна

Шеф, все пропало!

Итак, у нас инцидент второго типа, и есть разница в том, что мы видим

В СЛУЧАЕ НЕДОСТУПНОСТИ КАНАЛОВ СВЯЗИ:

в случае централизованной системы часть событий просто выпала* или мы получаем неконсистентную информацию

в случае децентрализованной системы часть событий недоступна наблюдателю в центре, но в теории все еще доступна** для post-mortem-анализа

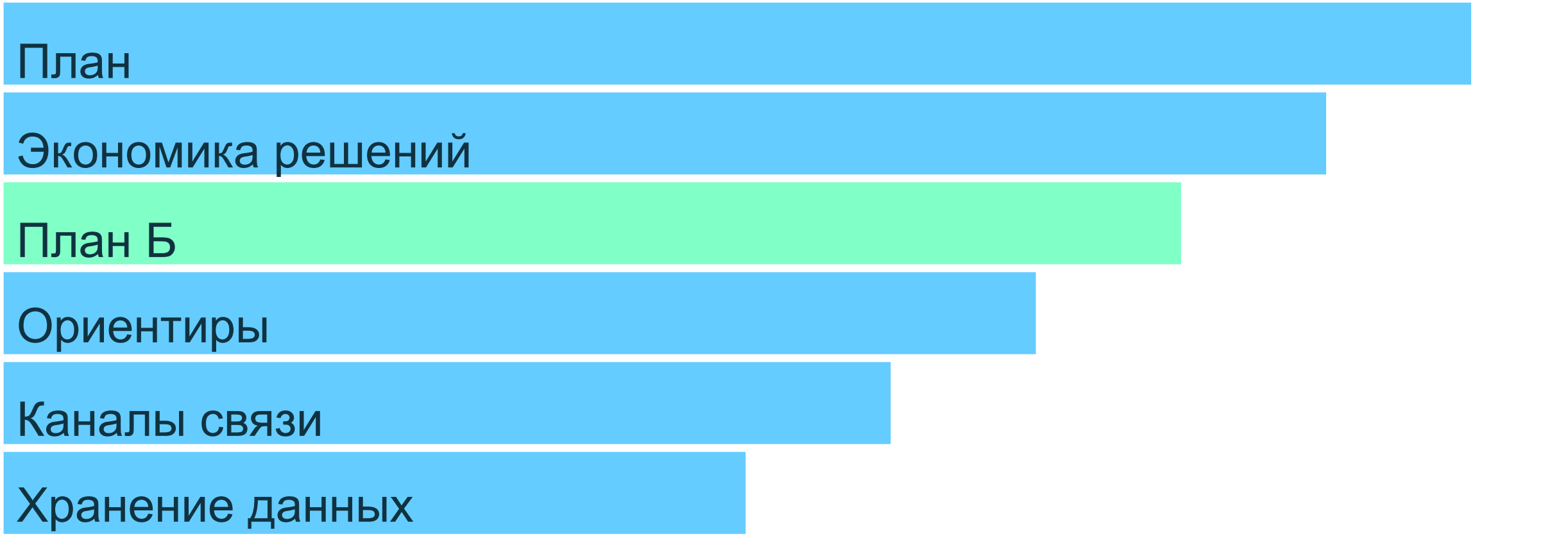
* В теории большинство агентов часть хранят в буфере, но кто из вас может сказать, насколько его хватит?

** Если хватит места на дисках, производительности в изменившихся условиях и система грамотно спроектирована.

SOC к бою готов!

SOC FORUM 2023

Что нужно, чтобы правильно выбрать стратегию сбора?



Что лучше? То, что работает! (ваш К.О.)

SOC FORUM 2023

Ноги, крылья… Главное – хвост! (с)

ЕСЛИ СЕРЬЕЗНО – ТО, ЧТО ПОЗВОЛЯЕТ РЕШИТЬ ЗАДАЧУ ОПТИМАЛЬНЫМ (ИЛИ ХОТЯ БЫ УДОВЛЕТВОРИТЕЛЬНЫМ) ОБРАЗОМ:

- С точки зрения достижения поставленных целей
- Стоимости
- Масштабируемости
- Удобства обслуживания и обновления системы
- Удобства использования
- Отказоустойчивости

В каждом конкретном случае нужно провести инженерную работу – собрать данные о каналах и обслуживаемых системах, проанализировать требования и выбрать наиболее подходящий финансовый вариант.

SOC FORUM 2023

+7 985 761 99 28