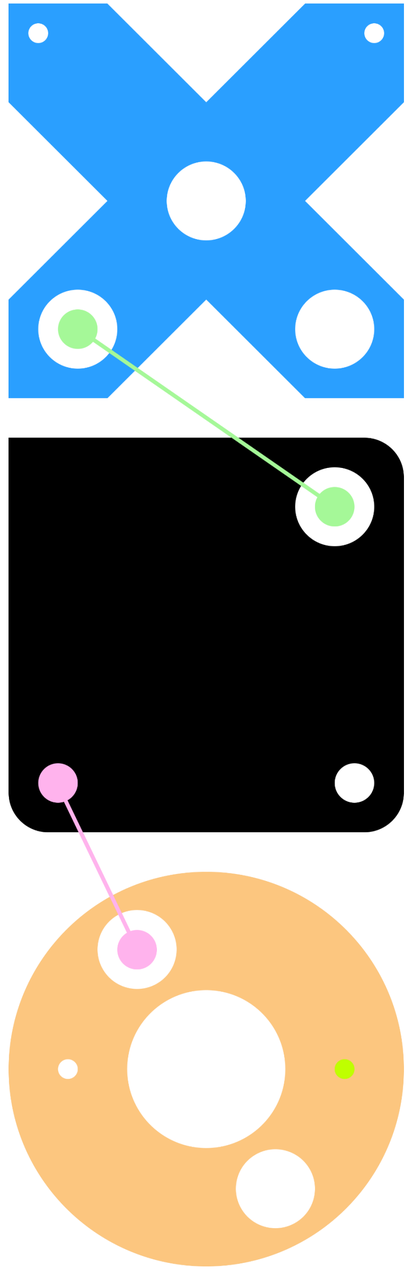
Yandex Cloud × кибердом

# Исследование пользователей SIEM

Security Information and Event Management



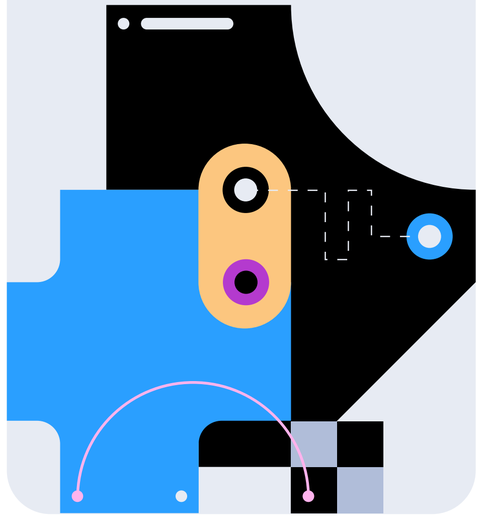
Июнь 2026

# Описание опроса

# Метод и сроки сбора данных

## Метод

Количественный онлайн-опрос



## Размер выборки

- 223 компании

## Целевая аудитория

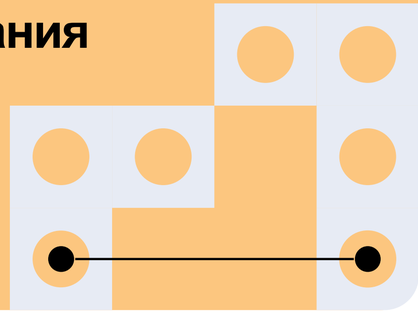
- Сотрудники или собственники компаний (SMB, enterprise)
- Относятся к ИБ или IT-ролям
- Знают о том, какие классы security-решений используются в компании

## Сроки проведения полевых работ

Февраль — апрель 2026 года

## География исследования

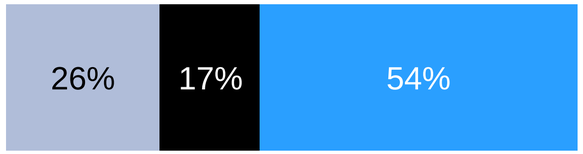
Вся Россия



* По условию в анкете компании переходили к блоку вопросов в случае, если пользуются хотя бы 1 классом решений из представленных.

# [1/3] Портрет аудитории опроса

### Размер бизнеса* (кол-во сотрудников)




- Mass (до 100 сотрудников)
- Medium (от 100 до 500 сотрудников)
- Enterprise (500+ сотрудников)
- Затруднились с ответом (3%)

База: n = 223 (сотрудники компаний).

### Выбор решений*


- ЛПР
- ЛВР
- Пользователь

База: n = 223 (сотрудники компаний).

### Роль*


База: n = 223 (сотрудники компаний).

