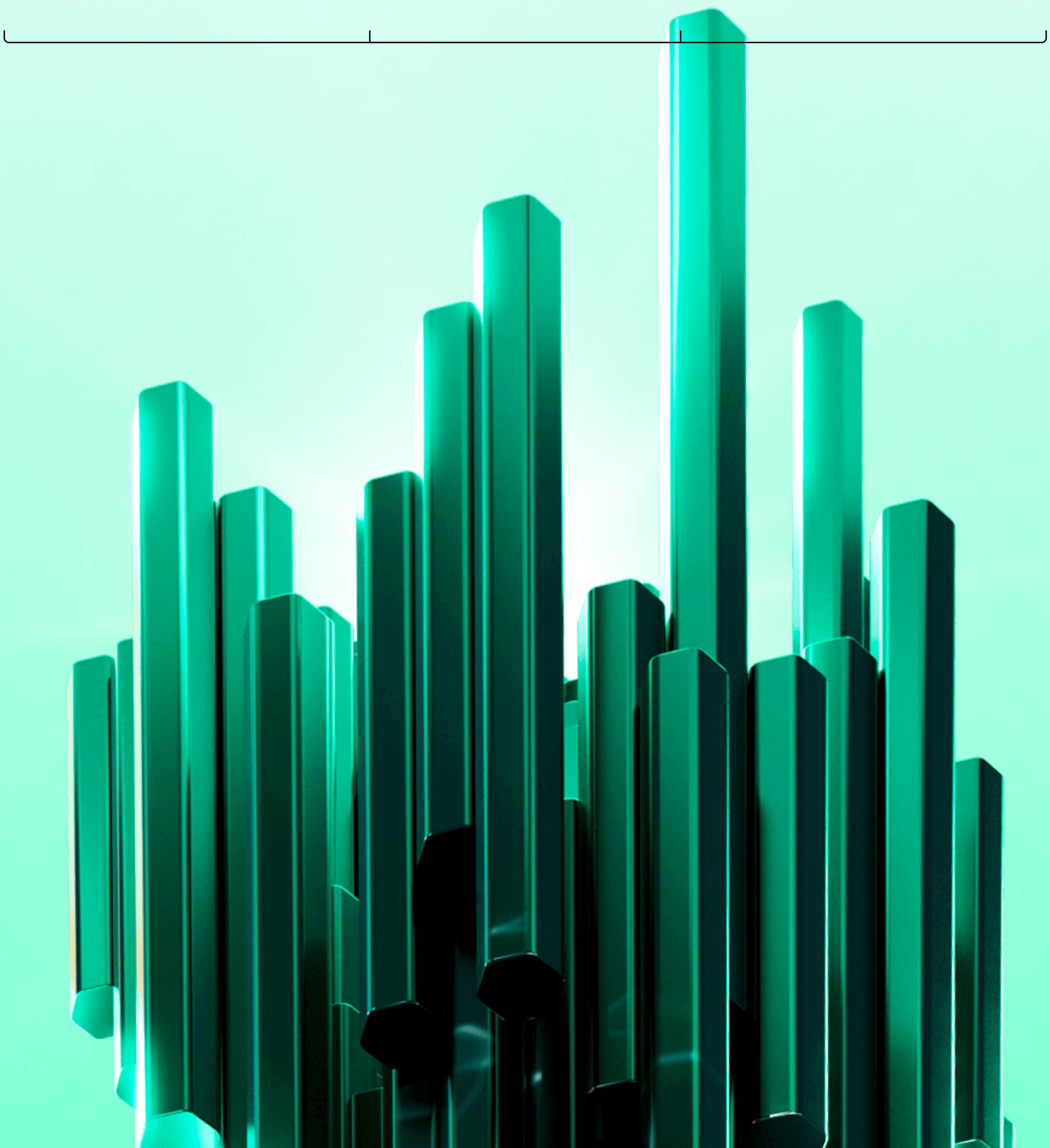
kaspersky

2022

АНАЛИТИЧЕСКИЙ ОТЧЕТ | MDR | SOC

MANAGED DETECTION AND RESPONSE

от Центра мониторинга кибербезопасности «Лаборатории Касперского»



Оглавление

Введение

Ежегодный аналитический отчет Managed Detection and Response освещает результаты анализа инцидентов, выявленных командой Центра мониторинга кибербезопасности (SOC) «Лаборатории Касперского».

Целью отчета является предоставление сведений о наиболее часто встречающихся тактиках и техниках атакующих, характере выявленных инцидентов и их распределении по отраслям и географии.

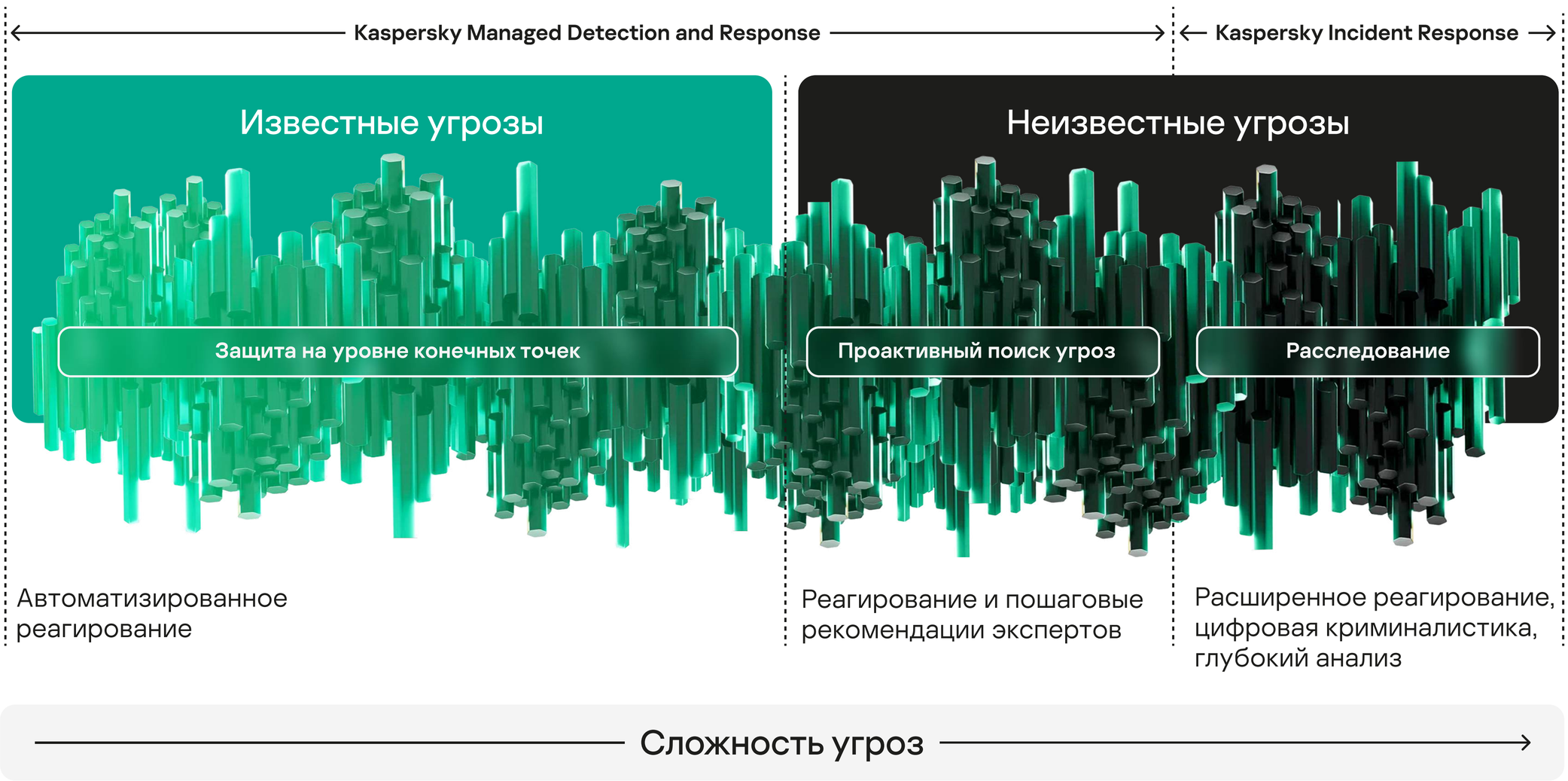
Этот отчет поможет получить ответы на следующие вопросы:

- Кто ваши потенциальные атакующие?
- Как можно обнаружить их действия?
- Как они действуют сегодня?

Подход «Лаборатории Касперского» к выявлению инцидентов и реагированию на них

Благодаря сервисам Kaspersky Managed Detection and Response (MDR) и Kaspersky Incident Response (IR) «Лаборатория Касперского» покрывает полный цикл управления инцидентами — от выявления угрозы до восстановления после атаки.

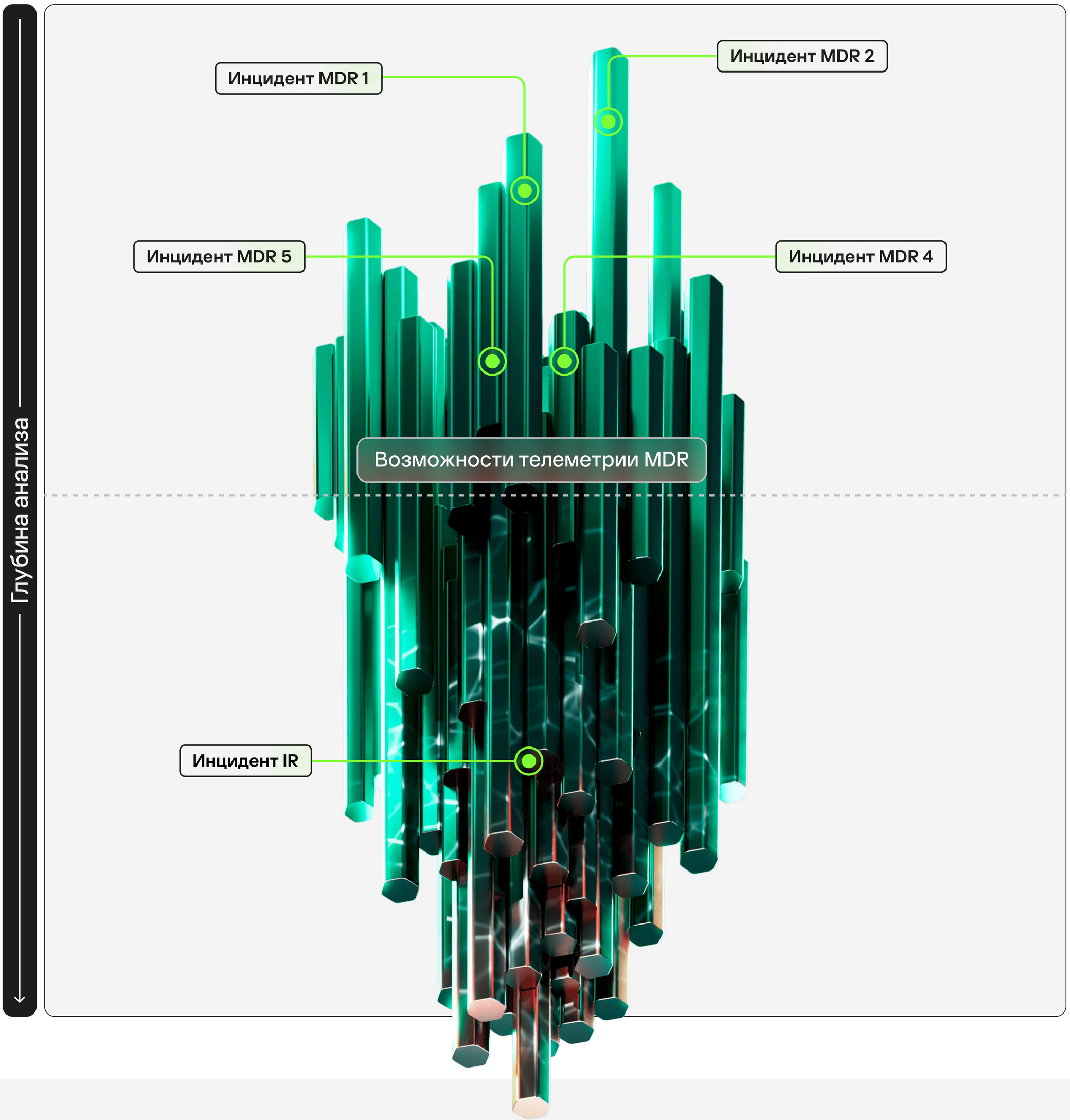
Основной целью сервиса MDR является обнаружение угроз на всех этапах атаки — как до фактической компрометации, так и после проникновения злоумышленников в инфраструктуру организации. Это достигается за счет превентивных систем безопасности и активного поиска угроз (threat hunting), являющихся неотъемлемыми компонентами MDR.



