Kaspersky Managed Detection and Response в 2022 году

Сергей Солдатов

руководитель центра мониторинга
кибербезопасности «Лаборатории Касперского»

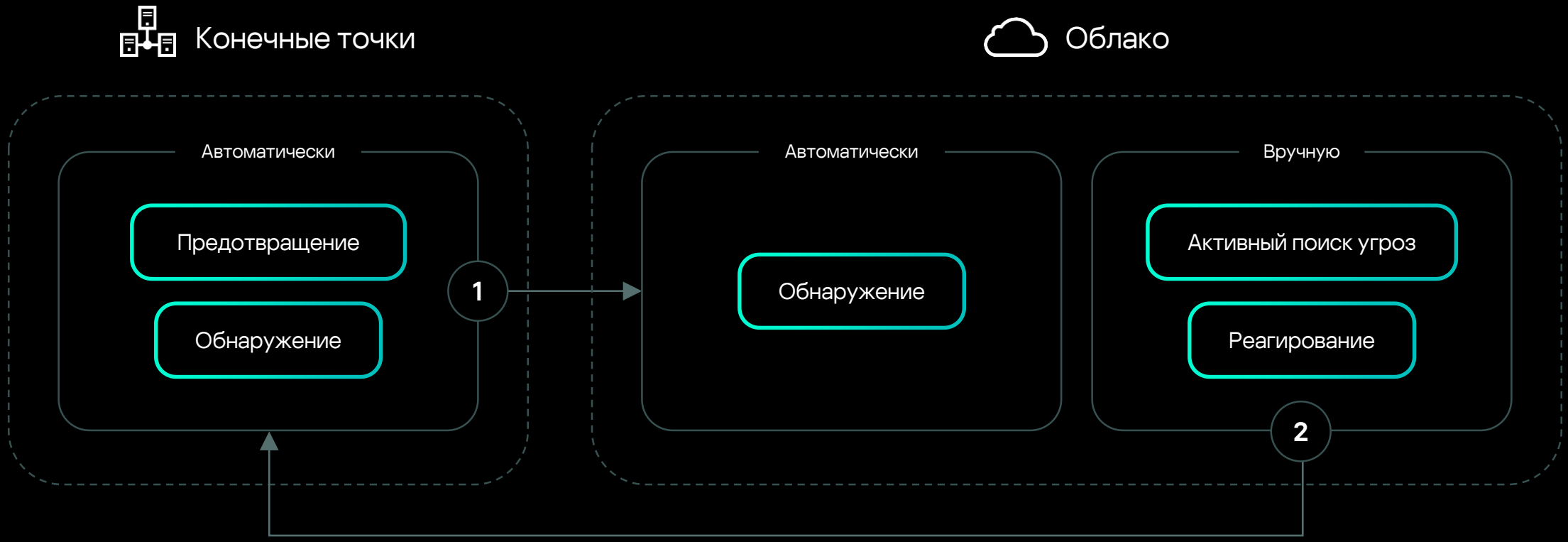
kaspersky

План вебинара

1. Kaspersky MDR: краткий обзор
2. Анонс акции
3. Отчет за 2022 год: статистика и результаты
   - Охват услуги сервиса
   - Критичность инцидентов
   - Природа критичных инцидентов
   - Тактики злоумышленников
   - Техники и инструменты злоумышленников
4. Основные выводы

Kaspersky MDR: краткий обзор

Многоуровневая архитектура Kaspersky MDR



1 **Телеметрия**

Стандартные события безопасности EDR.
Точные и неточные детекты EPP-решения

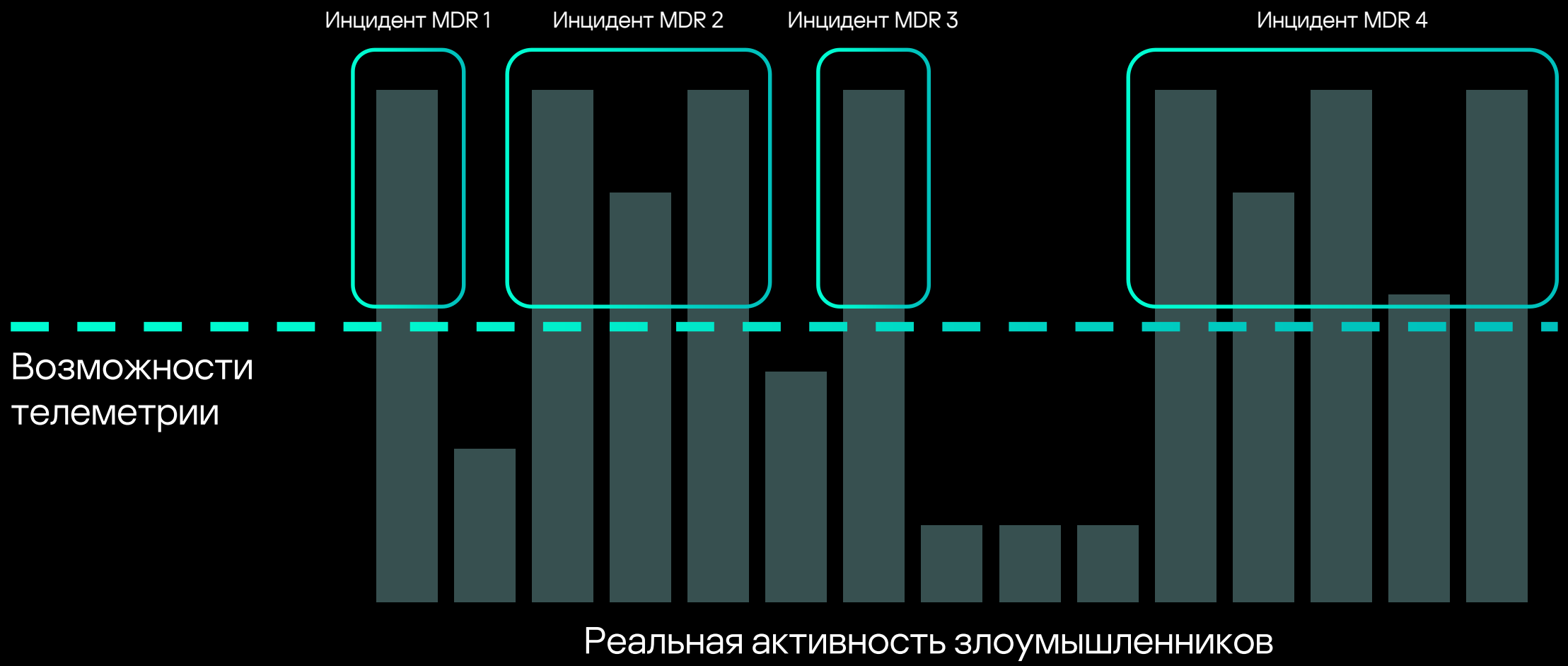
2 **Реагирование**

Стандартные меры реагирования EDR.
Обновление детектов EPP-решения

Как это работает: Kaspersky MDR

Предоставление рекомендаций по реагированию
и удаленное реагирование

Активность атакующего в рамках инцидента



Уровни Kaspersky MDR

Optimum

- Круглосуточный мониторинг
- Проактивный поиск угроз (Threat Hunting) силами экспертов «Лаборатории Касперского»
- Консультации аналитиков SOC «Лаборатории Касперского»
- Автоматизированный поиск угроз
- Сценарии реагирования и автоматическое реагирование на инциденты
- Обзор всех защищаемых ресурсов с их текущим статусом
- Консоль управления с панелями мониторинга и отчетами
- Хранение истории инцидентов безопасности в течение 1 года
- Хранение необработанной телеметрии в течение 1 месяца

Expert

- Круглосуточный мониторинг
- Проактивный поиск угроз (Threat Hunting) силами экспертов «Лаборатории Касперского»
- Консультации аналитиков SOC «Лаборатории Касперского»
- Автоматизированный поиск угроз
- Сценарии реагирования и автоматическое реагирование на инциденты
- Обзор всех защищаемых ресурсов с их текущим статусом
- Консоль управления с панелями мониторинга и отчетами
- Хранение истории инцидентов безопасности в течение 1 года

Только в Expert

- Хранение необработанной телеметрии в течение 3 месяцев
- Доступ к порталу Kaspersky Threat Intelligence
- API для интеграции с IRP / SOAR
- Возможность самостоятельно зарегистрировать инцидент при подозрении на компрометацию

Условия предложения

Ранее не использовали
и не пилотировали Kaspersky MDR

Используются продукты линейки Kaspersky Security для бизнеса

Количество защищаемых устройств от 3000

Предложение действительно на территории России, стран Средней Азии и Закавказья

Заполнить заявку на получение сервиса нужно до 31 мая 2023 года

Хотите узнать подробности?