### Тип занятости*


- B2B (в найме)
- B2B (собственники)

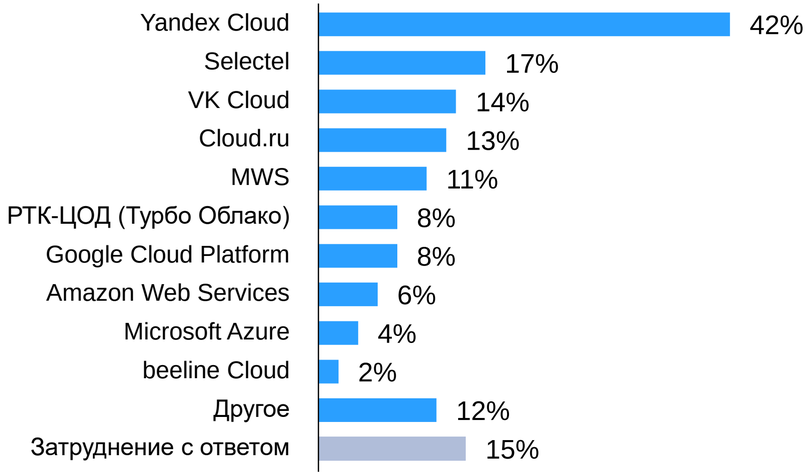
База: n = 223 (сотрудники компаний).

### Тип инфраструктуры*


- Гибрид
- On-premises
- Only cloud
- Private cloud
- Затруднились с ответом (5%)

База: n = 223 (сотрудники компаний).

### Какие облака используют?*




База: n = 133 (пользуются облаком).

* По вопросу в анкете.

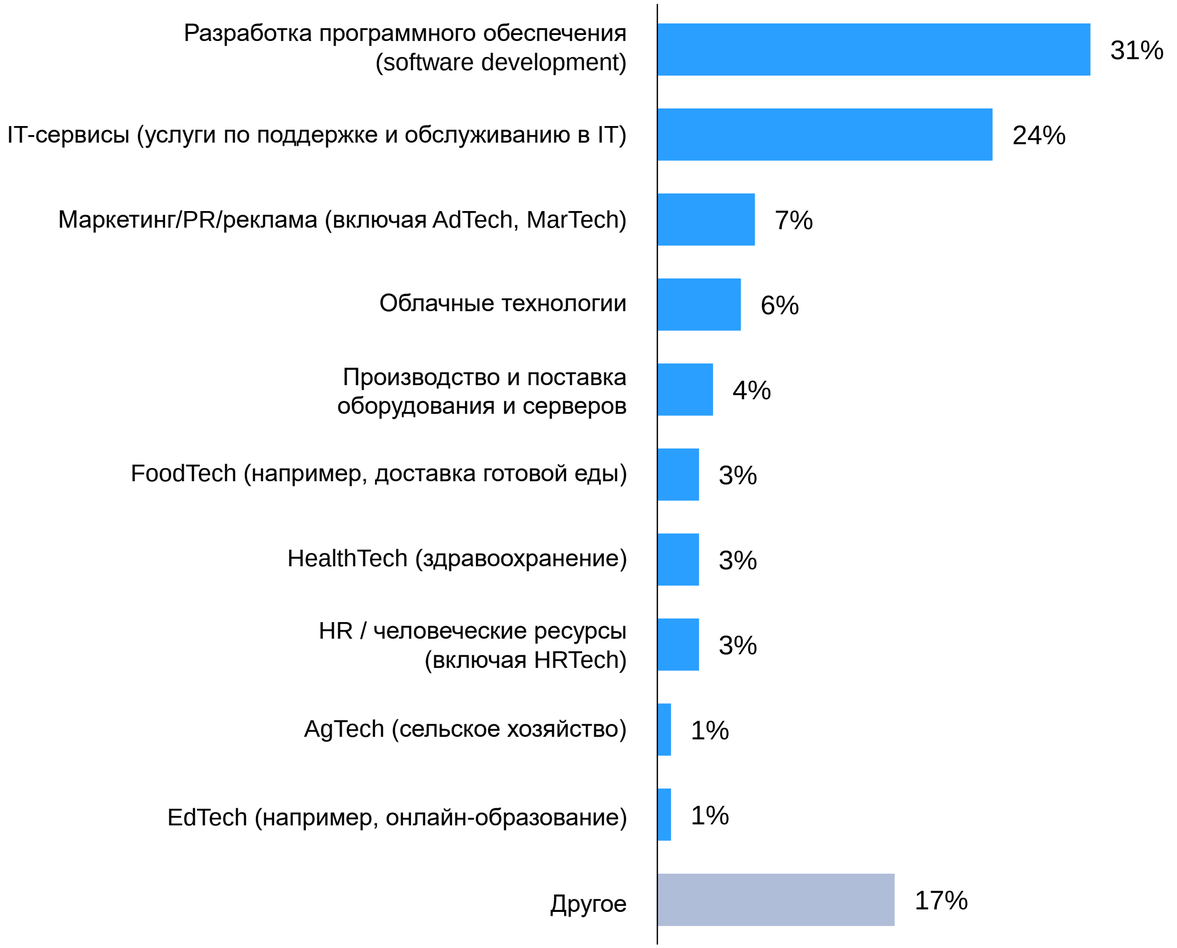
# [2/3] Портрет аудитории опроса — отрасль