Расследование и обеспечение реагирования на инцидент также предоставляются в рамках MDR, однако их глубина ограничена возможностями используемого технологического стека. Если требуются глубокий анализ артефактов и расширенные возможности по реагированию, не ограниченные каким-либо фиксированным набором инструментов, возможно привлечение команды Incident Response, которая адаптивно выработает оптимальный план в рамках расследования*.

* Сервисы MDR и IR могут приобретаться совместно. При этом каждый выявленный MDR-инцидент по решению заказчика может быть передан в команду IR в случае, если требуется расширенное реагирование, выходящее за рамки MDR. Как правило, это инциденты высокого уровня критичности при непосредственном участии атакующих.

Активность атакующего в рамках инцидента

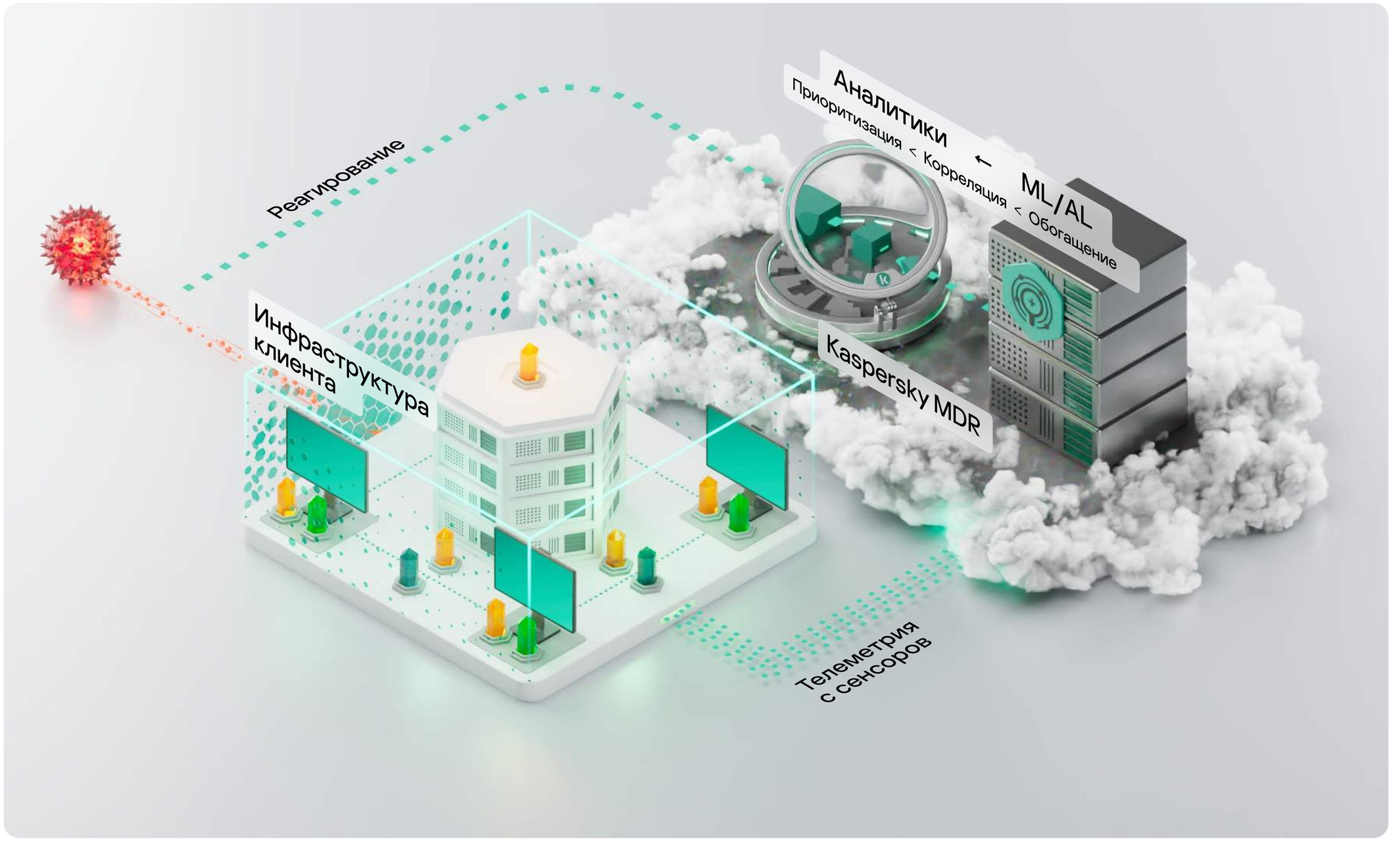


О Kaspersky Managed Detection and Response (MDR)

Kaspersky MDR — это сервис круглосуточного мониторинга и реагирования на выявленные инциденты, основанный на технологических решениях и экспертизе команды SOC «Лаборатории Касперского»*.

Решения для защиты конечных точек, установленные на стороне заказчика, собирают и передают телеметрию, которая дальше анализируется с использованием технологий машинного обучения и при непосредственном участии экспертов SOC. При этом сенсоры защиты конечных точек обеспечивают реагирование.

Аналитики SOC расследуют события безопасности (alerts) и оповещают клиента о вредоносной активности, предоставляя инструментальное реагирование и рекомендации.



* Поддерживаются все продукты для защиты конечных точек, а также Kaspersky Anti Targeted Attack.

Основные выводы 2022

Общая статистика по инцидентам

3+ критичных инцидента ежедневно

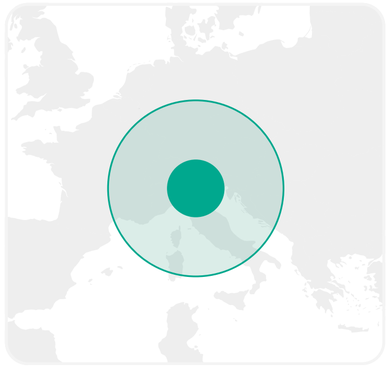
43,8 мин. Среднее время обнаружения инцидента высокого уровня критичности

72% инцидентов были успешно устранены после получения одного события безопасности

Отрасли с наибольшим количеством зафиксированных инцидентов

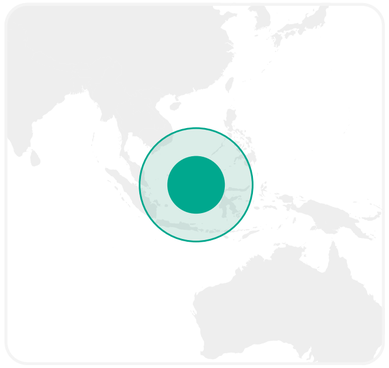
- Промышленный сектор — 22%
- Информационные технологии — 16%
- Госучреждения — 15%

Ключевые регионы



Европа — 44%

Россия и СНГ — 25%



АТР — 15%

Распределение инцидентов по критичности

- Высокая — 8,1%
- Средняя — 71,8%
- Низкая — 20,1%

Наиболее часто встречающийся профиль атакующих

- Целевая атака — 30%
- Криминал* — 26%
- Анализ защищенности — 19%

Наиболее популярные техники MITRE ATT&CK

- **T1210** Эксплуатация удаленных служб
- **T1078** Существующие учетные записи
- **T1098** Манипуляции с учетной записью

Наиболее популярные инструменты атакующих

- powershell.exe — 1,29%
- rundll32.exe — 1,02%
- msiexec.exe — 0,44%

* Атака, выполняемая с использованием вредоносного ПО без видимого участия человека.

Общие рекомендации

Многоуровневый подход к защите

В связи с тем что более 25% инцидентов высокого уровня критичности связаны с вредоносными программами, необходим многоуровневый подход к ИБ-защите.

Threat Hunting

В связи с ежегодным увеличением количества целевых атак, осуществляемых при непосредственном участии человека, рекомендуется внедрение инструментов для активного поиска угроз (threat hunting) в сочетании с классическим мониторингом событий безопасности, что позволяет эффективно обнаруживать угрозы.

Для технологической поддержки активного поиска угроз рекомендуется использовать профессиональные инструменты: платформы управления данными об угрозах, специализированные изолированные среды и системы атрибуции угроз для определения правильных защитных мер.

Threat Intelligence

Любая целевая атака предполагает тщательную подготовку, и на этом этапе классические системы безопасности бессильны против действий злоумышленников, так как отсутствует активное воздействие на инфраструктуру. Рекомендуется уделять особое внимание тактическим, операционным и стратегическим данным об угрозах, относящихся непосредственно к вашей организации. Немаловажным здесь является анализ техник и инструментов известных APT кампаний и киберкриминальных группировок.

Реагирование на инциденты

Успех управления инцидентами во многом зависит от корректного реагирования на выявленные угрозы: насколько эффективно проведен анализ обнаруженных подозрительных объектов, корректно ли интерпретированы все артефакты, правильно ли организован процесс реагирования.

Red Teaming

Проведение киберучений с участием Red Team является эффективным способом тренировки команд по обнаружению атак и оценки безопасности организации.

MITRE ATT&CK®

Использование базы знаний MITRE ATT&CK® позволяет эффективно обнаруживать сложные атаки, которые могут состоять из простых шагов и техник. Рекомендуется использовать эту базу знаний в сочетании с другими инструментами обнаружения и защиты.