Отсканируйте QR-код
или просто перейдите по ссылке

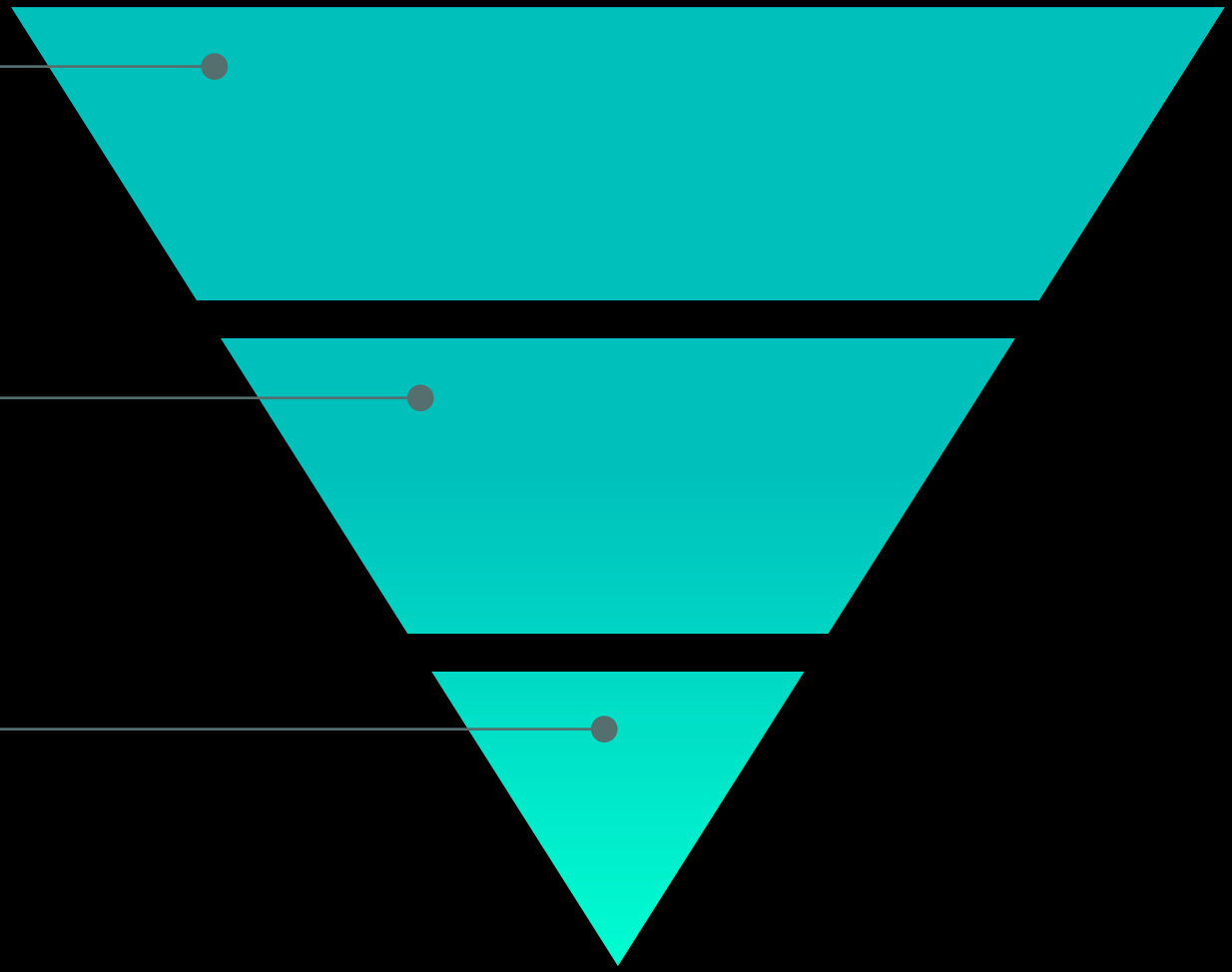
https://kas.pr/offer-mdr-free

Отчет за 2022 год: статистика и результаты

Охват услуги MDR

Воронка обработки телеметрии

~14 000 необработанных событий от каждого хоста ежедневно



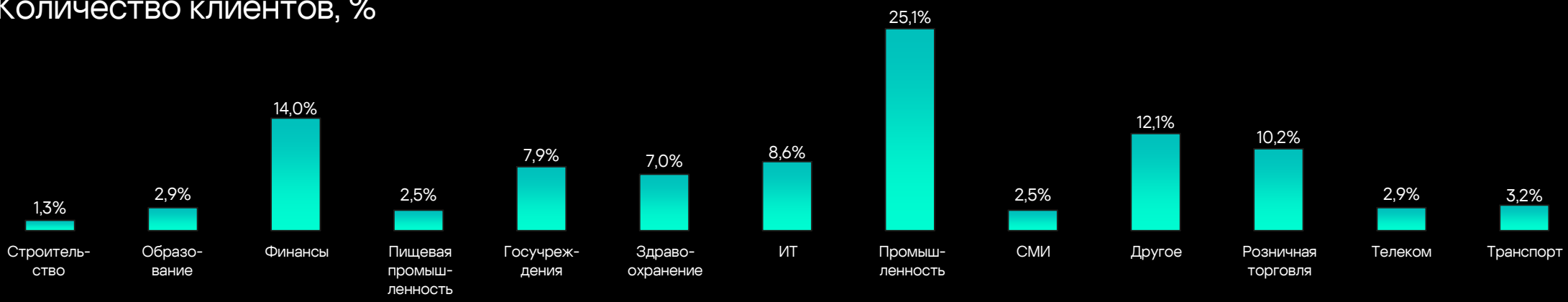
>141 000 автоматически на основе ИИ

>292 000 аналитиками SOC

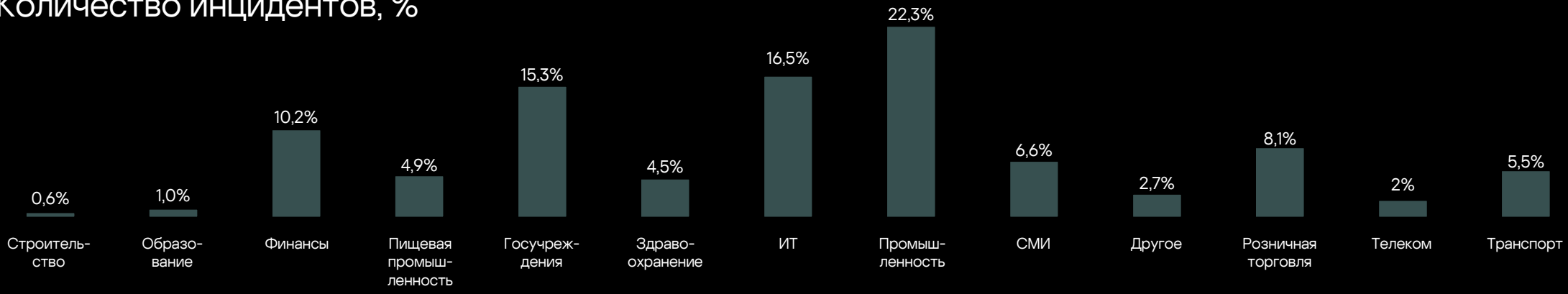
~33 000 событий безопасности преобразованы в ~12 000 инцидентов