## 79% от выборки [не IT]

База: n = 153.


## 31% от выборки [IT]

База: n = 70.




Часть компаний не указали отрасль.

# Резюме

# SIEM: результаты исследования

- В процессе использования SIEM-систем компании сталкиваются со следующими вызовами: **ложные срабатывания** (43%), **высокая стоимость владения** (33%) и **нехватка специалистов** (33%). Более половины **ограничивают сбор событий** (~60%) и **выбирают оптимизированный вариант по срокам хранения данных** (55% до полугода, только 16% — более года)
- **80% компаний не планируют менять текущее решение** в ближайшие 2–3 года (демонстрируя высокую лояльность текущему решению). 66% используют on-premise-модели без планов на переход (может указывать на консервативный подход к внедрению технологий безопасности или низкую распространённость решений класса в других средах)
- При выборе вендора приоритет отдаётся базовым критериям: **удобству интерфейса** (57%), **производительности и гибкому масштабированию** (57%), **функциональности/возможности корреляции** (56%), тогда как более продвинутые функции менее важны. Например, встроенные ИИ-ассистенты для помощи в работе с решением важны лишь для 12% респондентов
- 34% используют Data Lake для аналитики безопасности, а еще 31% планируют его внедрение. Основными драйверами перехода отмечают **возможности в виде хранения больших объёмов информации** (47%), **данных из разных систем** (45%) и **объединения разных источников данных** (45%)
- Несмотря на то, что 80–84% компаний успешно используют SIEM для базовых задач (мониторинг, расследование, корреляция), потребность внедрения более продвинутой функциональности ниже: **threat hunting** применяют 42%, **автоматизацию реагирования (SOAR)** — 38%. Это подкрепляется обратной связью от SMB и enterprise-сегментов, где ключевыми нереализованными потребностями названы проактивный поиск угроз, поведенческий анализ (UEBA) и расследование по клику

# Почему не пользуются решениями внутри класса SIEM?

Enterprise

## 500+ сотрудников

- Дорогое решение. Требует больших ресурсов (CISO)
- Ещё не внедрили / в процессе внедрения (CISO)
- Нет ресурсов (начальник управления IT)

Mass

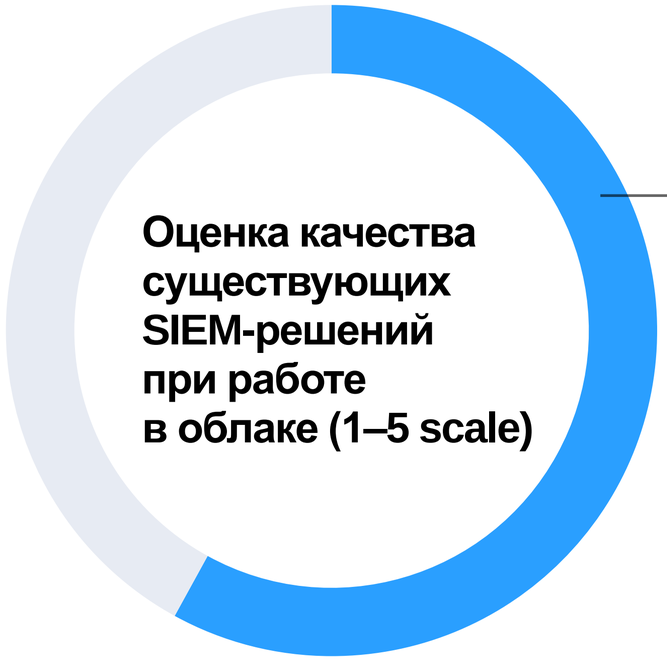
## 10–100 сотрудников

- В данный момент не используют SIEM из-за ограниченных ресурсов и приоритета более базовых средств защиты (endpoint- и сетевые решения). Для их масштаба внедрение и сопровождение SIEM выглядит слишком ресурсоёмким, при этом основные риски закрываются более простыми инструментами (ИБ-специалист)
- Пока достаточно консоли NGFW и настройки оповещений ЦУ EPP (ИБ-специалист)
- У компании нет настолько распределённой инфраструктуры и такого большого количества ресурсов, чтобы использовать SIEM (руководитель ИБ-продукта)
- Является избыточным инструментом для текущей инфраструктуры, регуляторных требований нет (руководитель отдела ИБ)
- Нет бюджета (ИБ-специалист)
- Закрытая система (СТО)

Без ответов компаний из medium-сегмента.