Ландшафт инцидентов MDR в мире

Основные атакуемые отрасли

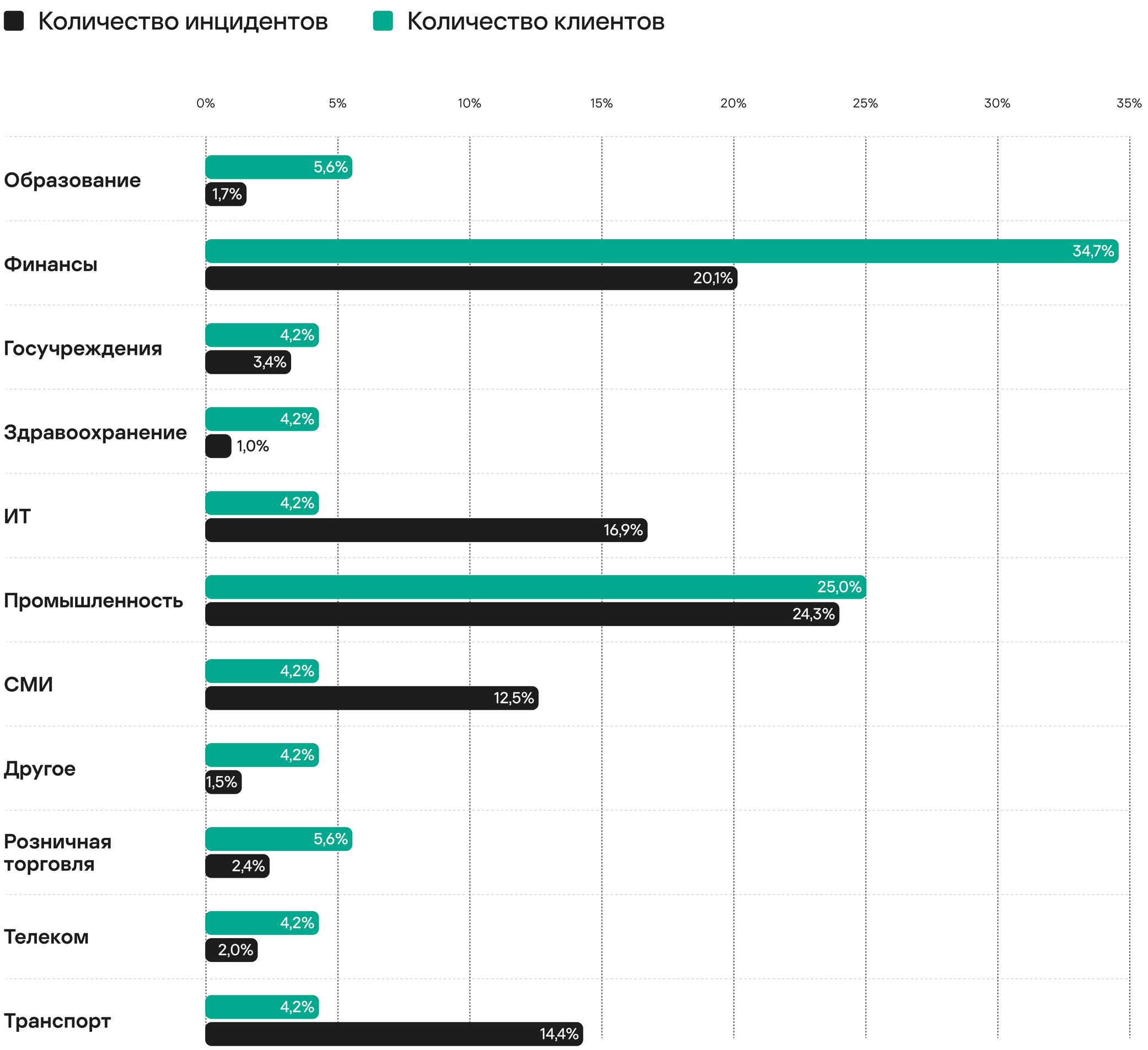
В 2022 году наибольшее количество инцидентов MDR фиксировалось в промышленном секторе (22,3%), государственных учреждениях (15,3%), ИТ-компаниях (16,4%), финансовых организациях (10,2%), на предприятиях розничной торговли (8,1%) и в СМИ (6,6%).

Ландшафт инцидентов MDR в России и СНГ

Основные атакуемые отрасли

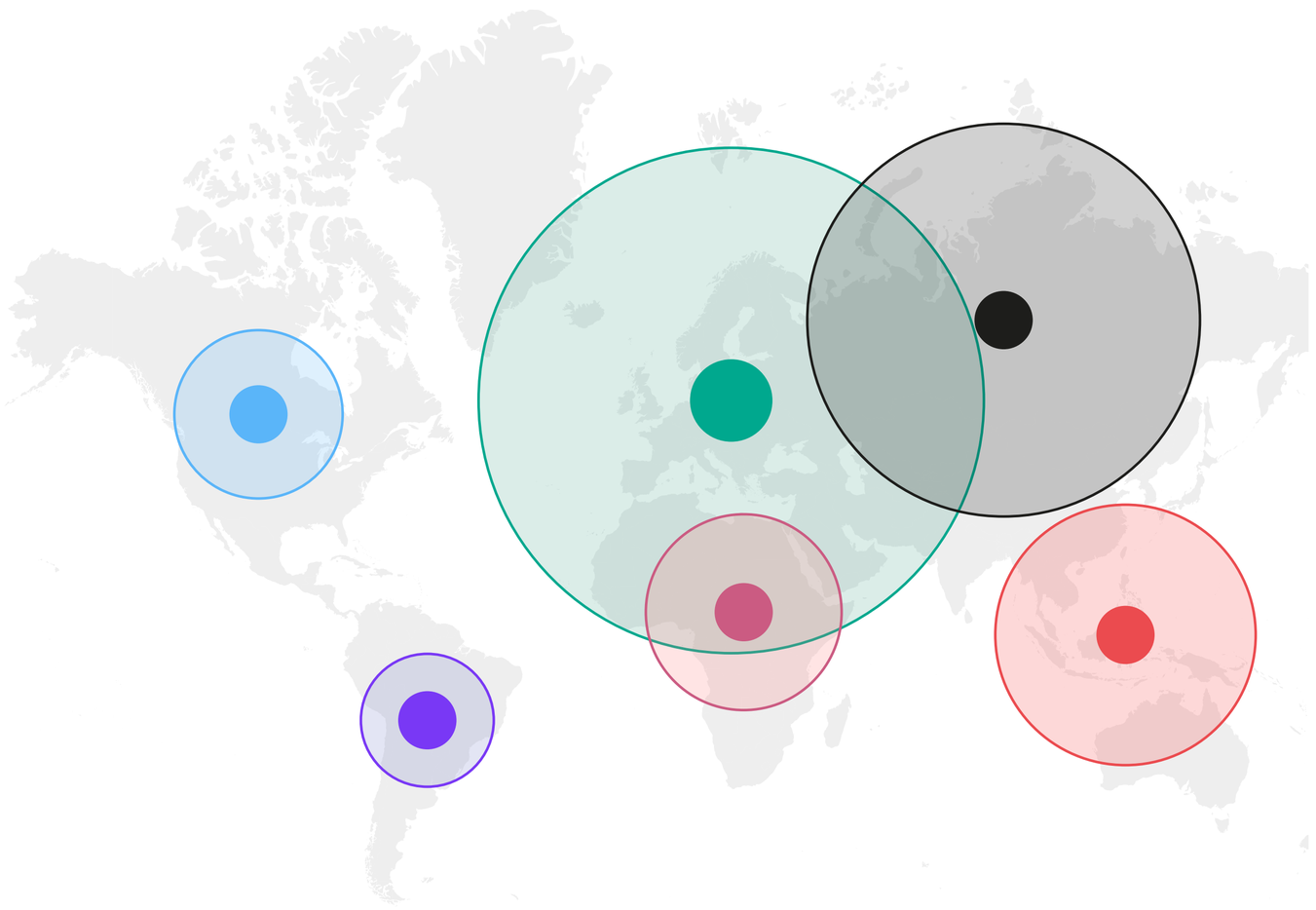
Наиболее атакуемыми отраслями в этом регионе в 2022 году были промышленность (24,3%), финансовые организации (20,1%), ИТ-компании (16,9%), транспорт (14,4%) и СМИ (12,5%).

Данные по инцидентам, зафиксированным Kaspersky MDR в России и СНГ, могут значительно отличаться от мировой статистики, и именно поэтому эти данные представлены в отчете отдельно.



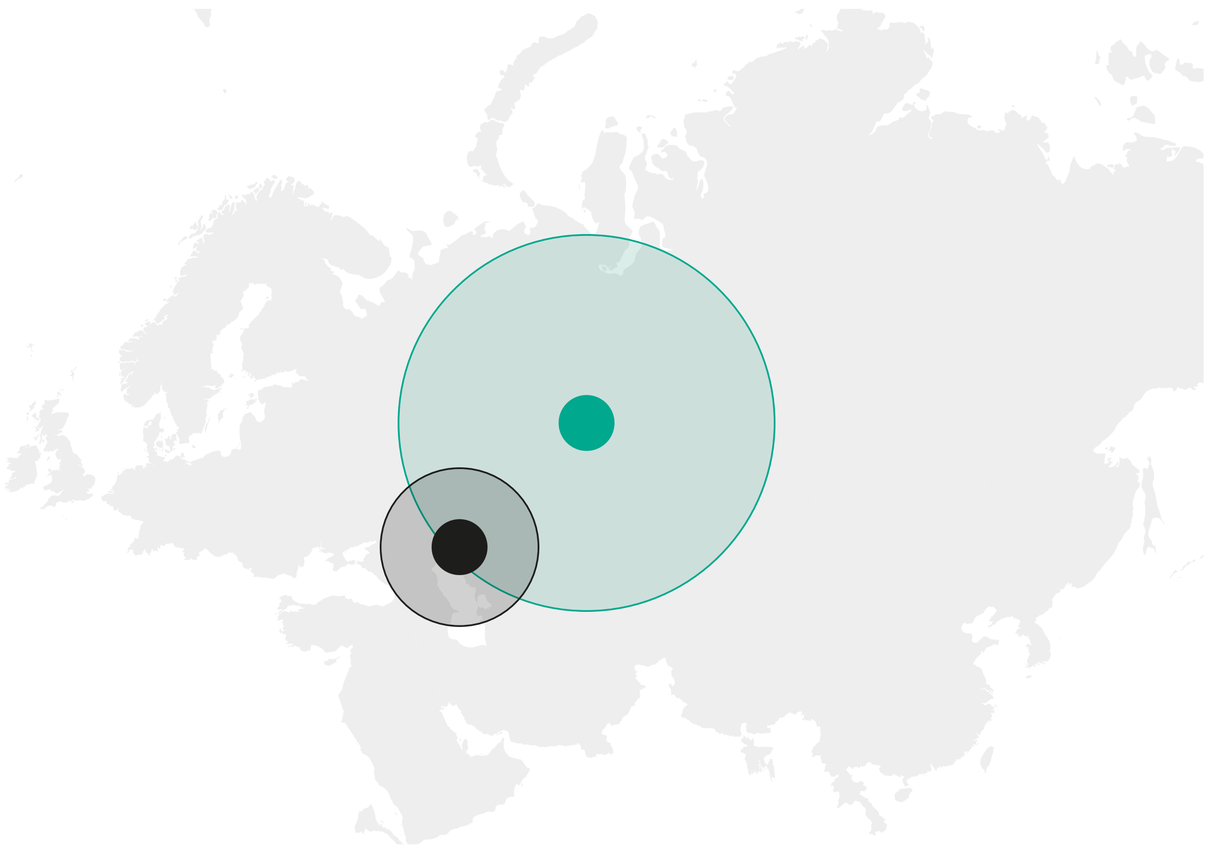
География покрытия Kaspersky MDR

Для того чтобы иметь полное представление об угрозах, необходимо получать информацию из разных регионов, так как мотивация, тактики и техники атакующих имеют географическую специфику.



Регион	%
Европа	44
Россия и СНГ	25
АТР	15
Ближний Восток	8
Северная Америка	5
Латинская Америка	3

Россия и СНГ находятся на втором месте в мире с точки зрения покрытия сервисом MDR: при этом 90% клиентов приходится на Россию.



Страна	%
Россия	90
СНГ	10

Количество реальных инцидентов MDR в 2022 году

В 2022 году инфраструктура MDR ежедневно получала огромное количество телеметрии, в результате процесса обработки которой формировались события безопасности (алерты).

Около 33% событий были обработаны алгоритмами на основе машинного обучения. Еще около 11% были проанализированы экспертами SOC и оказались следствием реальных инцидентов, о которых клиентов информировали через портал MDR.

433 000+

событий безопасности

292 000+

событий было проанализировано аналитиками SOC.

Из них **122 000+** событий в России и СНГ

141 000+

событий безопасности было обработано автоматически с помощью технологий ИИ

33 000+

событий безопасности было классифицировано как следствия реальных инцидентов

12 000+

реальных инцидентов зафиксированы в 2022 году.