Охват сервиса по отраслям

Количество клиентов, %



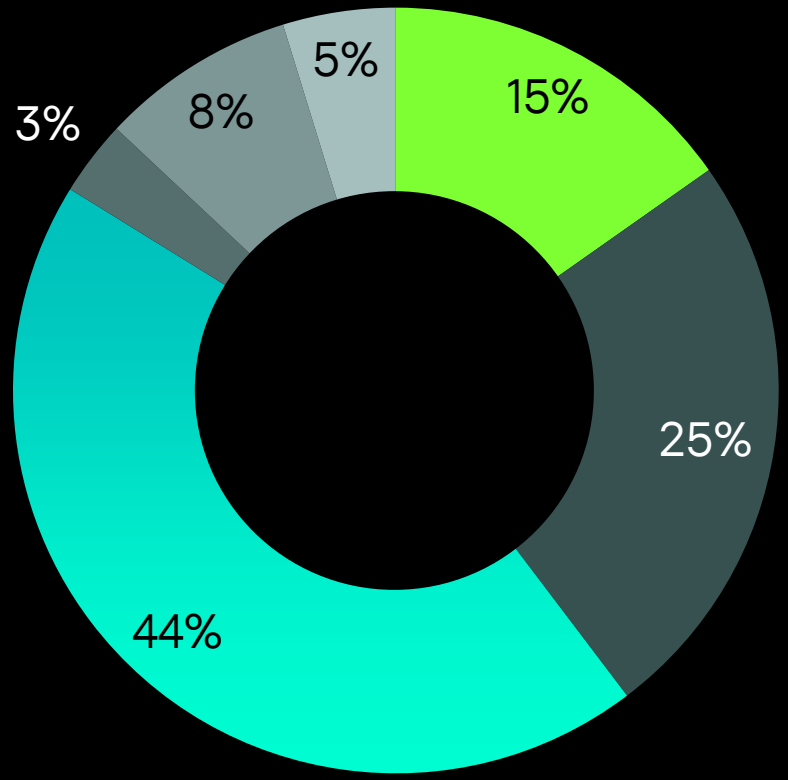
Количество инцидентов, %



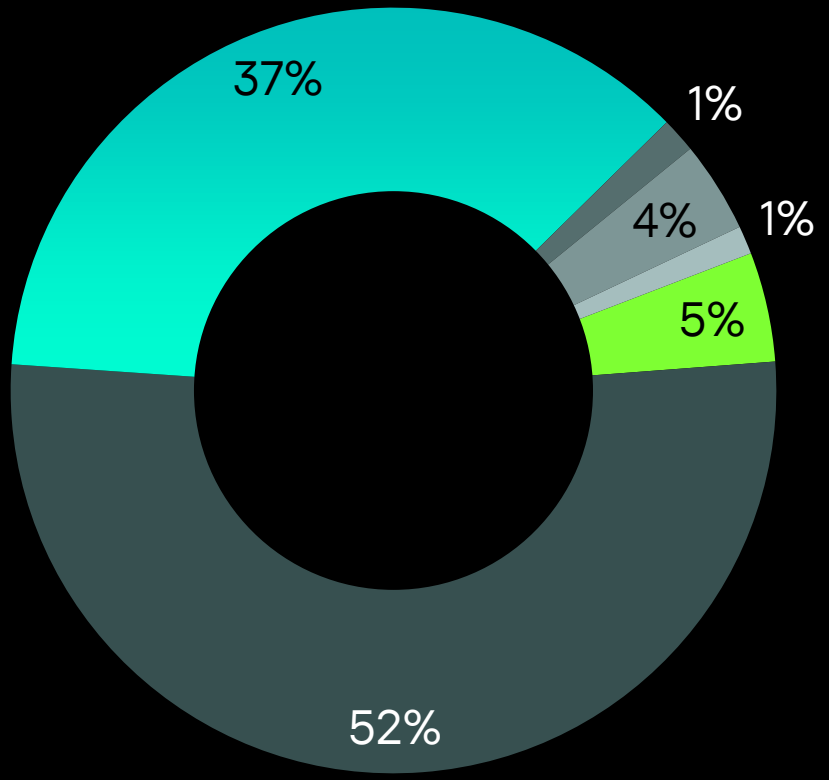
Охват сервиса по регионам

Europe
CIS
APAC
META
North America
LatAm

Число клиентов, %



Число защищаемых устройств, %



Отчет за 2022 год: статистика и результаты

Критичность инцидентов

Критичность инцидентов

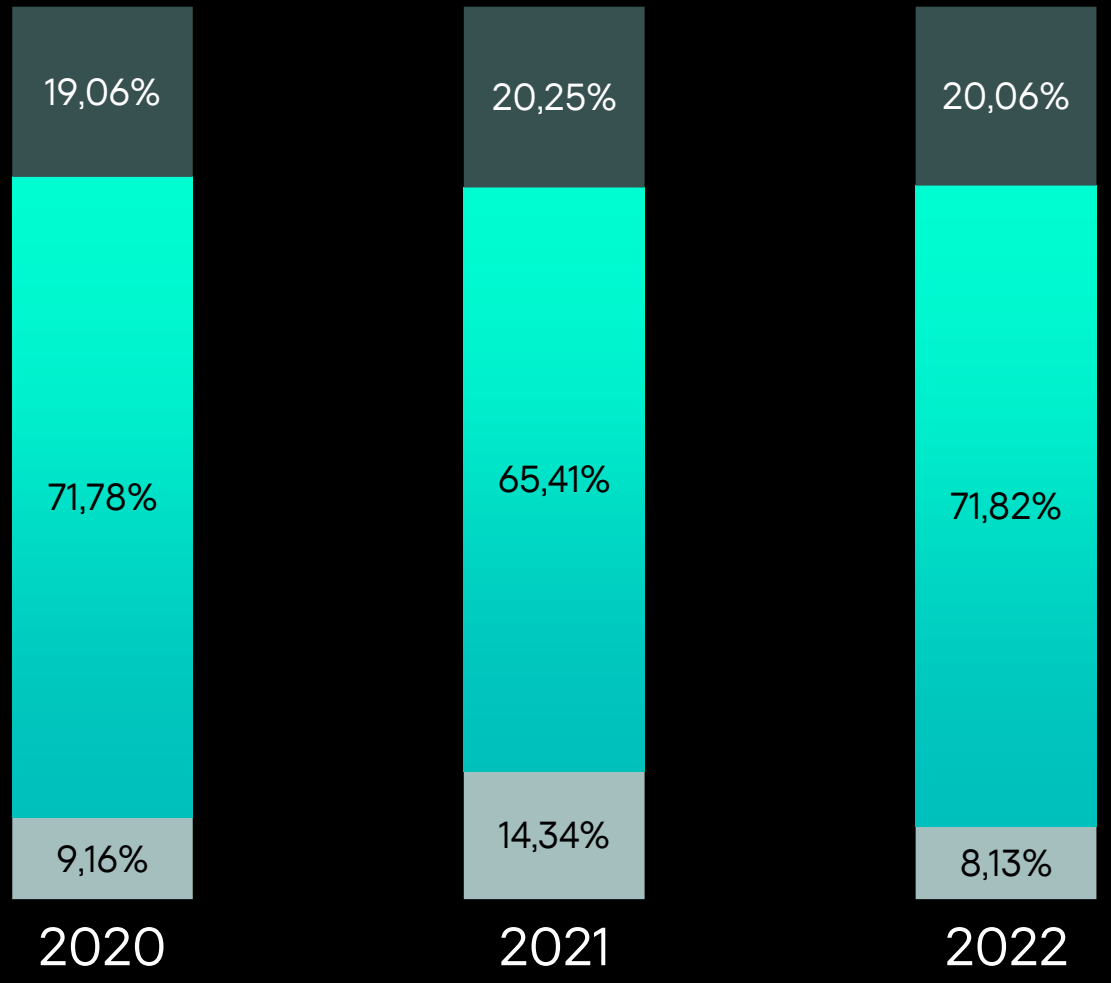
Низкий уровень влияния на бизнес

Средний уровень воздействия на бизнес

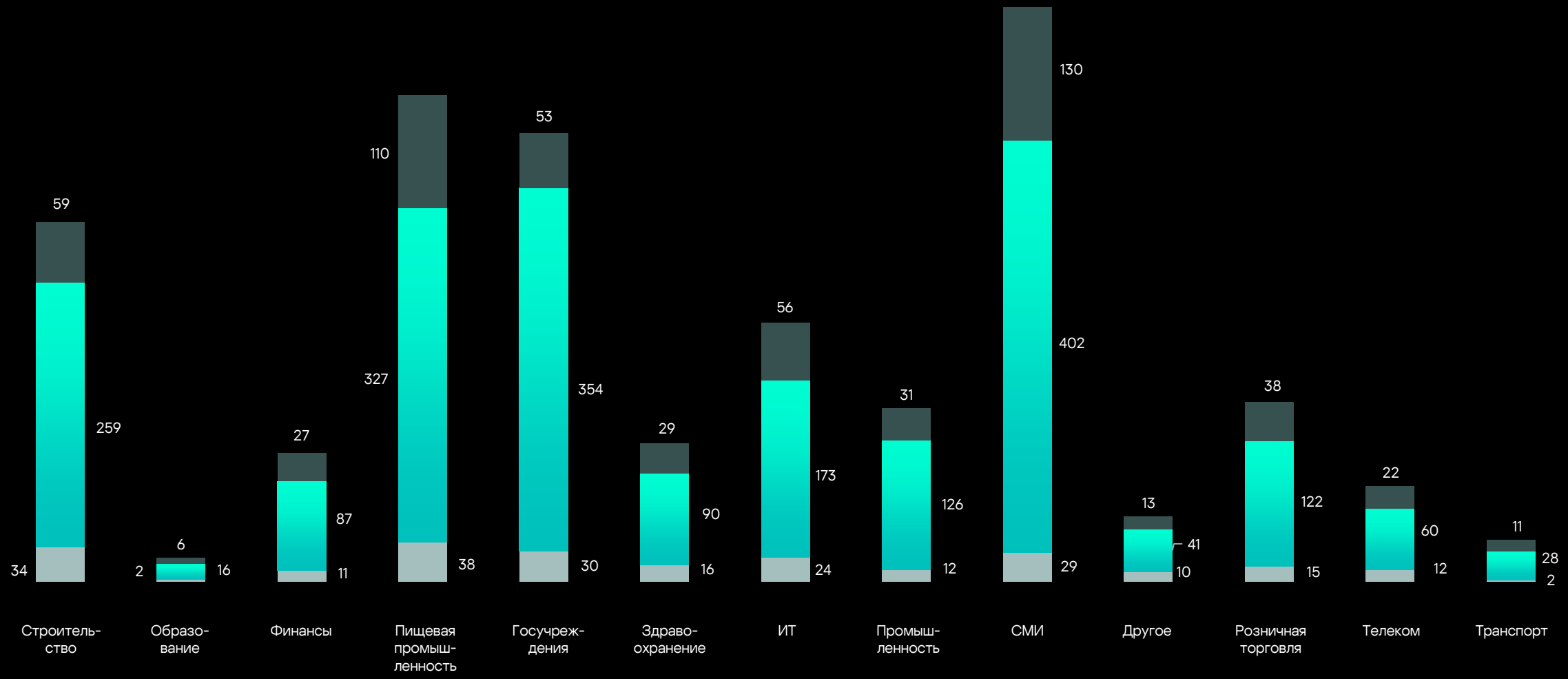
Без участия человека

Большой ущерб — потенциальный или реальный

С участием человека

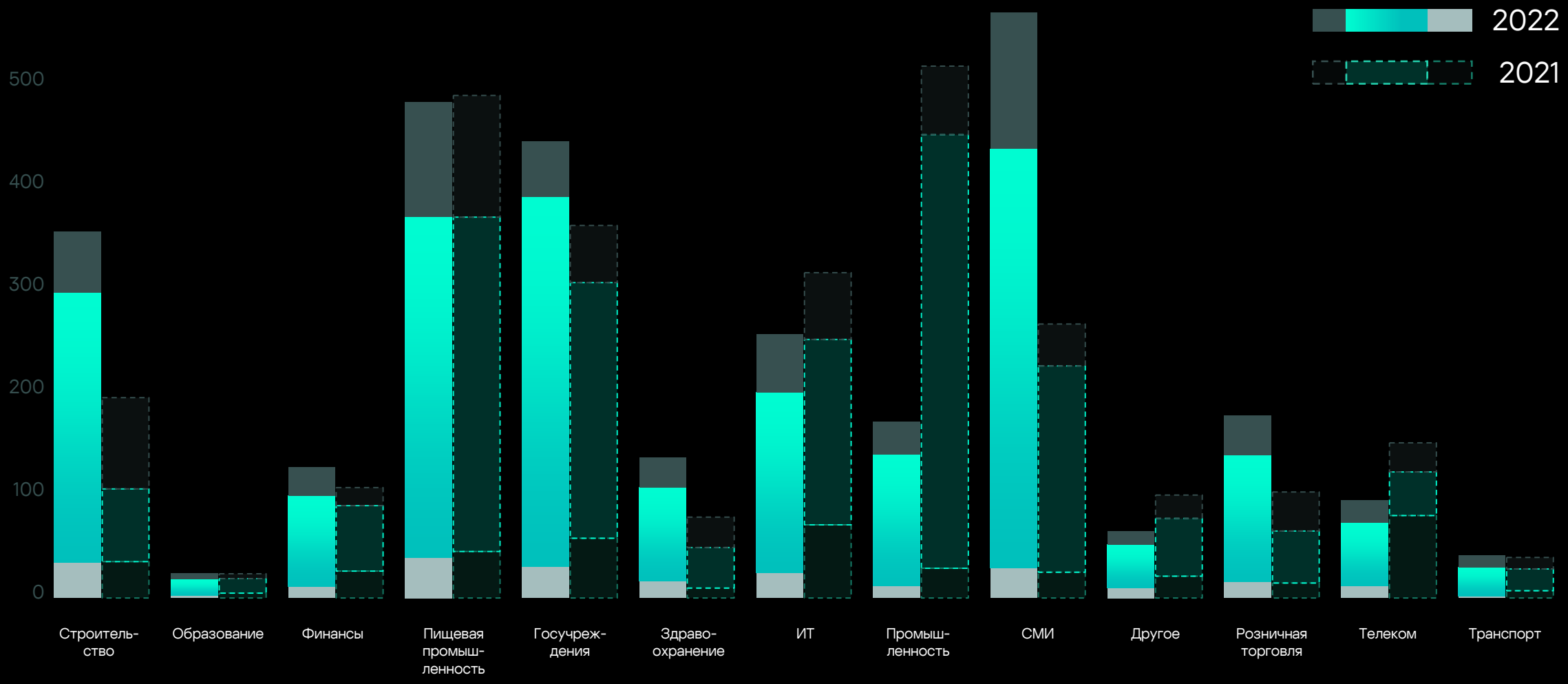


Критичность инцидентов по отраслям*



* Количество инцидентов в отношении на 10 000 конечных точек

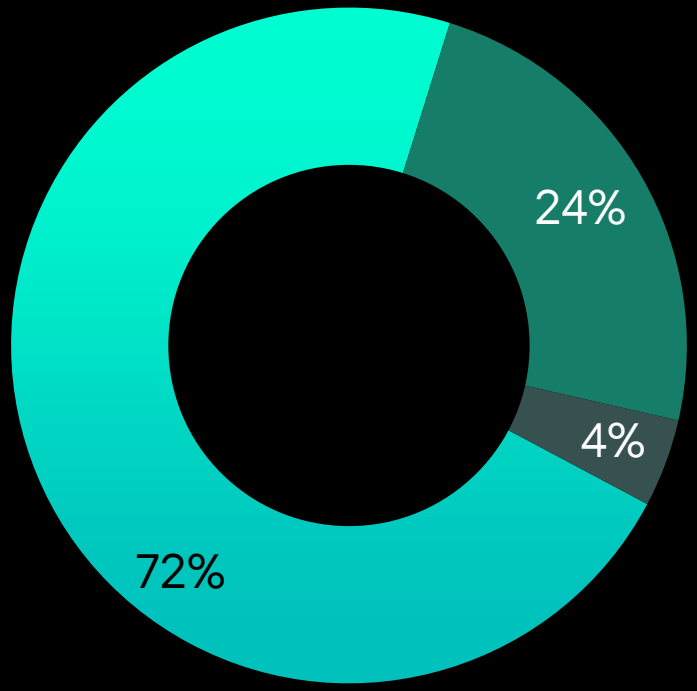
Критичность инцидентов в разных отраслях: сравнение 2022 и 2021 гг.



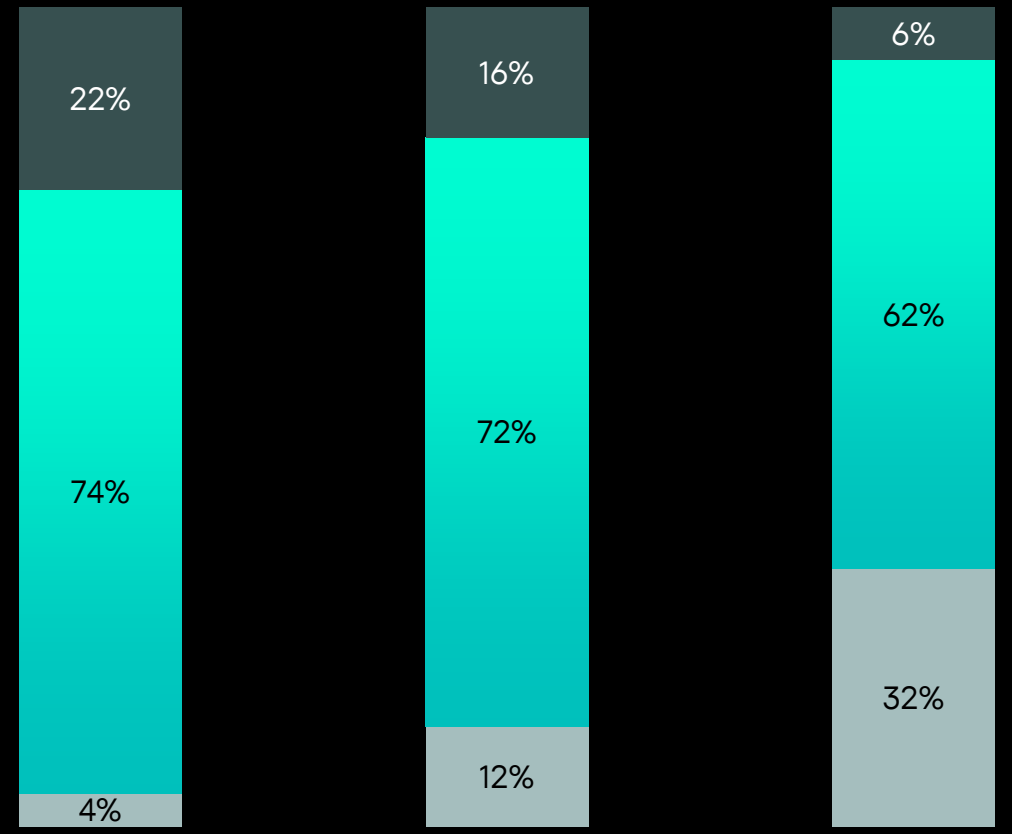
Скорость обнаружения инцидента

Критичность высокая	43,75	Самые сложные инциденты, требующие наибольшего времени на дополнительное обогащение данных и составление хронологии событий. Время обработки увеличилось примерно на 6% по сравнению с 2021 годом. Это связано с ростом в 2022 году числа атак с участием человека – их расследование трудно автоматизировать, требуется активное участие аналитиков SOC.
средняя	30,92	Инциденты с таким уровнем критичности происходят чаще других и обычно являются последствиями применения вредоносного ПО. Время реагирования на них сократилось по сравнению с 2021 годом благодаря повышению уровня автоматизации обработки новых типов инцидентов.