# Знание о рынке SIEM сконцентрировано в основном на решениях для гибридной инфраструктуры

58% пользователей высоко оценивают качество существующих SIEM-решений в облаке

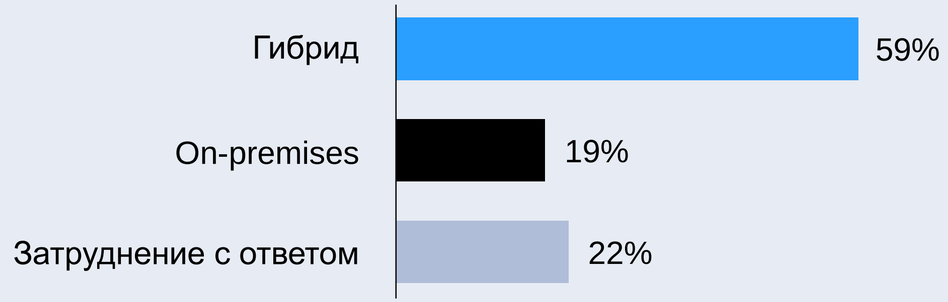



**58%**

Высоко оценили качество существующих SIEM-систем

(4/5 по шкале от 1 до 5)

**«Для каких типов инфраструктуры на рынке есть вендоры, которые предоставляют SIEM-системы?»**




Ни один из участников **не отметил** наличие only-cloud-SIEM-системы

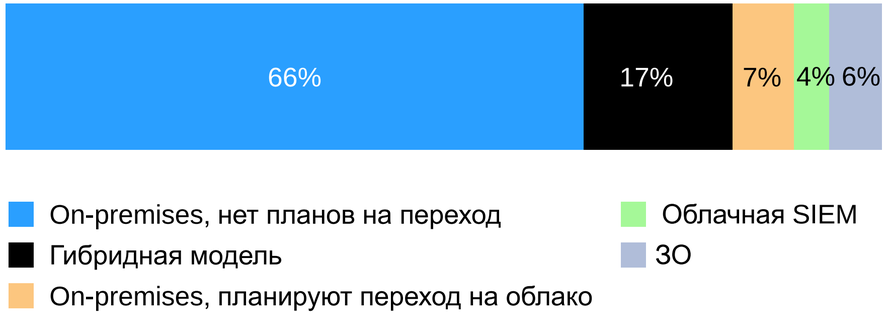
«Для каких типов инфраструктуры на рынке есть вендоры, которые предоставляют SIEM-системы?»
«Как вы оцениваете качество существующих SIEM-решений при работе в облаке?»

# Компании в основном используют SIEM для базовых задач: мониторинга, расследования и корреляции инцидентов (80–84%)

Продвинутые функции вроде threat hunting или SOAR применяются менее чем в половине случаев

**«Какие задачи вы решаете с помощью SIEM-решения в вашей компании?»**


**Модель SIEM-системы в компании**




Большинство компаний (66%) используют on-premise- SIEM-системы без планов на переход, что может указывать на консервативный подход к внедрению технологий безопасности или низкую распространённость решения в других средах

«Какие задачи вы решаете с помощью SIEM-решения в вашей компании?»
«Какая модель SIEM-системы используется в вашей компании?»

# Главные проблемы при работе с SIEM: ложные срабатывания (43%), высокая стоимость владения и нехватка специалистов (по 33%)

Также заметны трудности с автоматизацией, настройкой и интеграцией с другими источниками данных, что указывает на сложность внедрения и сопровождения SIEM-решений