Из них **4100+** инцидентов в России и СНГ

~14 000

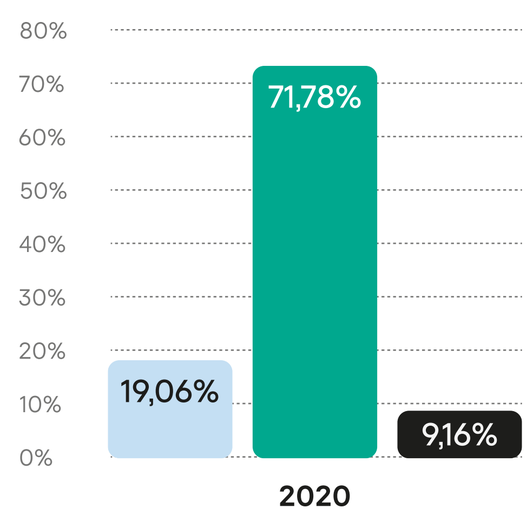
событий телеметрии с одного хоста. Этот показатель может существенно меняться в зависимости от активности хоста и типа сенсора

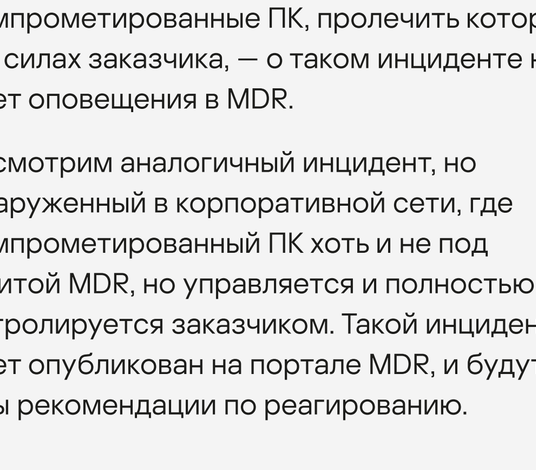
89%

событий безопасности было отклонено аналитиками SOC «Лаборатории Касперского» как ложноположительные

Критичность инцидентов

В 2022 году мы ежедневно обнаруживали более трех инцидентов высокой критичности. В сравнении с предыдущими годами доля критичных инцидентов сохраняется в пределах 10%. Исключение составил 2021 год, когда атак такого типа стало более 14%.





Мы сообщаем заказчикам только об инцидентах, на которые возможна эффективная реакция с их стороны*.

Высокая → 8,13% — Атака с участием человека или вирусное заражение, оказывающее серьезное воздействие на бизнес

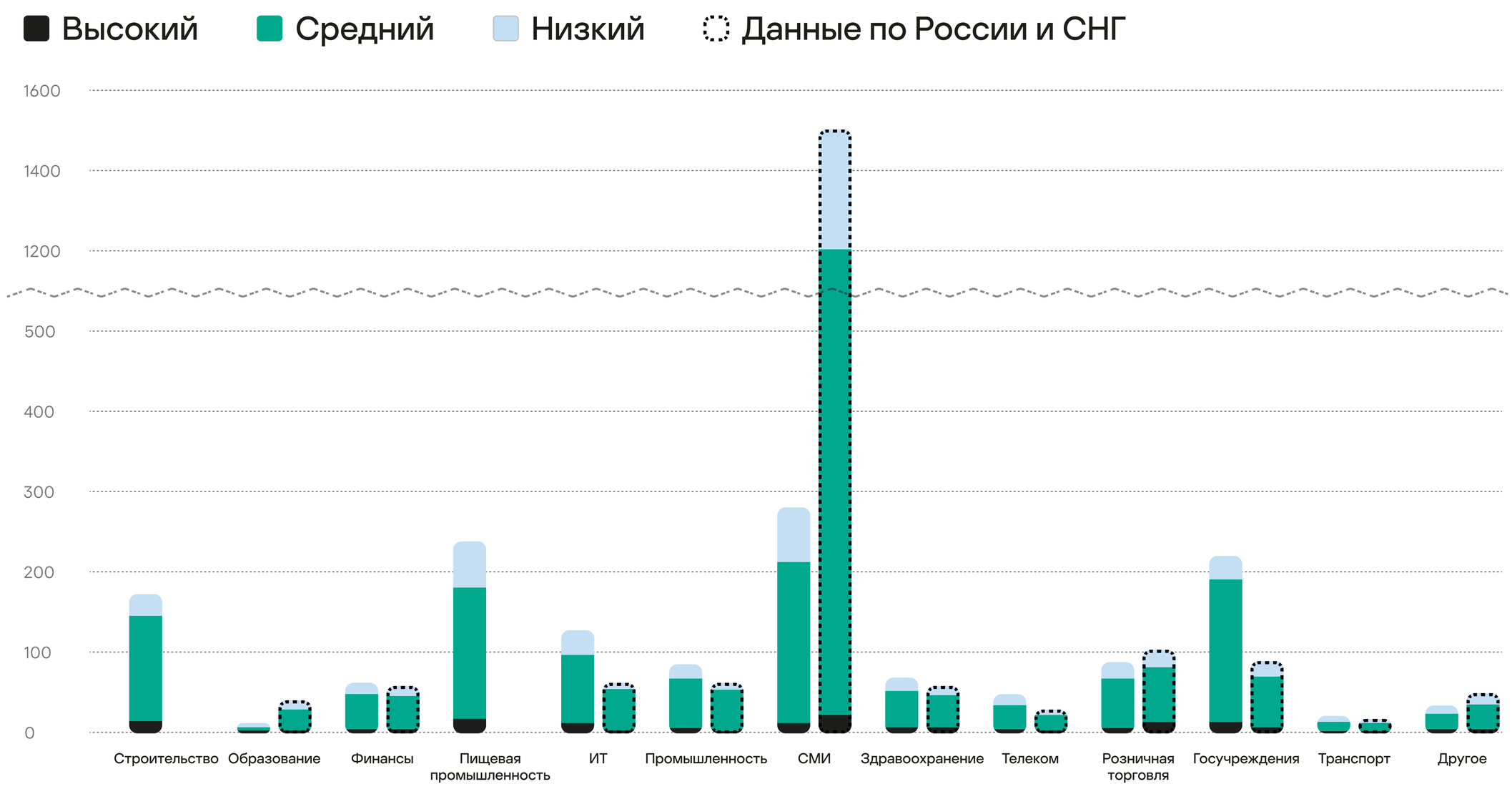
Средняя → 71,82% — Нет подтверждений участия человека; атака способна повлиять на бизнес, но без тяжелых последствий

Низкая → 20,05% — Без существенного воздействия на бизнес; тем не менее существуют мероприятия, которые повысят уровень безопасности

* Например, если портативный ПК подключен к публичной БЛВС и система предотвращения сетевых вторжений фиксирует попытки эксплуатации EternalBlue — это, безусловно, инцидент. Однако он не требует реакции, так как к публичной БЛВС нередко подключаются скомпрометированные ПК, пролечить которые не в силах заказчика, — о таком инциденте не будет оповещения в MDR.

Рассмотрим аналогичный инцидент, но обнаруженный в корпоративной сети, где скомпрометированный ПК хоть и не под защитой MDR, но управляется и полностью контролируется заказчиком. Такой инцидент будет опубликован на портале MDR, и будут даны рекомендации по реагированию.

Уровень критичности инцидента



Высокий	Мир	Россия и СНГ
Строительство	34,15	-
Образование	2,28	5,68
Финансы	10,86	10,71
Пищевая промышленность	38,45	-
ИТ	23,97	2,37
Промышленность	11,78	2,37
СМИ	28,75	46,92
Здравоохранение	16,23	12,16
Телеком	11,83	6,29
Розничная торговля	15,37	25,53
Госучреждения	30,11	14,01
Транспорт	1,97	1,57
Другое	9,96	9,45

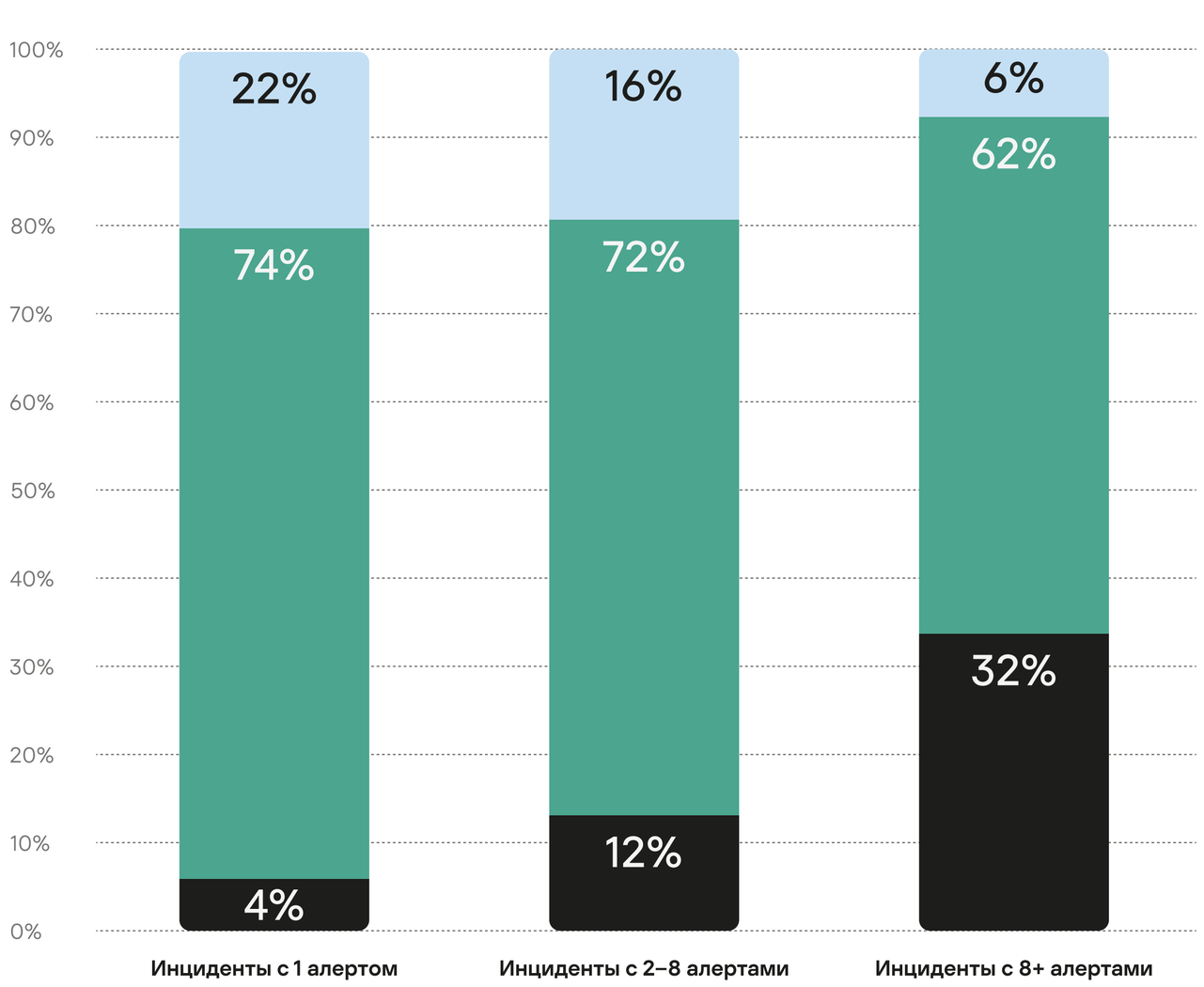
Средний	Мир	Россия и СНГ
Строительство	258,54	-
Образование	15,57	52,27
Финансы	87,22	84,47
Пищевая промышленность	326,82	-
ИТ	173,06	104,53
Промышленность	126,12	104,53
СМИ	401,82	1158,36
Здравоохранение	89,53	82,07
Телеком	59,92	37,76
Розничная торговля	121,73	140,43
Госучреждения	354,45	124,86
Транспорт	27,62	26,49
Другое	41,17	62,99