низкая	34,15	Инциденты самой низкой степени критичности, большинство из которых возникают вследствие использования нежелательного ПО. Они могут находиться в очереди на обработку дольше других. Для обработки таких инцидентов используются различные механизмы автоматизации. Это помогает сократить степень участия аналитиков SOC и время реагирования.

Эффективность реагирования



- Инциденты с 1 алертом
- Инциденты с 2-8 алертами
- Инциденты с 8+ алертами



Инциденты с 1 алертом

Инциденты с 2-8 алертами

Инциденты с 8+ алертами

Отчет за 2022 год: статистика и результаты

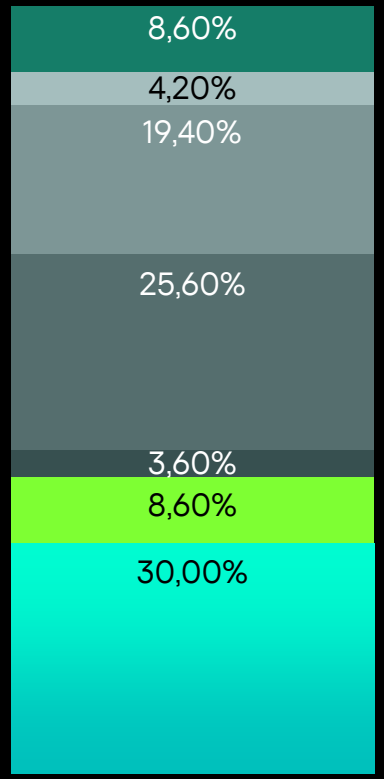
Природа критичных инцидентов

Типы инцидентов высокой критичности

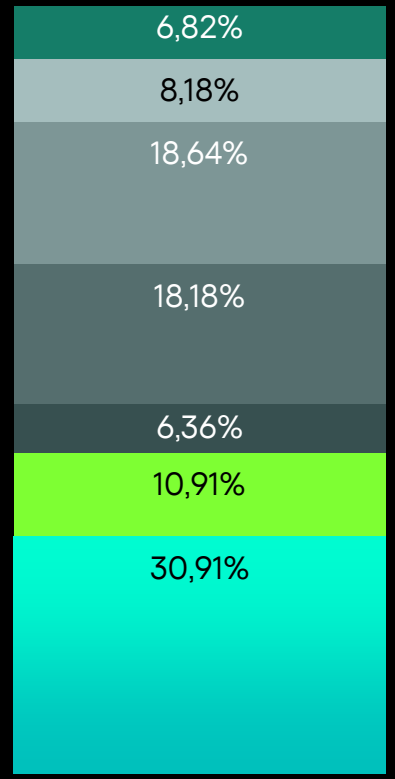
Угроза	Название	Подробности
APT	Целевая атака	Целевая атака, любая атака с участием человека без подтверждения киберучений
PT	Red teaming	Анализ защищенности / Киберучения
Неактивная APT / RT	Артефакты ЦА	Артефакты предыдущих APT-атак / любых атак с участием человека
Атака с использованием вредоносного ПО, приносящая ущерб	Вредоносное ПО	Активность вредоносного ПО, приносящая крупный ущерб (волна атак шифровальщиков)
Публично доступная уязвимость	Уязвимость	Уязвимость, которую могут использовать злоумышленники (известная уязвимость в периметре)
DoS-атака, приносящая ущерб		DDOS / DOS-атака с воздействием на бизнес
Внутренняя угроза, приносящая ущерб	Инсайдер	Угроза инсайдера с воздействием на бизнес (саботаж, мошенничество)
Успешное применение социальной инженерии, приносящее ущерб	Соц. инженерия	Успешная социальная инженерия (пользователь кликнул / запустил / скачал), последствия которой не удается устранить автоматически