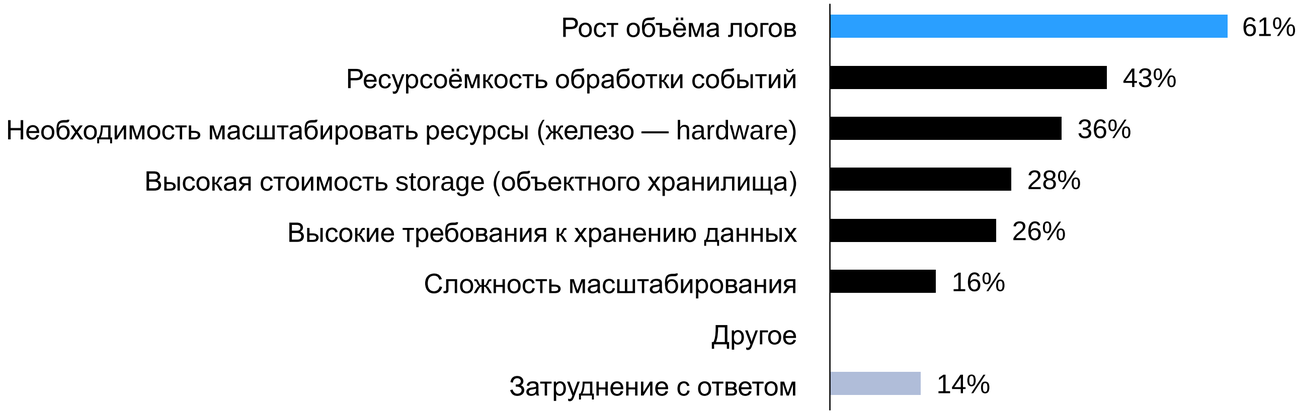
**«С какими проблемами сталкиваются в работе с SIEM-решениями?»**


«С какими проблемами вы столкнулись при работе с текущим SIEM-решением?»

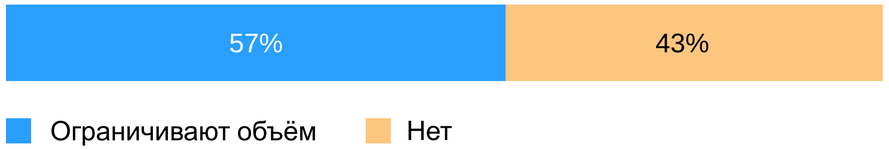
# Компании сталкиваются с растущей нагрузкой на SIEM-инфраструктуру из-за роста объёмов логов и высоких затрат на их обработку и хранение

Более половины компаний вынуждены ограничивать сбор событий.
Как возможное последствие — большинство выбирает компромиссный срок хранения данных

**«Какие факторы создают наибольшую нагрузку на инфраструктуру SIEM?»**




**Ограничение объёма собираемых событий**




Около 60% компаний ограничивают объём из-за ограничений инфраструктуры или высокой стоимости хранения иногда/регулярно.
Лишь 14% никогда с этим не сталкивались

**«Какой срок хранения событий безопасности используется в вашей SIEM-системе?»**

- **3%** Менее 30 дней
- **27%** От 30 до 90 дней
- **25%** От 90 дней до 6 мес.
- **20%** От 6 мес. до 1 года
- **16%** Более года
- **9%** Затруднение с ответом

Высокая стоимость и ограничения инфраструктуры могут влиять на срок хранения данных — 55% (до полугода).
Лишь 16% отметили период более года

«Какие факторы создают наибольшую нагрузку на инфраструктуру SIEM?»
«Приходилось ли вам ограничивать объём собираемых событий из-за ограничений инфраструктуры или высокой стоимости хранения?»*
* Доля банковского сектора внутри ответов — не более 5%.

# При выборе SIEM ключевыми критериями являются удобство интерфейса, производительность и функциональность

Низкую значимость имеют рекомендации коллег, онбординг и ИИ-ассистенты — значения 15% и ниже

**Важность критериев при выборе SIEM-систем**

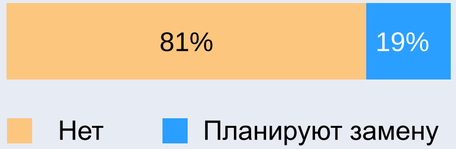



«Какие критерии наиболее важны для вас / вашей компании при выборе решения для управления событиями и инцидентами безопасности (SIEM)?»