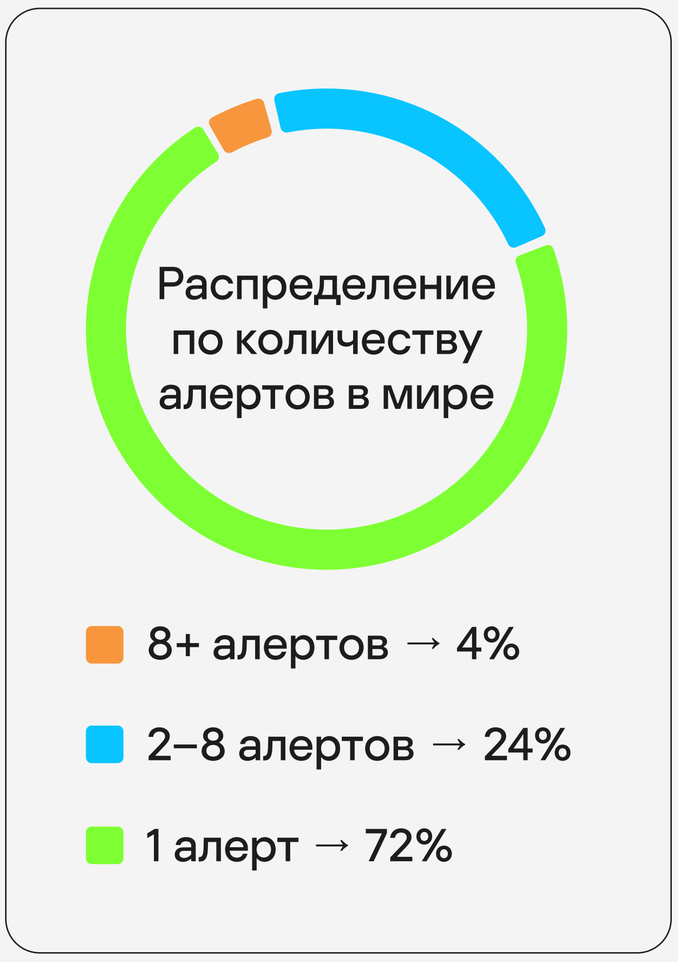
Низкий	Мир	Россия и СНГ
Строительство	58,54	-
Образование	5,50	21,59
Финансы	27,16	28,55
Пищевая промышленность	109,74	-
ИТ	56,01	18,69
Промышленность	31,22	18,69
СМИ	130,43	307,92
Здравоохранение	29,02	24,32
Телеком	21,76	13,29
Розничная торговля	37,99	42,55
Госучреждения	53,16	40,77
Транспорт	11,41	10,95
Другое	12,64	28,35

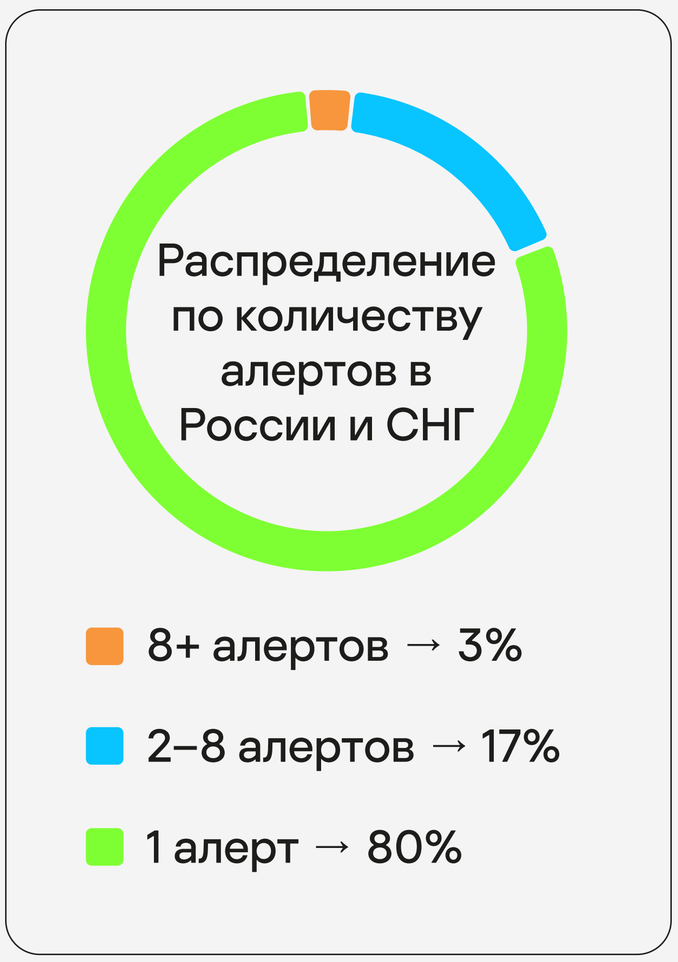
На приведенной выше диаграмме отражено количество инцидентов в отношении к 10 000 конечных точек в мониторинге, распределенное по индустриям.

- Из диаграммы следует, что наибольшая интенсивность атак в 2022 году наблюдалась в сфере СМИ, но инциденты эти были главным образом средней и низкой критичности, то есть крайне редко представляли собой целевые атаки с активным участием атакующего.
- Интересно также отметить, что прошлогодний лидер по количеству высококритичных инцидентов — телеком — в этом году ничем не выделяется.

Эффективность реагирования







72% инцидентов было обнаружено на основе одного события безопасности, после чего атака была остановлена, что свидетельствует о высокой эффективности реакции. В эту категорию попадают типовые инциденты с четкими сценариями реагирования*. Доля критичных инцидентов здесь самая низкая — 4%; подавляющее большинство за инцидентами среднего (74%) и низкого (22%) уровня критичности.

24% инцидентов выявлено на основе 2-8 событий безопасности. Для затруднения обхода обнаружения для одной и той же угрозы мы используем набор технологий, создающих разные события безопасности. Эта категория отражает инциденты, не отработанные полностью автоматически после первого же события безопасности: либо к реагированию подключался человек, либо корректная классификация инцидента была выполнена не с первого релевантного алерта.

4% инцидентов связано с 8 и более событиями безопасности. Это случаи, когда реакция была отклонена клиентом или была неэффективна: новая целевая атака, требующая тщательного расследования перед реагированием, или клиент запросил мониторинг атаки без активного противодействия (сценарий киберучений). Доля инцидентов высокого уровня критичности здесь самая большая — 32%, а низкого — всего 6%.

* Примерами могут являться: подмена файлов функционала специальных возможностей Windows (T1546.008), атака грубой силы (T1110), обнаружение песочницей в составе KATA (T1566.001) без дальнейшего развития на конечных точках и многие другие инциденты.

Скорость обнаружения инцидента

Время на обработку инцидента

Критичность

Высокая

Время на обработку, мин.

Самые сложные инциденты, требующие наибольшего времени на дополнительное обогащение данных и составление хронологии событий.

В сравнении с предыдущими периодами это время увеличилось на ~6%, что связано с ростом инцидентов с участием человека в 2022 году, расследование которых требует большего вовлечения аналитиков SOC и в меньшей степени поддается автоматизации.

Критичность

Средняя

Время на обработку, мин.

Наиболее распространенный уровень критичности. Бóльшая часть таких инцидентов — последствия активности вредоносного ПО.
В сравнении с предыдущими периодами это время сократилось за счет повышения уровня автоматизации обработки новых типов инцидентов.

Критичность

Низкая

Время на обработку, мин.

Инциденты самого низкого уровня критичности, бóльшая часть которых связана с последствиями использования нежелательного ПО, провели больше времени в очереди. Для этого типа инцидентов реализовано множество механизмов автоматизации, что привело к ощутимому сокращению участия аналитиков SOC в их обработке и, следовательно, сокращению времени на эти работы.

Процесс обнаружения инцидента

1. Распределение событий

Специализированный алгоритм распределяет событие безопасности из общего потока в очередь доступному аналитику SOC.

2. Анализ алерта

Аналитик обрабатывает алерт, исходя из уровня критичности и гарантированного SLA*.

3. Проверка на ложное срабатывание

Если анализ показывает ложное срабатывание**, событие безопасности игнорируется и создаются клиентские и (или) глобальные фильтры***.

4. Создание инцидента

В противном случае событие безопасности импортируется в новый или существующий инцидент, который или может быть закрыт как ложное срабатывание, или может быть передан клиенту через портал MDR вместе с рекомендуемой реакцией.

5. Выполнение рекомендаций

Если клиент согласовывает рекомендации по реагированию, то это приводит к их автоматическому выполнению агентами на конечных точках.

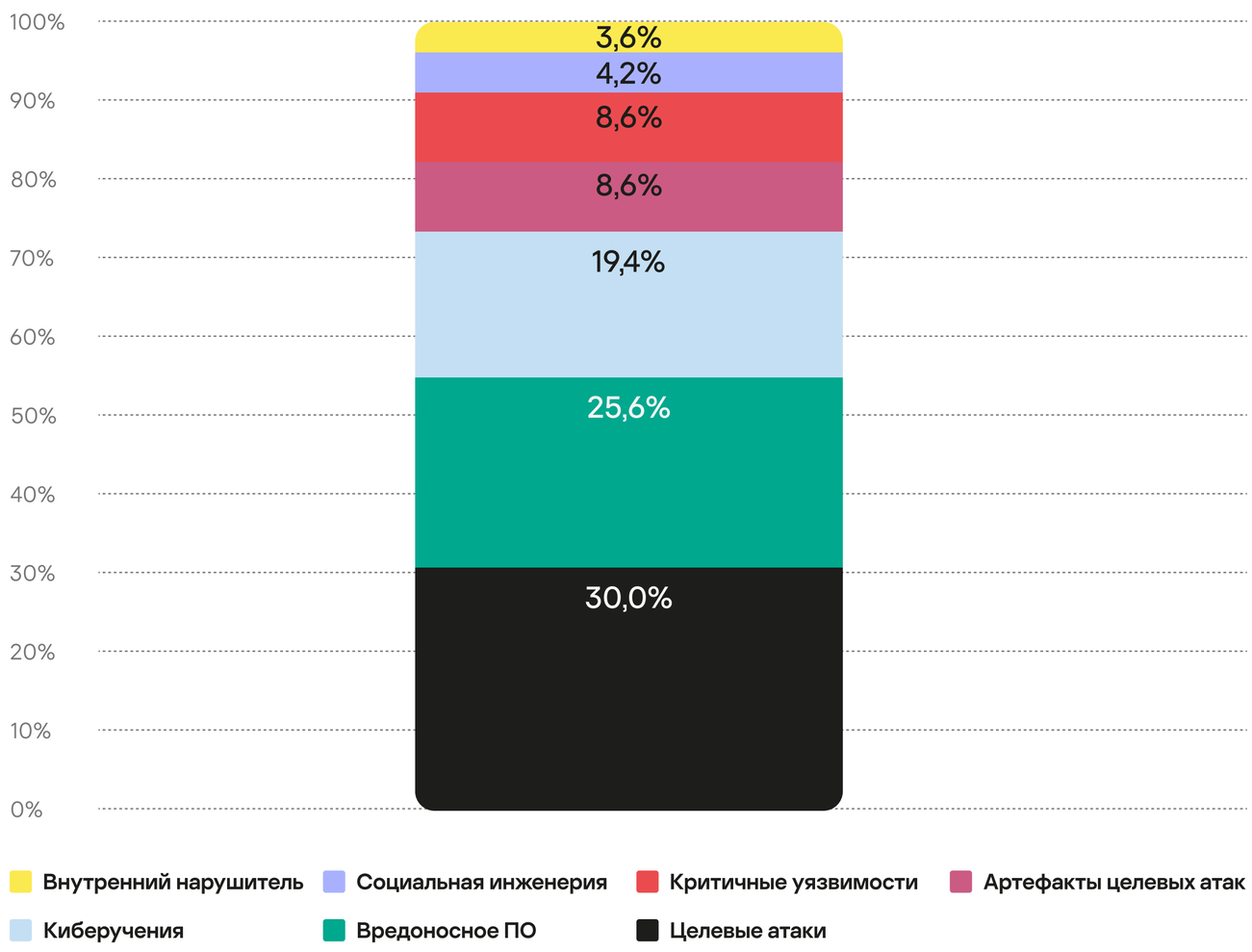
* SLA — соглашение об уровне сервиса (Service Level Agreement).