Природа критичных инцидентов

- Уязвимость
- Социальная инженерия
- Киберучения
- Вредоносное ПО
- Инсайдер
- Артефакты целевой атаки
- Целевая атака

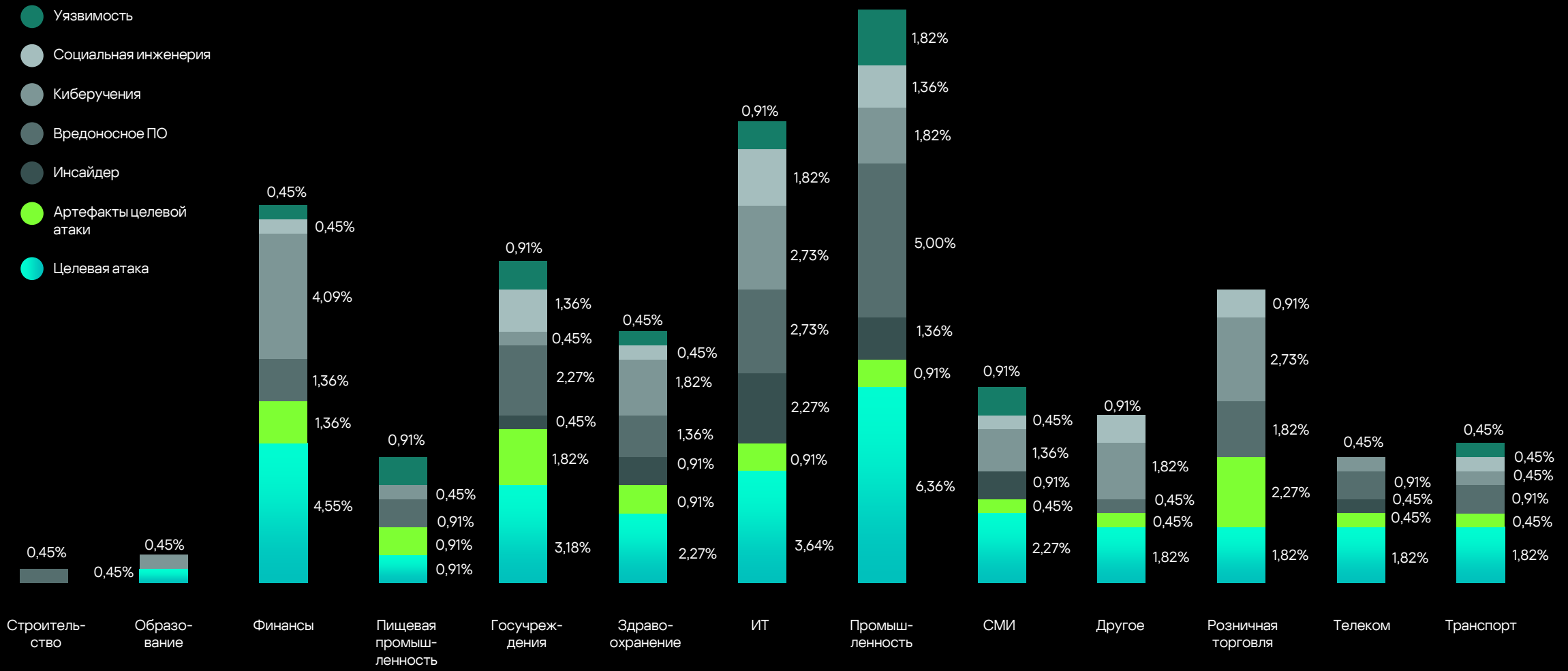


Количество инцидентов

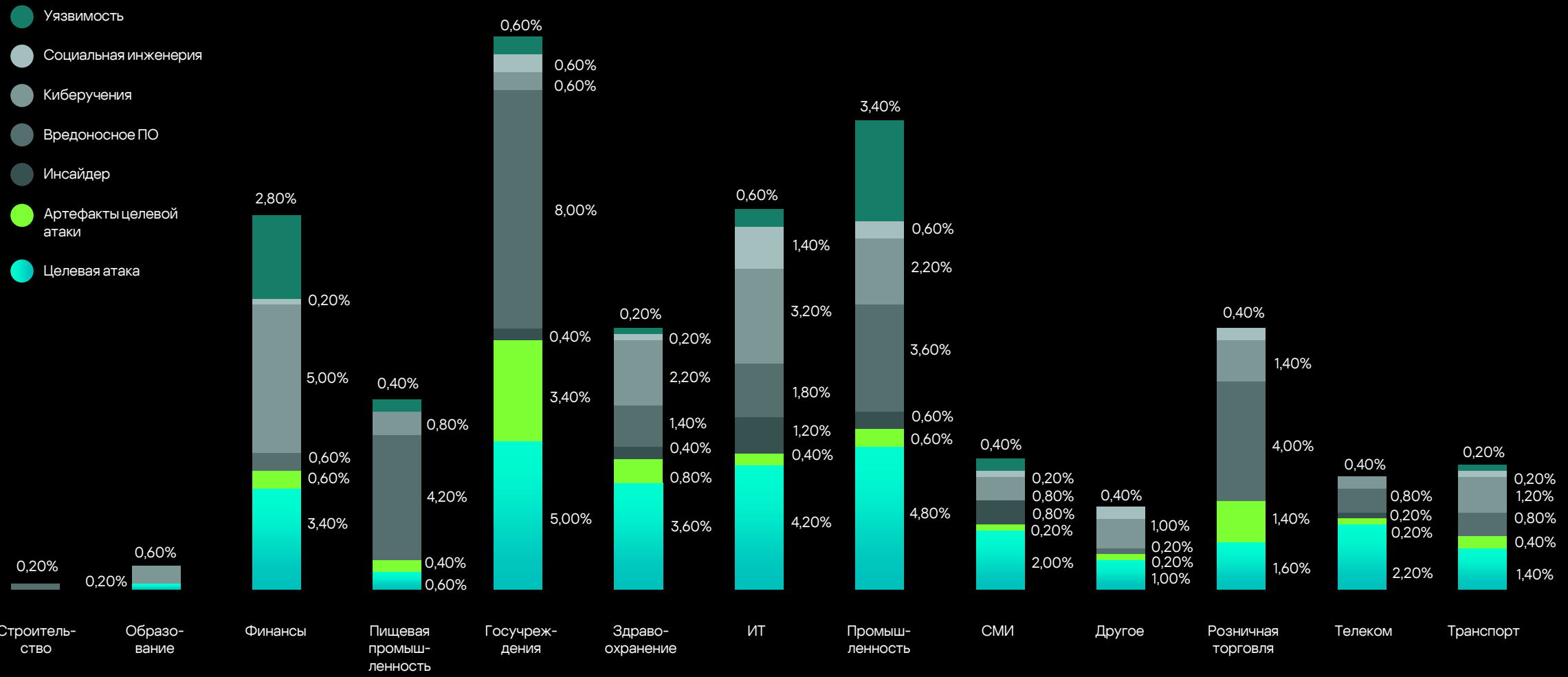


Количество организаций

Природа критичных инцидентов: распределение по отраслям. Число клиентов



Природа критичных инцидентов: распределение по отраслям. Количество инцидентов

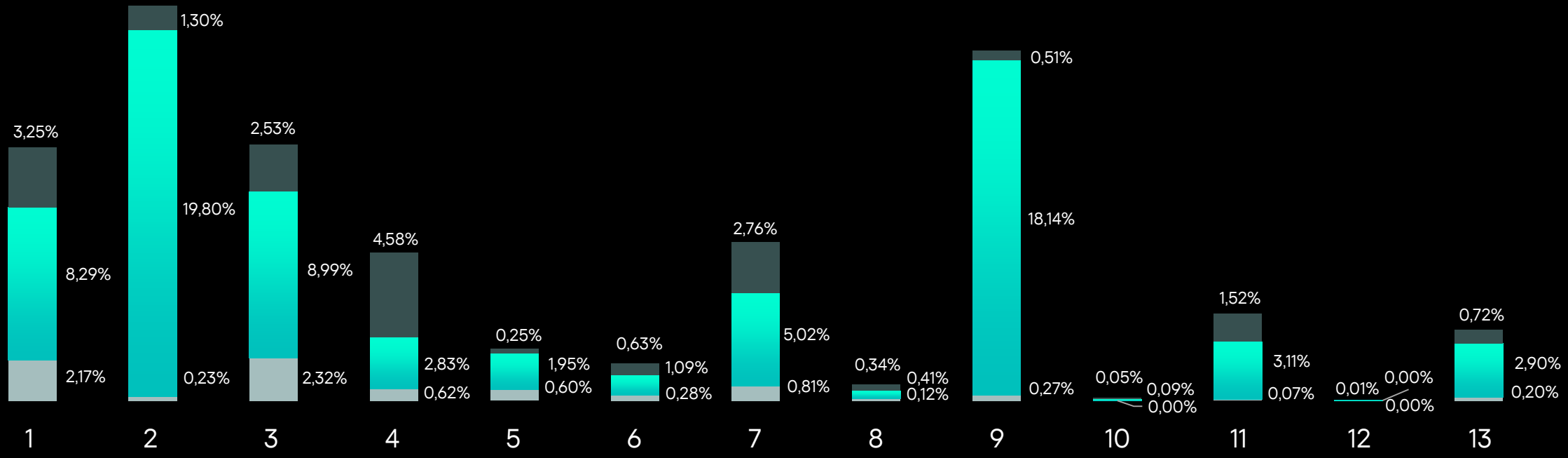


Отчет за 2022 год: статистика и результаты

Тактики злоумышленников

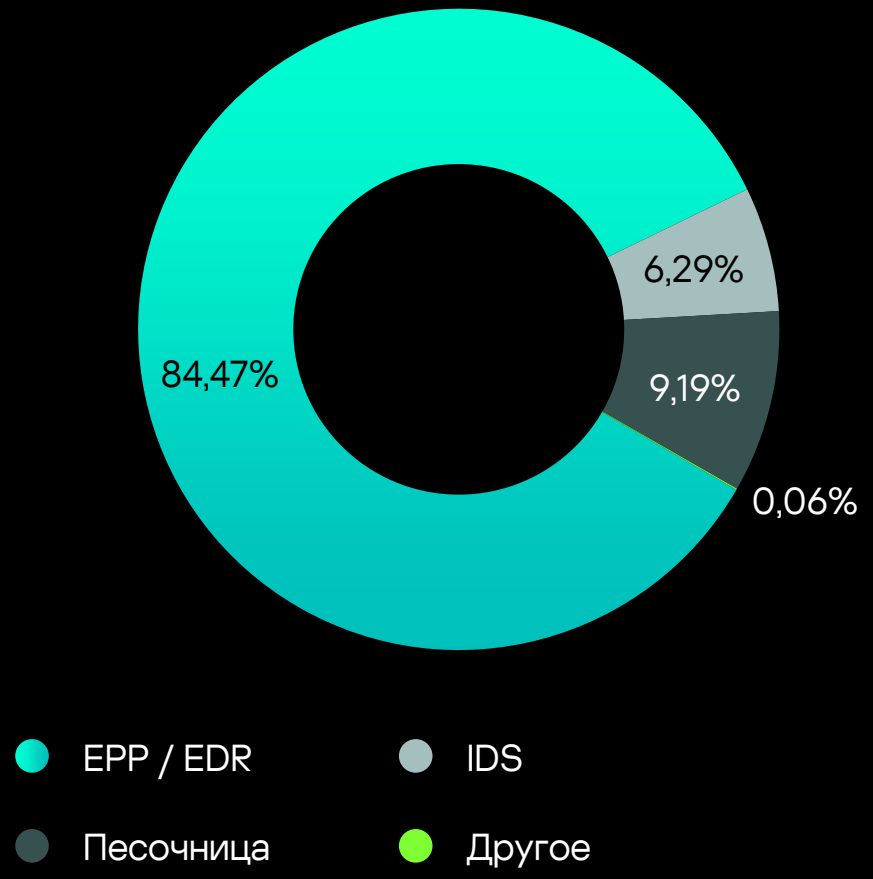
Наиболее ранняя тактика – уровень критичности

1 TA0042 Подготовка ресурсов
2 TA0001 Первоначальный доступ
3 TA0002 Выполнение
4 TA0003 Закрепление
5 TA0004 Повышение привилегий
6 TA0005 Предотвращение обнаружения
7 TA0006 Получение учетных данных
8 TA0007 Исследование
9 TA0008 Горизонтальное перемещение
10 TA0009 Сбор данных
11 TA0011 Управление и контроль
12 TA0010 Эксфильтрация данных
13 TA0040 Ущерб



Технологии обнаружения

Обнаруженные инциденты, %



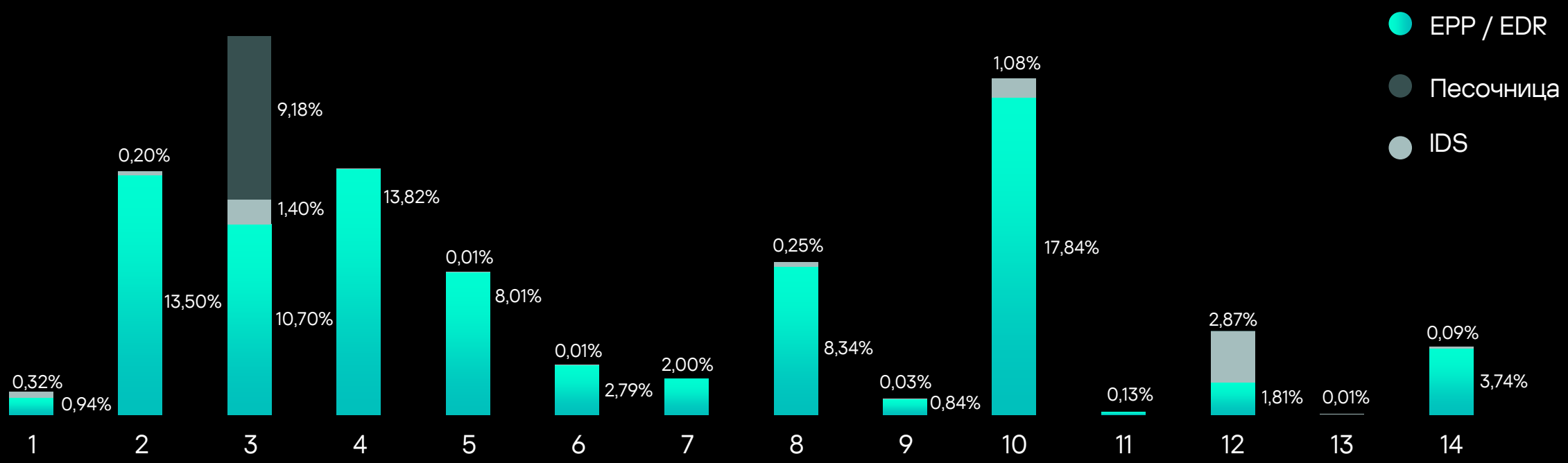
Песочница (SB) и сетевая система обнаружения вторжений (IDS) – компоненты платформы Kaspersky Anti Targeted Attack

EPP / EDR входят в Kaspersky Endpoint Security для бизнеса с подключенным сервисом MDR. Система обнаружения вторжений на уровне хоста (Host IDS) входит в EPP

Другое – запросы заказчиков и / или проблемы с покрытием хостов MDR

Технологии обнаружения

1 TA0043 Разведка
2 TA0042 Подготовка ресурсов
3 TA0001 Первоначальный доступ
4 TA0002 Выполнение
5 TA0003 Закрепление
6 TA0004 Повышение привилегий
7 TA0005 Предотвращение обнаружения