# Около 80% компаний лояльны к текущему решению и не планируют его менять

При этом наиболее распространёнными источниками данных для интеграции остаётся сетевое оборудование (79%) и серверы (78%), тогда как облачные сервисы и IoT-системы интегрированы у 40 и 16% соответственно

**«Рассматриваете ли вы замену или модернизацию SIEM в ближайшие 2–3 года?»**




**Каждая пятая компания планирует замену текущей SIEM (7%) или добавление ещё одного решения (12%)**

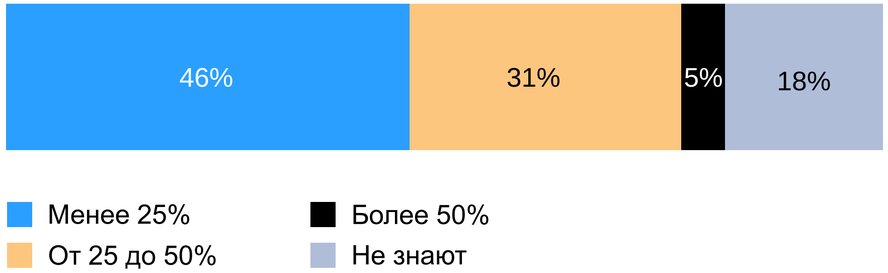
**«Какие источники данных интегрированы с вашей SIEM-системой?»**


«Рассматриваете ли вы замену или модернизацию SIEM в ближайшие 2–3 года?»
«Какие источники данных интегрированы с вашей SIEM-системой?»

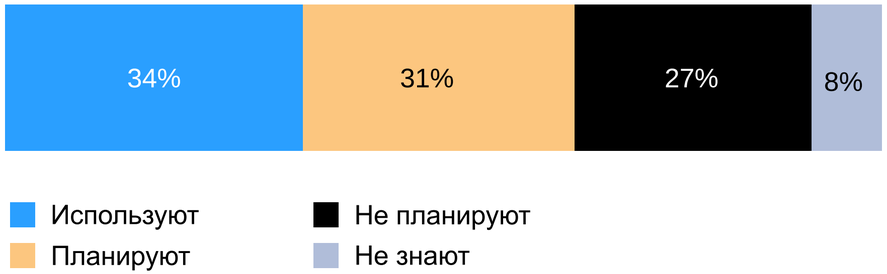
# 34% компаний используют Data Lake для аналитики безопасности, ещё 31% планируют внедрение

Основные преимущества — централизация данных, использование для работы с большими данными

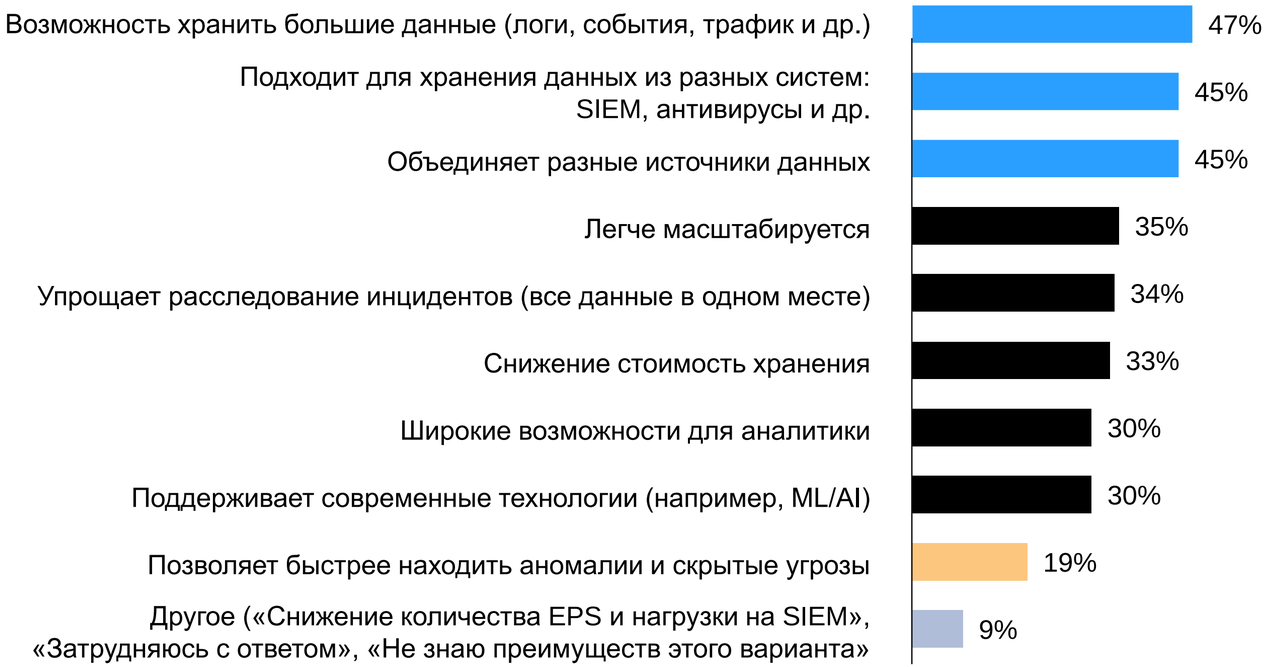
### Доля бюджета на SIEM (серверы, storage)




### Отдельные хранилища для событий




### Преимущества в архитектуре Data Lake для аналитики систем безопасности




«На ваш взгляд, какие преимущества в архитектуре Data Lake для аналитики систем безопасности можно выделить?»
«Используете ли вы отдельные хранилища (Data Lake или архивные системы) для хранения событий безопасности?»
«Какая часть общего бюджета на SIEM приходится на инфраструктуру (серверы, storage) в вашей компании?»