** Мы различаем два основных типа ложных срабатываний: инфраструктурное — логика создания события безопасности корректна, но из-за особенностей инфраструктуры заказчика данное оповещение не является следствием инцидента; технологическое — логика создания события безопасности работает неправильно и требует корректировки.

*** Клиентский фильтр — это настройка логики обнаружения под конкретную инфраструктуру заказчика; такие фильтры создаются для исправления инфраструктурных ложных срабатываний. Глобальный фильтр — корректировка логики обнаружения глобально для всех клиентов в случае технологических ложных срабатываний.

Природа критичных инцидентов

Основные причины



Распределение по количеству компаний в значительной степени повторяет статистику по количеству инцидентов.

Лидеры аналогичны

31% компаний столкнулись с целевыми атаками

19% киберучения

18% вредоносное ПО с дальнейшим воздействием на бизнес

30% всех выявленных в 2022 году критичных инцидентов было связано с целевыми атаками с непосредственным участием человека.

Большое количество инцидентов этого типа также может быть связано и с разного рода киберучениями, так как в обоих случаях наблюдается активная работа атакующего, и по умолчанию мы их классифицируем как «Целевые атаки» и изменяем тип инцидента на «Киберучения» только при получении явного подтверждения от заказчика.

Атаки вредоносного ПО с серьезными последствиями составили почти 26%.

Киберучения (тестирование на проникновение, учения с участием Red Team и т.п.) превысили 19%.

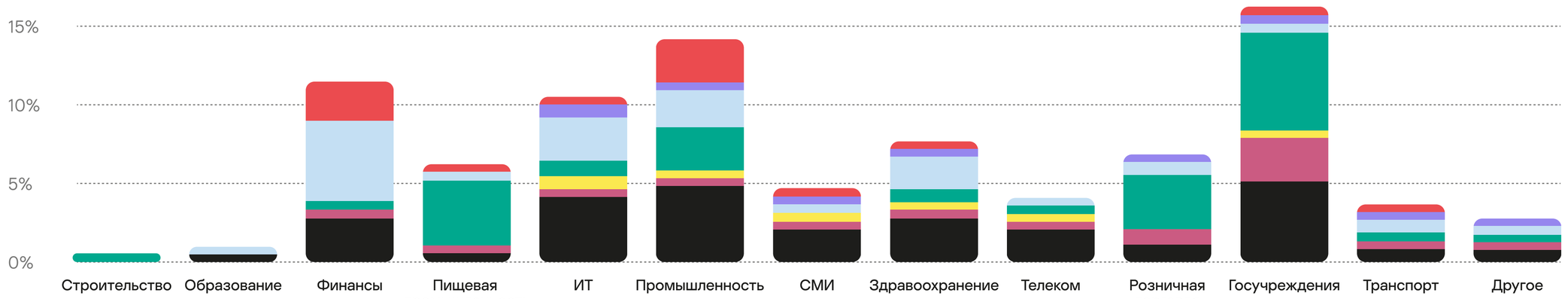
Около 9% — доля инцидентов, связанных с публично доступными критичными уязвимостями, и инцидентов, основанных на обнаружении следов ранее активных атак с участием человека (целевые атаки или киберучения).

Около 4% инцидентов — результат успешного использования социальной инженерии с последующим развитием, приведшим к серьезным последствиям.

Немногим менее 4% инцидентов было связано с внутренними нарушителями*.

* В инцидентах такого типа нам не удалось выявить каких-либо признаков внешних злоумышленников; подозрительные действия выполнялись от имени легитимных привилегированных учетных записей. В связи с отсутствием информации от клиентов о том, была ли обнаруженная активность легитимной или нет, нет оснований классифицировать эти инциденты как ложноположительные (например, это могли быть попытки проверить оперативную готовность сервиса MDR или действительно незаконные действия ИТ-персонала, о которых заказчики предпочли нам не сообщать).
Ввиду наличия из года в год небольшой доли таких инцидентов начиная с 2023 года мы ввели дополнительный тип инцидента — «Нарушение политики безопасности», которым будут помечаться критичные инциденты, выполненные от легитимных учетных записей без следов их компрометации. Пометка «Внутренний нарушитель» будет ставиться только при наличии подтверждения инцидента с участием внутреннего нарушителя.

Количество критичных инцидентов по отраслям



Киберучения	%
Финансы	5,00
ИТ	3,20
Промышленность	2,20
Здравоохранение	2,20
Розничная торговля	1,40
Транспорт	1,20
Другое	1,00
Пищевая промышленность	0,80
СМИ	0,80
Образование	0,60
Госучреждения	0,60
Телеком	0,40

Целевые атаки	%
Госучреждения	5,00
Промышленность	4,80
ИТ	4,20
Здравоохранение	3,60
Финансы	3,40
Телеком	2,20
СМИ	2,00
Розничная торговля	1,60
Транспорт	1,40
Другое	1,00
Пищевая промышленность	0,60
Образование	0,20

Артефакты целевых атак	%
Госучреждения	3,40
Розничная торговля	1,40
ИТ	0,40
Здравоохранение	0,80
Финансы	0,60
Промышленность	0,60
Пищевая промышленность	0,40
Транспорт	0,40
СМИ	0,20
Телеком	0,20
Другое	0,20

Вредоносное ПО	%
Госучреждения	8,00
Пищевая промышленность	4,20
Розничная торговля	4,00
Промышленность	3,60
ИТ	1,80
Здравоохранение	1,40
Телеком	0,80
Транспорт	0,60
Финансы	0,20
Строительство	0,20
Другое	0,14

Социальная инженерия	%
ИТ	1,40
Промышленность	0,60
Госучреждения	0,40
Розничная торговля	0,40
Другое	0,20
СМИ	0,20
Здравоохранение	0,20
Транспорт	0,14

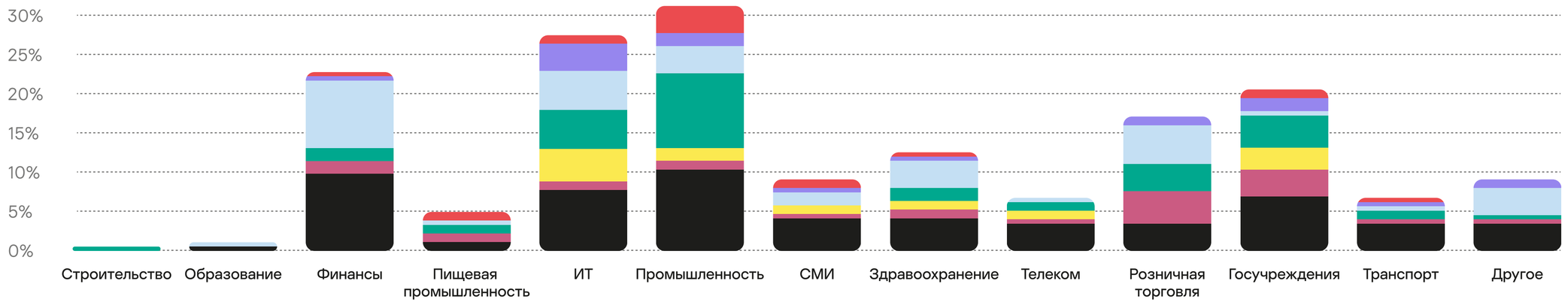
Критичные уязвимости	%
Промышленность	3,40
Финансы	2,80
ИТ	0,60
Госучреждения	0,60
Пищевая промышленность	0,40
СМИ	0,40
Здравоохранение	0,20
Транспорт	0,20

Внутренний нарушитель	%
ИТ	1,20
СМИ	0,80
Промышленность	0,60
Здравоохранение	0,40
Госучреждения	0,40
Телеком	0,20

Из статистики можно сделать следующие выводы:

1. Все типы критичных инцидентов, наблюдаемые за период, фиксировались в государственных учреждениях, ИТ-компаниях, на промышленных предприятиях и в сфере здравоохранения.
2. На всех предприятиях, где фиксировались инциденты с непосредственным участием человека (целевые атаки), также наблюдались и инциденты, связанные с обнаружением следов прошлых целевых атак (за исключением образовательных учреждений, где в 2022 году фиксировались активные атаки, однако следов прошлых взломов обнаружено не было). Это подтверждает тот факт, что атакующие возвращаются.
3. Статистика активных целевых атак повторяет статистику киберучений; единственное исключение — строительство. Это может свидетельствовать о том, что в большинстве своем компании корректно оценивают риски ИБ.
4. Практически во всех индустриях наблюдались инциденты, связанные с ВПО без видимых следов участия человека; исключение — образование и СМИ.
5. Статистика целевых атак во многом схожа с распределением инцидентов, связанных с ВПО; исключение составляют образование и СМИ. Это подтверждает наблюдаемую в последнее время тенденцию, что атаки ВПО с большим ущербом начинаются как целевые с участием человека: первоначальное проникновение и запуск выполняются вручную, а дальнейшее распространение ВПО происходит без участия человека. Ввиду неполного покрытия мониторинга обнаружение происходит на этапах, когда на уровне телеметрии MDR не удается связать вредоносную активность с ранее обнаруженными действиями человека, поэтому регистрируются два несвязанных инцидента: целевая атака и ВПО.

Количество организаций по отраслям, столкнувшихся с критичными инцидентами



Киберучения	%
Финансы	4,09
ИТ	2,73
Розничная торговля	2,73
Здравоохранение	1,82
Промышленность	1,82
Другое	1,82
СМИ	1,36
Образование	0,45
Пищевая промышленность	0,45
Телеком	0,45
Госучреждения	0,45
Транспорт	0,45

Целевые атаки	%
Промышленность	6,36
Финансы	4,55
ИТ	3,64
Госучреждения	3,18
СМИ	2,27
Здравоохранение	2,27
Телеком	1,82
Розничная торговля	1,82
Транспорт	0,91
Пищевая промышленность	0,91
Другое	0,45
Образование	0,45

Артефакты целевых атак	%
Розничная торговля	2,27
Госучреждения	1,82
Финансы	1,36
Пищевая промышленность	0,91
ИТ	0,91
Промышленность	0,91
Здравоохранение	0,91
СМИ	0,45
Телеком	0,45
Транспорт	0,45
Другое	0,45

Вредоносное ПО	%
Промышленность	5,00
ИТ	2,73
Госучреждения	2,27
Розничная торговля	1,82
Здравоохранение	1,36
Финансы	1,36
Пищевая промышленность	0,91
Телеком	0,91
Транспорт	0,91
Строительство	0,45
Другое	0,45

Социальная инженерия	%
ИТ	1,82
Промышленность	1,36
Госучреждения	1,36
Розничная торговля	0,91
Другое	0,91
Финансы	0,45
СМИ	0,45
Здравоохранение	0,45
Транспорт	0,45

Критичные уязвимости	%
Промышленность	1,82
Пищевая промышленность	0,91
ИТ	0,91
СМИ	0,91
Госучреждения	0,91
Финансы	0,45
Здравоохранение	0,45
Транспорт	0,45

Внутренний нарушитель	%
ИТ	2,27
Промышленность	1,36
СМИ	0,91
Здравоохранение	0,91
Телеком	0,45
Госучреждения	0,45

Основные выводы из статистики.