8 TA0006 Получение учетных данных
9 TA0007 Исследование
10 TA0008 Горизонтальное перемещение
11 TA0009 Сбор данных
12 TA0011 Управление и контроль
13 TA0010 Эксфильтрация данных
14 TA0040 Ущерб



Отчет за 2022 год: статистика и результаты

Инструменты и техники злоумышленников

Конверсия

Отношение событий безопасности, классифицированных как инциденты, к общему количеству событий безопасности, соответствующим конкретной технике MITRE ATT&CK

Характеризует эффективность логики обнаружения

Вклад

Отношение числа инцидентов, где наблюдалась та или иная техника, к общему количеству инцидентов

Характеризует результативность логики обнаружения

Техники с наибольшим показателем конверсии*

Техника	Конверсия
T1569: Вмешательство в системные службы	47,69%
T1110.001: Угадывание пароля	36,14%
T1496: Взлом ресурсов	32,02%
T1210: Эксплуатация удаленных служб	27,42%
T1546.008: Специальные возможности	24,98%
T1078: Существующие учетные записи	22,70%
T1098: Манипуляции с учетной записью	20,44%
T1021: Службы удаленного доступа	20,40%
T1055.002: Инъекция PE-файла	18,70%
T1003.001: Дамп учетных данных из памяти LSASS	17,74%
T1486: Шифрование данных	16,89%

Техника	Конверсия
T1485: Уничтожение данных	16,89%
T1561.001: Повреждение содержимого диска	16,89%
T1561.002: Повреждение структуры диска	16,89%
T1588.001: Вредоносное ПО	16,22%
T1588.002: Инструмент	14,95%
T1565.003: Манипуляция активными данными	14,92%
T1565.001: Манипуляция хранимыми данными	14,92%
T1565.002: Манипуляция передаваемыми данными	14,80%
T1587.001: Вредоносное ПО	14,42%
T1204.002: Вредоносный файл	13,14%
T1190: Эксплуатация уязвимости общедоступного приложения	11,99%