# Важные сценарии для SMB, которые не до конца реализованы в текущих решениях

SMB: цитаты Открытый вопрос

## Обнаружение сложных многоэтапных атак и поведенческий анализ

«Система не всегда способна корректно связать разрозненные события в единую цепочку инцидента. Поведенческая аналитика и автоматизация либо работает неточно, либо не используется из-за риска ложных срабатываний»

## Активное автоматизированное реагирование (SOAR внутри SIEM)

«Критически не хватает возможности быстрого выполнения действий по купированию инцидента (изоляция источника угроз) непосредственно из SIEM через интеграцию с защитным ПО»

## Контекстуализация событий и поддержка гибридных сред

«Недостаточно реализовано обогащение событий контекстом, а поддержка облачных сред нередко остаётся ограниченной, создавая потенциальные слепые зоны»

## Юзабилити, визуализация и финансовые риски

«Критическое снижение функциональности при просрочке лицензирования, а также дефицит удобных средств визуализации и кастомизации интерфейса»

«Какие сценарии использования решений для управления событиями и инцидентами безопасности (SIEM) вы считаете наиболее важными, но они плохо реализованы в текущем решении?»

# Примеры актуальных сценариев от SMB-аудитории: открытая обратная связь

- Проактивный threat hunting на больших объёмах данных
- Зрелая автоматизация реагирования
- Поведенческий анализ на базе ML
- Удобная визуализация и кастомизация

Интеграция с ИИ, который будет верно подбирать, а иногда и создавать плейбуки (хотя это больше к SOAR)

Сложность внедрения и интеграции с новыми данными

Мониторинг привилегированных учётных записей, контроль облачной и гибридной инфраструктуры

Возможности быстрого выполнения действий по купированию инцидента (изоляция источника угроз и т. п.) непосредственно из SIEM на основе соответствующей интеграции SIEM с ПО и оборудованием, которые могут предоставить исполнительные механизмы (антивирус, сетевое оборудование)

Предотвращение попыток подбора паролей, авторизация подрядчиков на коммутационном оборудовании

Одним из ключевых, но слабо реализованных сценариев в SIEM, является выявление сложных многоэтапных атак, где система не всегда способна корректно связать разрозненные события в единую цепочку инцидента. Также часто недостаточно реализовано обогащение событий контекстом, из-за чего аналитикам приходится тратить больше времени на разбор. Поведенческая аналитика и автоматизация реагирования обычно либо работают неточно, либо практически не используются из-за риска ложных срабатываний. А поддержка облачных сред нередко остаётся ограниченной, создавая потенциальные слепые зоны в мониторинге

# Важные сценарии для enterprise, которые не до конца реализованы в текущих решениях

Enterprise: цитаты

### Интеллектуальное расследование и предиктивная аналитика

«Отсутствуют готовые модели угроз на основе MITRE ATT&CK® с предиктивной логикой», «Отсутствует встроенный режим расследования по клику, когда система сама предлагает связанные события, возможные векторы атаки и рекомендации по следующим шагам»

### Стабильность, масштабируемость и особенности архитектуры

«Низкая надежность платформы приводит к значительным операционным затратам, требуя сверхурочной работы специалистов для восстановления ее функциональности, «Мультитенантность»

### Работа с данными: нормализация, контекст активов и ложные срабатывания

«Управление false positive и активами», «Нормализация из коробки», «Возможность отслеживать все события, включая ненормализованные», «выявление горизонтальных перемещений, использования легального ПО для атак», «Обнаружен вирус. Даже если ВПО было удалено антивирусом, то иногда приходится обрабатывать как обычно»

### Глубокая автоматизация реагирования и взаимодействие

«Автоматическое подтверждение действия пользователем — было бы хорошо, будь что-то подобное из коробки», «Если активность продолжается, то алерт не обновляется новыми событиями с неуспешными брутами»

### Снижение порога входа: конструкторы правил и готовый контент

«Конструктор правил корреляций. Сложный порог входа в собственный от вендора язык программирования», «Гибкость настройки правил корреляции. Отсутствие готовых шаблонов по известным уязвимостям и атакам»

«Какие сценарии использования решений для управления событиями и инцидентами безопасности (SIEM) вы считаете наиболее важными, но они плохо реализованы в текущем решении?»