1. Наибольшее количество атакованных организаций относится к промышленному сегменту, где имели место все типы критичных инцидентов, причем целевые атаки были выявлены в 34% организаций, а жертвами ВПО стали 27%.
2. Не меньший интерес для атакующих представляет и финансовый сектор, где в 2022 году наблюдались все виды критичных инцидентов, за исключением работы инсайдеров. Целевые атаки здесь были обнаружены в 37% организаций.
3. В сравнении с 2021 годом значительно возросло количество организаций СМИ: в 2022 году у каждого заказчика были выявлены инциденты высокого уровня критичности и более чем у трети — целевые атаки*.
4. ИТ-компании по-прежнему популярные цели для атакующих. В 2022 году в этом секторе наблюдались все типы инцидентов, но в сравнении с 2021 годом ситуация незначительно улучшилась: менее чем в четверти организаций наблюдались целевые атаки, и только 18% стали жертвами ВПО с большим ущербом.
5. Сектор строительства в 2022 году продемонстрировал наилучшие результаты: там фиксировались только критичные инциденты, связанные с ВПО.
6. В телеком-секторе более чем в 40% организаций фиксировались целевые атаки, в 20% — ВПО с ущербом, а киберучения были замечены только в 11% организаций.

* Здесь и далее в этом разделе указаны проценты от количества организаций данного сектора; на графике — проценты от общего количества заказчиков услуги MDR в 2022 году.

Технологии обнаружения

Наибольшее количество инцидентов высокого уровня критичности

TA0002 Выполнение — 2,32%

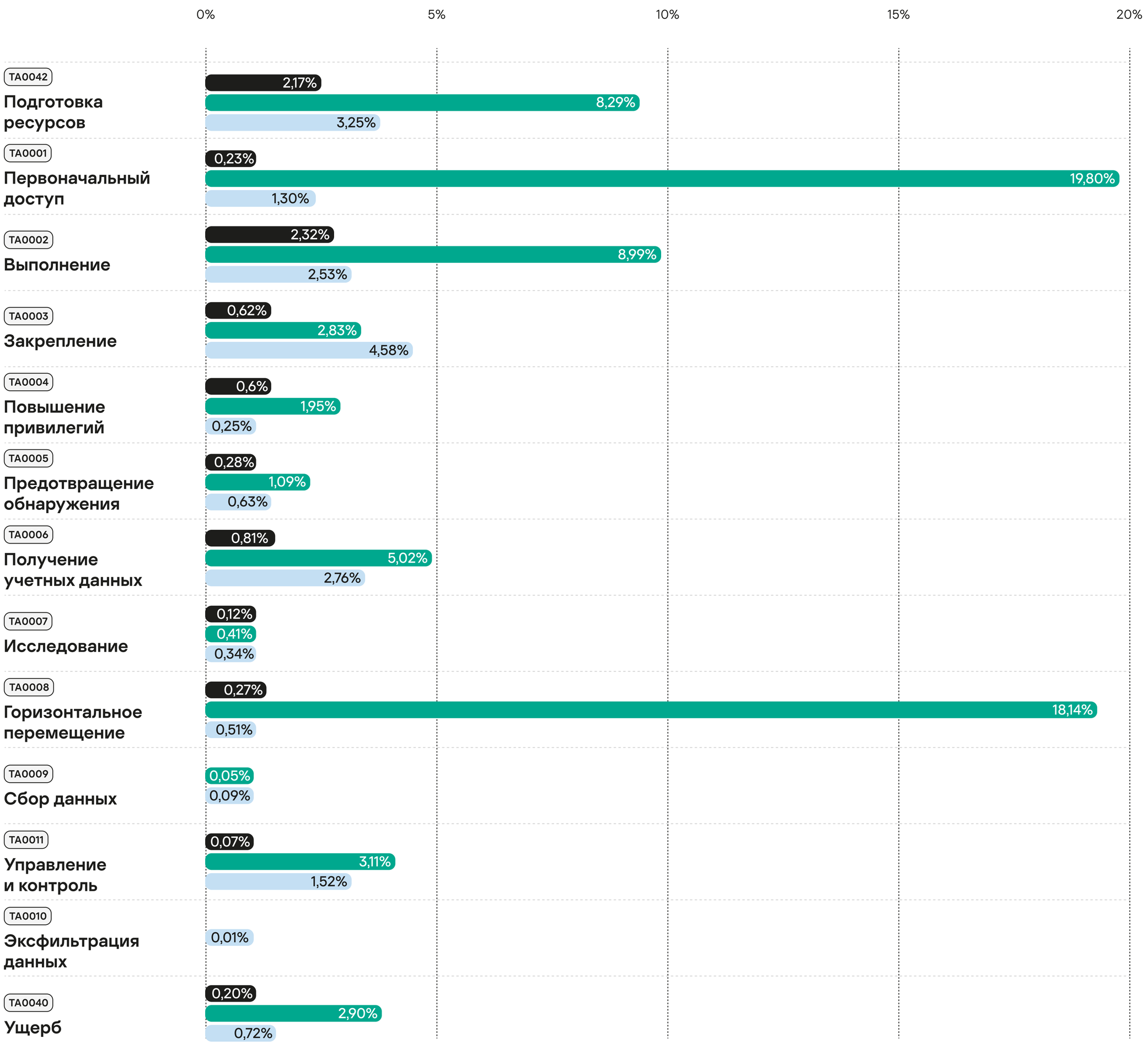
Наибольшее количество инцидентов среднего уровня критичности

TA0001 Первоначальный доступ — 19,80%

Тактики злоумышленников

MDR позволяет обнаруживать инциденты на разных этапах атаки. Обычно инцидент проходит через все стадии (тактики **MITRE ATT&CK®**), но на диаграмме ниже отображена наиболее ранняя тактика.

Уровень критичности инцидента



Основные тактики, с помощью которых мы обнаруживаем инциденты

Подготовка ресурсов

TA0042

Выявленные на данном этапе инциденты относятся к типу «Обнаружен подозрительный файл», когда потенциально опасный инструмент наблюдался без каких-либо признаков запуска. Часто это связано с киберучениями, но иногда позволяет выявить реального атакующего, еще не перешедшего в активную фазу.

Первоначальный доступ

TA0001

В основном покрывается платформой Kaspersky Anti Targeted Attack на сетевом периметре: обнаруживаются фишинг и социальная инженерия.

Выполнение

TA0002

Обнаружение на этом шаге очень схоже с предыдущим этапом, но здесь наблюдается запуск инструмента. Выполнение тяжело скрыть, поэтому наибольшее количество критичных инцидентов обнаружено тут. Высокая эффективность выявления атак на данном этапе обусловлена частым использованием атакующими стандартных наборов инструментов.

Закрепление

TA0003

Этот этап традиционно эффективен для обнаружения разного рода вредоносного и нежелательного ПО, поэтому доля инцидентов низкого уровня критичности здесь наибольшая.

Получение учетных данных

TA0006

Данная тактика оказалась достаточно эффективной для обнаружения. Большая доля инцидентов, выявленных на этом этапе, была связана с проверками оперативной готовности сервиса MDR, однако небольшое количество опубликованных инцидентов обусловлено выявлением активных атак, начавшихся до момента подключения к MDR.

Горизонтальные перемещения

TA0008

На данный этап приходится большая доля обнаруженных инцидентов, однако их уровень критичности — средний. Например, когда наблюдается активность сетевого червя, эксплуатирующего **SMB** без видимых признаков непосредственного участия атакующего, и по данным телеметрии следует, что обновления ОС установлены, а система защиты конечных точек успешно предотвращает попытки распространения.

Сбор данных

TA0009

Как и в прошлые годы, этот этап выглядит, как «слепая зона», однако этому есть объективные объяснения. Сбор данных характерен далеко не для всех инцидентов, поэтому велика вероятность, что подобные случаи — это, как правило, целевые атаки с активным участием человека, которые были обнаружены и предотвращены на более ранних этапах (данный этап эффективно покрывается правилами обнаружения MDR).

Управление и контроль

TA0011

Хотя данный этап эффективен для обнаружения, доля критичных инцидентов составила менее 0,1%. Почти все обнаруженные инциденты связаны с хостами, для которых не был активирован сервис MDR, поэтому основанием здесь являлся только подозрительный трафик, атрибутированный к функционалу какого-либо вредоносного или нежелательного ПО.

Эксфильтрация

TA0010

Эксфильтрация не всегда надежно отличима от управления и контроля, и в неопределенных случаях аналитики предпочитают последний, как наиболее частый сценарий.

Ущерб

TA0040

На этапе было обнаружено не так много инцидентов. Важно учитывать, что при выявлении атаки на стадии получения ущерба уже не всегда удается избежать серьезных последствий.

Тактики и технологии обнаружения

Хотя сетевая система обнаружения вторжений (СОВ), анализирующая сетевой трафик, также входит в состав сенсора конечной точки, ее вердикты учитываются в рамках данного отчета как события безопасности, выявленные последним.

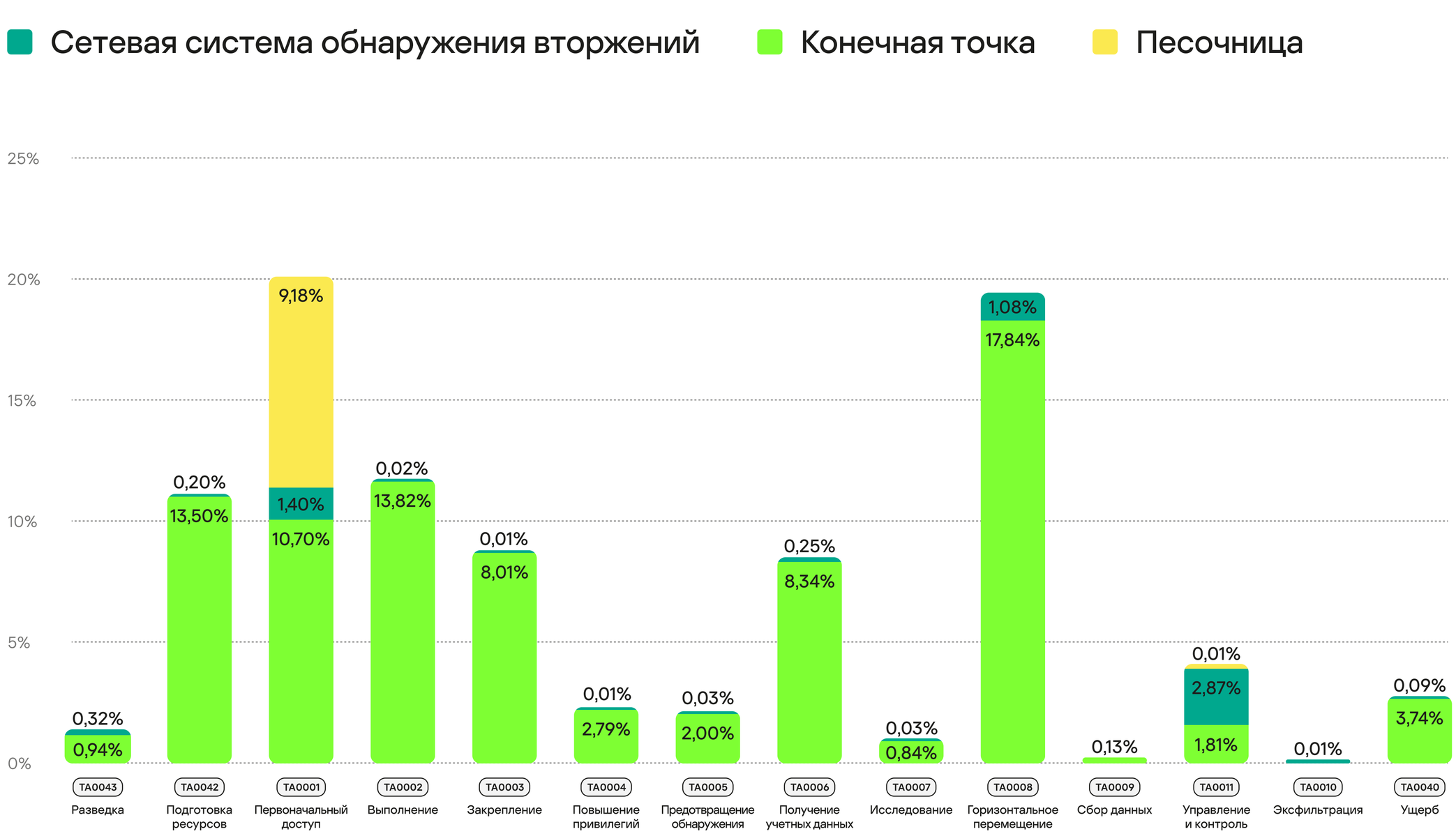
Доли инцидентов, обнаруженных различными типами сенсоров, представлены на диаграмме ниже.