* Техники со вкладом более 1%, показано TOP-22 техники из 35

Техники с наибольшим вкладом*

Техника	Конверсия
T1204: Выполнение с участием пользователя	22,55%
T1566: Фишинг	17,82%
T1565: Манипуляция данными	9,65%
T1587: Разработка собственного ПО	9,36%
T1071: Протоколы прикладного уровня	8,55%
T1588: Подготовка необходимых ресурсов	7,48%
T1003: Получение дампа учетных данных	7,04%
T1021: Службы удаленного доступа	6,81%
T1078: Использование действительных учетных записей	5,63%
T1098: Манипуляция данными учетной записи	5,35%

Техника	Конверсия
T1059: Интерпретатор команд и сценариев	4,59%
T1569: Вмешательство в системные службы	2,89%
T1547: Автозапуск при загрузке или входе в систему	2,29%
T1561: Удаление данных с диска	2,16%
T1036: Маскировка	2,16%
T1110: Подбор пароля	1,78%
T1558: Кража или подделка билетов Kerberos	1,73%
T1055: Инъекция кода в процессы	1,56%
T1546: Выполнение по триггеру	1,49%

* Перечислены только техники со значениями выше 1%

Самые популярные LoL-утилиты

Инструмент	Все инциденты	Инциденты с высоким уровнем критичности
powershell.exe	1,29%	5,52%
rundll32.exe	1,02%	5,85%
msiexec.exe	0,44%	0,50%
reg.exe	0,22%	1,17%
comsvcs.dll	0,19%	1,51%
regsvr32.exe	0,15%	0,75%
certutil.exe	0,13%	0,67%

Основные выводы

Основные выводы

1

Более 30% всех критичных инцидентов связаны с целевыми атаками, проводимыми под управлением человека. Для их обнаружения необходимо использовать ручные методы активного поиска угроз в сочетании с традиционными методами мониторинга на основе оповещений.

2

Все целевые атаки были обнаружены механизмами защиты от вредоносного ПО. Ни одна атака не осталась незамеченной, если использовалось комплексное решение для защиты рабочих мест (эффективность различных технологий обнаружения указана в отчете).

3

Даже сложные атаки состоят из простых шагов и используют известные техники. Обнаружив конкретную технику, можно отследить всю атаку (техники, обнаружение которых оказалось эффективным или результативным, перечислены в отчете).

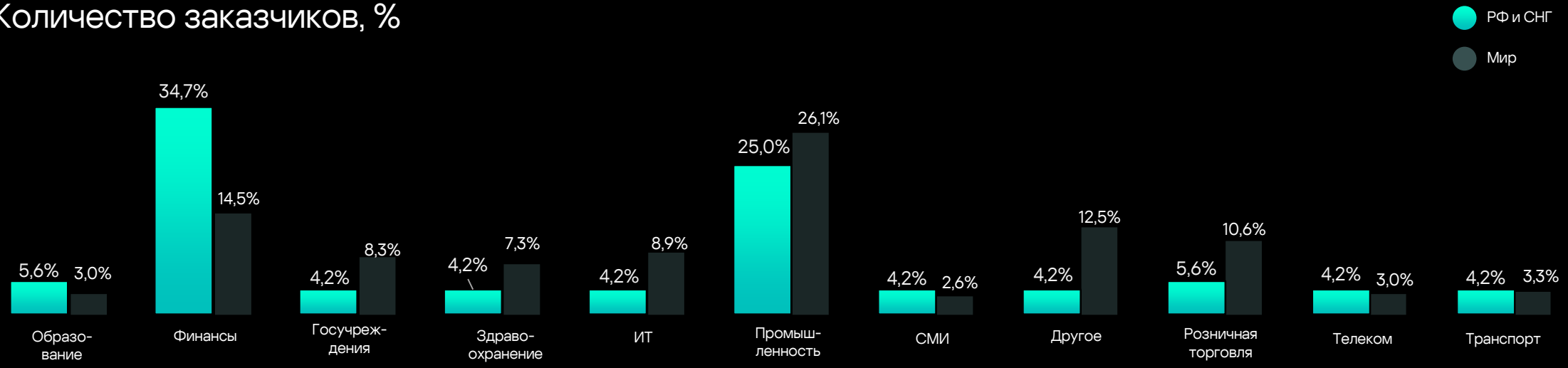
4

Различные технологии показывают различную эффективность в отношении тех или иных техник злоумышленников: необходимо использовать несколько защитных решений чтобы повысить вероятность обнаружения (как минимум на уровне рабочих мест и на уровне сети).

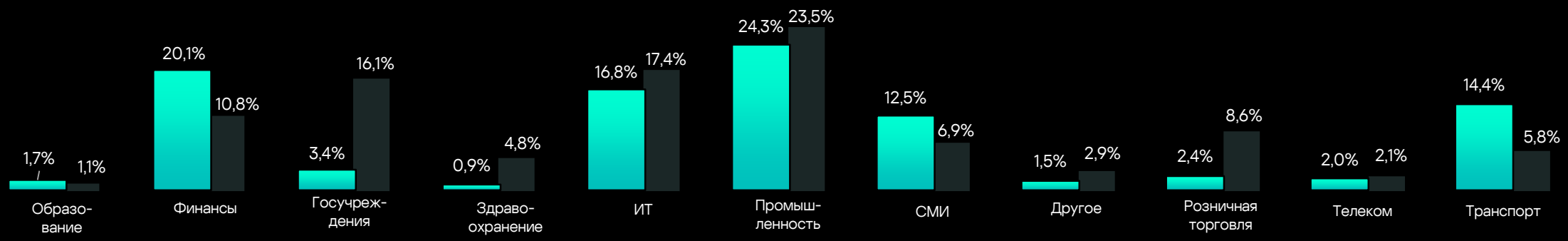
Российская специфика

Охват сервисом MDR (СНГ и Мир)