# Примеры актуальных сценариев от enterprise-аудитории: открытая обратная связь

Отсутствует встроенный режим **расследования по клику**, когда система сама предлагает связанные события, возможные векторы атаки и рекомендации по следующим шагам. Экспорт цепочек событий для отчётности требует ручной доработки

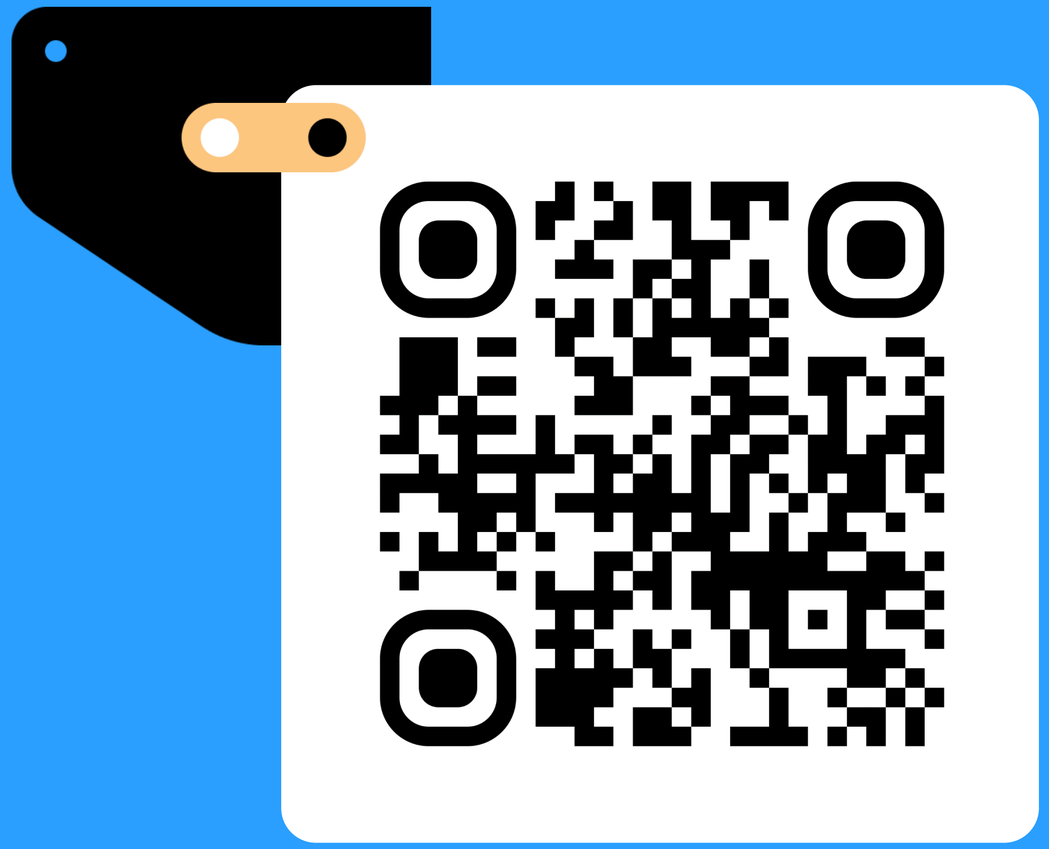
Выявление горизонтальных перемещений, использования легального ПО для атак, сбор и аналитика большого объёма данных, прикручивание ИИ и ML, полная гибкость в создании правил корреляции любой сложности

Автоматическое подтверждение действия пользователем

**Пример:** пользователь исполнил подозрительную команду в контейнере, SIEM-система получила событие, обработала его. Далее пользователю приходит автоматизированное уведомление вида «Вы или не вы? Подтвердите активность». Реализовали это при помощи кастомного сервиса

Этим же кастомным сервисом реализовали интеграцию SIEM с корпоративным мессенджером: при получении события в SIEM в отдельный канал корп. мессенджера приходит уведомление с кнопками. Было бы хорошо, будь что-то подобное **из коробки**

Ключевым требованием является бесперебойность базовых функций SIEM — мониторинга и детектирования инцидентов. Приоритет смещается на фундаментальные атрибуты эксплуатации: стабильность, предсказуемость масштабирования и глубокую экспертизу вендора



# Безопасно говоря

Наш телеграм-канал
t.me/yndxcloudsecurity