Количество заказчиков, %

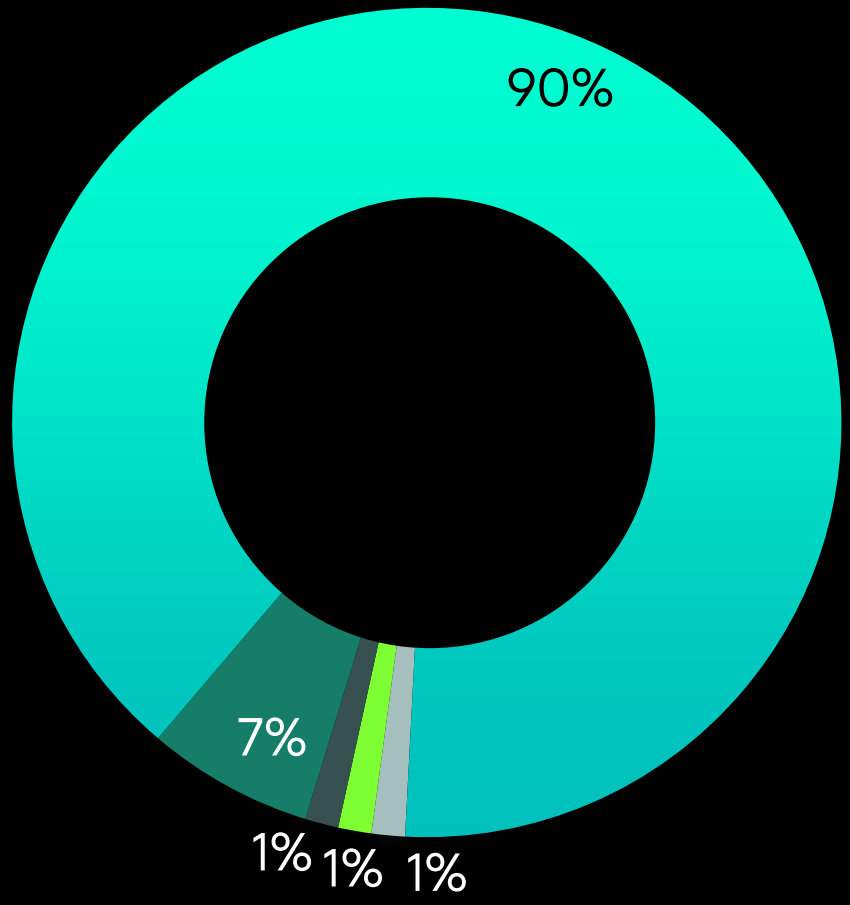


Количество инцидентов, %



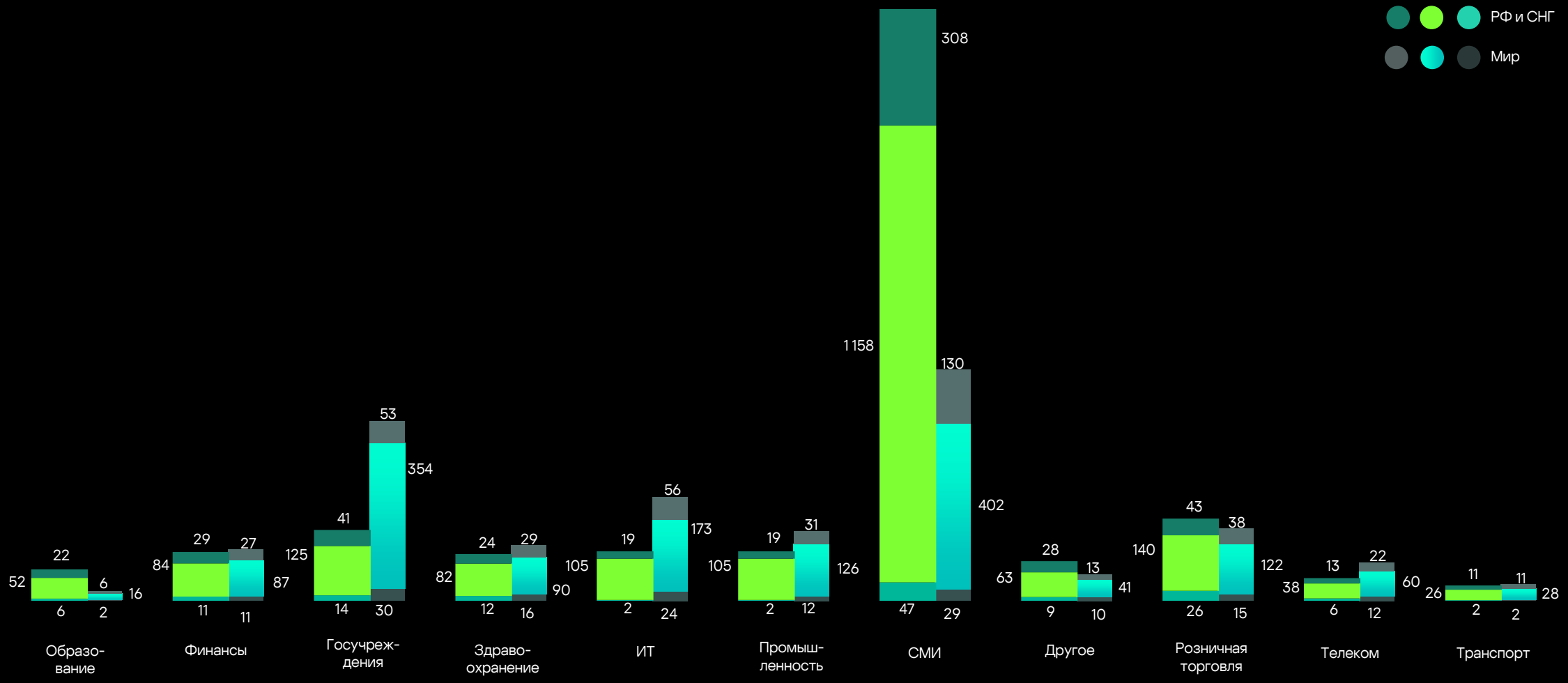
Количество организаций

- Россия
- Казахстан
- Грузия
- Азербайджан
- Армения



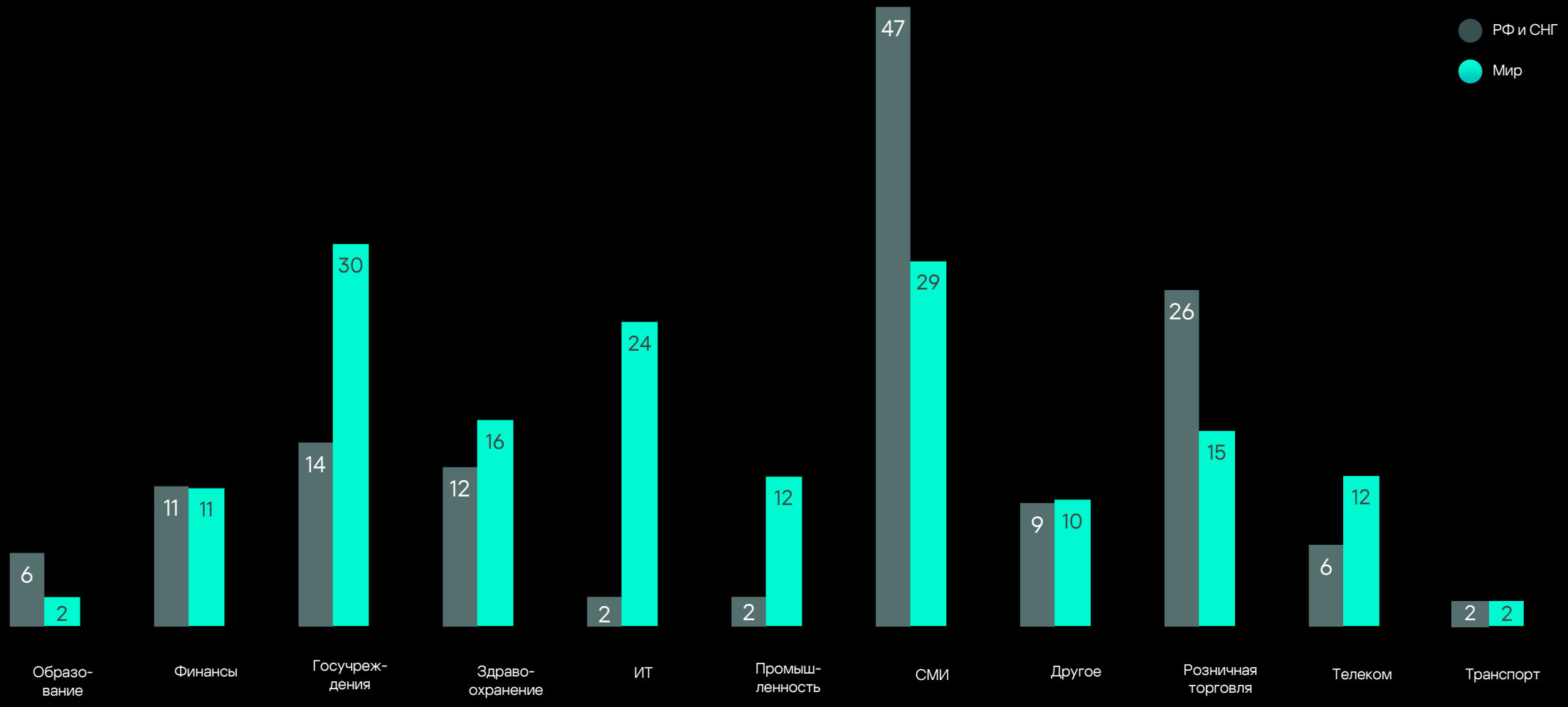
Критичность инцидентов

Критичность инцидентов по отраслям (СНГ и Мир)*



* Количество инцидентов в отношении на 10 000 конечных точек

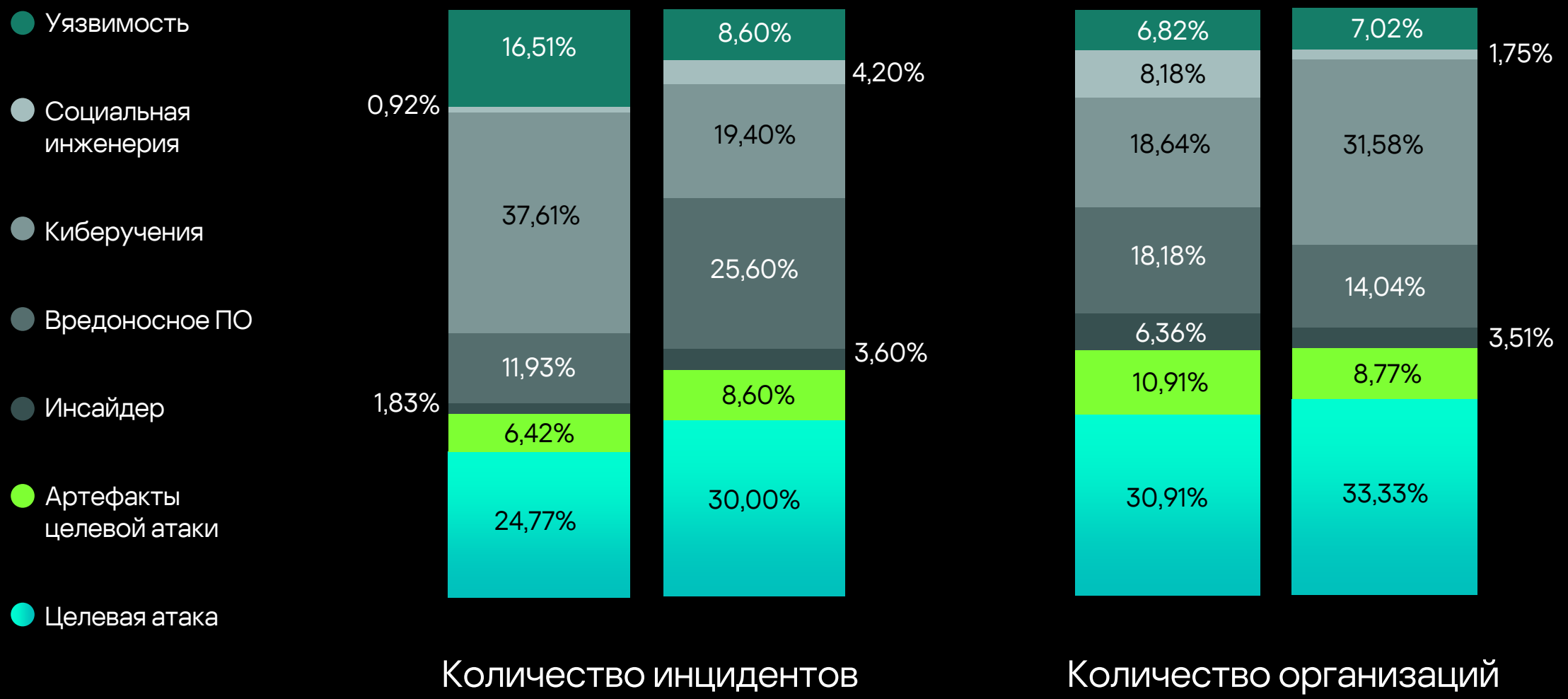
Количество критичных инцидентов (СНГ и Мир)*



* Количество инцидентов в отношении на 10 000 конечных точек

Природа критичных инцидентов

Типы критичных инцидентов (СНГ и Мир)



Хотите узнать подробности акции?

Отсканируйте QR-код
или просто перейдите по ссылке

https://kas.pr/offer-mdr-free