В MDR анализируется телеметрия с разных типов сенсоров:

- конечная точка

- СОВ
- песочница

Являются частью платформы Kaspersky Anti Targeted Attack (KATA)



Высокая эффективность «песочницы» и сетевых СОВ на этапе **Первоначальный доступ** обусловлена распространенным сценарием использования KATA для обнаружения фишинговых атак на сетевом периметре. Также сетевая СОВ эффективна на этапах **Горизонтальные перемещения** и **Управление и контроль**.

На этапах **Выполнение**, **Закрепление**, **Повышение привилегий**, **Обход защиты**, **Получение первоначальных данных** и **Ущерб** сенсор конечной точки является основным. Интересно отметить, что он также эффективен для тактики **Горизонтальные перемещения**, поскольку используются встроенные механизмы ОС, которые хорошо покрыты правилами обнаружения. Как видно из диаграммы, сенсоры конечных точек проявляют эффективность и на этапе **Управление и контроль** — где как раз работает встроенная СОВ.

Тактика **Разведка** обнаруживалась сенсором конечной точки и сетевой СОВ — сюда попали разного рода сканирования и инвентаризации сети.

Наличие срабатываний сетевой СОВ для тактики **Получение учетных данных** обуславливается возможностью СОВ распознавать по сетевому трафику использование стандартных инструментов, например, для интерактивного подбора пароля.

В России и СНГ на стадии «Первоначальный доступ» выявляется большее количество инцидентов среднего уровня критичности по сравнению с общемировой статистикой: 32,53% против 19,80%. Это может быть обусловлено популярностью использования продукта Kaspersky Anti Targeted Attack (KATA) в регионе.

Если смотреть на общую статистику по тактикам, то можно заметить, что в России и СНГ «песочница» выявляет 25,07% инцидентов против 9,19% в мире, что также подтверждает утверждение о распространенности KATA в России и его эффективности.

Техники злоумышленников

Самые популярные LOL-утилиты

	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%

Инструменты, применяемые в атаках

Злоумышленники используют встроенные инструменты ОС, чтобы минимизировать риск обнаружения во время доставки своих инструментов на взломанную систему.

Самые популярные **LOL-утилиты**, которые наблюдались практически в любом инциденте, — это **powershell.exe**, **rundll32.exe** и **reg.exe**. В прошлом году встречались критичные инциденты с использованием **comsvcs.dll** — несмотря на то что техника не нова, ранее настолько часто она не фиксировалась.

certutil.exe, использование которой уже трудно пропустить, по-прежнему популярна среди атакующих.

Часто вредоносные нагрузки* для следующих стадий после **Первоначального доступа** реализуются в виде MSI; этим объясняется популярность **msiexec.exe** вообще и в критичных инцидентах — в частности.

Классификация инцидентов по MITRE ATT&CK®

Наша логика обнаружения поддерживает классификацию MITRE ATT&CK®. Для каждого правила обнаружения мы рассчитываем конверсию и вклад**, поэтому мы можем их оценить и для техник MITRE ATT&CK®. Ниже перечислены девять техник, показавших наилучшую конверсию***, а тепловая карта в Приложении демонстрирует вклад обнаруженных нами техник в 2022 году. Невысокий процент конверсии объясняется тем, что на практике за счет используемых превентивных средств безопасности, не все реализации злоумышленниками выявленных техник привели к развитию атаки и требующим реакции инцидентам.

* Например, MSF Meterpreter или CobaltStrike beacon.

** Конверсия — отношение событий безопасности, классифицированных как инциденты, к общему количеству событий безопасности, соответствующим конкретной технике MITRE ATT&CK®.
Вклад — отношение инцидентов, где наблюдалась та или иная техника, к общему количеству инцидентов.

*** Для репрезентативности взяты во внимание техники, вклад которых превышает 5%, то есть которые встречались более чем в 5% инцидентов.

MITRE ATT&CK®

MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge — «тактики, техники и общеизвестные факты о злоумышленниках») — основанная на реальных наблюдениях база знаний компании MITRE, содержащая описание тактик, приемов и методов, используемых киберпреступниками, призванная упростить задачу реагирования на киберинциденты.

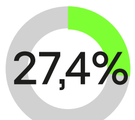
РАЗВЕДКА	ПОДГОТОВКА РЕСУРСОВ	ПЕРВОНАЧАЛЬНЫЙ ДОСТУП	ВЫПОЛНЕНИЕ	ЗАКРЕПЛЕНИЕ	ПОВЫШЕНИЕ ПРИВИЛЕГИЙ	ПРЕДОТВРАЩЕНИЕ ОБНАРУЖЕНИЯ	ПОЛУЧЕНИЕ УЧЕТНЫХ ДАННЫХ	ИССЛЕДОВАНИЕ	ГОРИЗОНТАЛЬНОЕ ПЕРЕМЕЩЕНИЕ
10 техник	7 техник	9 техник	13 техник	19 техник	13 техник	42 техники	17 техник	30 техник	9 техник
Active Scanning T1595	Acquire Infrastructure T1583	Drive-by Compromise T1189	Command and Scripting Interpreter T1059	Account Manipulation T1098	Abuse Elevation Control Mechanism T1548	Abuse Elevation Control Mechanism T1548	Adversary-in-the-Middle T1557	Account Discovery T1087	Exploitation of Remote Services T1210
Gather Victim Host Information T1592	Compromise Accounts T1586	Exploit Public-Facing Application T1190	Container Administration Command T1609	BITS Jobs T1197	Access Token Manipulation T1134	Access Token Manipulation T1134	Brute Force T1110	Application Window Discovery T1010	Internal Spearphishing T1534
Gather Victim Identity Information T1589	Compromise Infrastructure T1584	External Remote Services T1133	Deploy Container T1610	Boot or Logon Autostart Execution T1547	Boot or Logon Autostart Execution T1547	BITS Jobs T1197	Credentials from Password Stores T1555	Browser Bookmark Discovery T1217	Lateral Tool Transfer T1570
Gather Victim Network Information T1590	Develop Capabilities T1587	Hardware Additions T1200	Exploitation for Client Execution T1203	Boot or Logon Initialization Scripts T1037	Boot or Logon Initialization Scripts T1037	Build Image on Host T1612	Exploitation for Credential Access T1212	Cloud Infrastructure Discovery T1580	Remote Service Session Hijacking T1563

Техники с наилучшей конверсией в мире

Эксплуатация удаленных служб

Многие шифровальщики по-прежнему пытаются эксплуатировать переполнение в **SMB** для горизонтальных перемещений, и нередко довольно успешно.

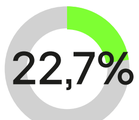
T1210



Существующие учетные записи

Доменные и локальные учетные записи использовались злоумышленниками для обхода защиты и последующего закрепления в системе.

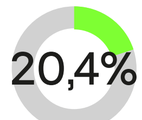
T1078



Манипуляции с учетной записью

Несмотря на то что привилегированные учетные записи и группы, как правило, контролируются, злоумышленники нередко активируют отключенные аккаунты и (или) добавляют членов в группы.

T1098



Вредоносное ПО

Предшествующие активной эксплуатации этапы атаки наиболее часто обнаруживались как потенциально вредоносный код без признаков запуска.

T1587.001

Вредоносный файл

Один из двух наиболее популярных сценариев инициации компрометации вследствие успешной социальной инженерии.

T1204.002

Эксплуатация публичных приложений

Как и в 2021 году, не все организации своевременно устанавливали обновления, поэтому почти в 12% случаев проникновения через сетевой периметр были успешны.

T1190

Вредоносная ссылка

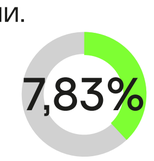
Второй из наиболее популярных сценариев инициации компрометации вследствие успешной социальной инженерии.

T1204.001

Протоколы прикладного уровня

Для связи с командными центрами используются стандартные протоколы прикладного уровня, которые могут быть надежным индикатором аномалии.

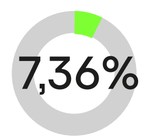
T1071



Фишинг

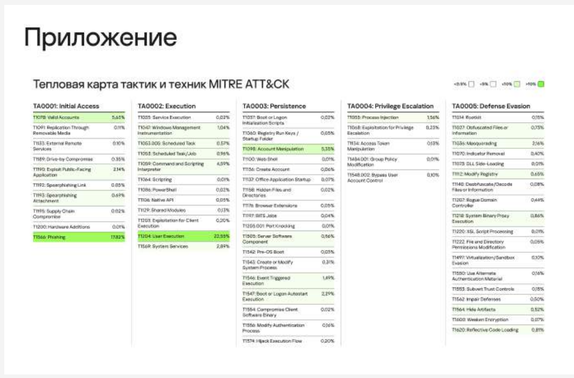
Направленный фишинг сохраняет лидерские позиции в качестве метода первоначального взлома, но в 2022 году, как и в 2021-м, он уступил первенство взломам сервисов на периметре.

T1566



Наиболее популярные сценарии обнаружения

В 2022 году общее количество уникальных сценариев, сработавших у наших заказчиков и имеющих ненулевую конверсию, — 550. В этом разделе мы рассмотрим наиболее часто срабатывающие, общий совокупный вклад которых превысил 70%. Для удобства мы разделили их на две группы: на основе срабатывания продуктов и на базе событий ОС. Безусловно, эффективно отработавших сценариев, основанных на «классических» событиях **EDR**, таких как «запуск процесса» или «сетевое соединение», также немало, но их совокупный вклад в 2022 году составил меньше трети, и, ввиду ограниченности объема настоящего отчета, мы не будем их рассматривать.


Приложение

Тепловая карта тактик и техник MITRE ATT&CK

Подробная тепловая карта с тактиками и техниками MITRE ATT&CK в Приложении на странице 27.

Техники с наилучшей конверсией в России и СНГ

Активное сканирование

Сканирование — популярная техника Разведки, но вместе с тем и хороший индикатор обнаружения, так как легитимна в исключительных случаях.

T1595 50,59%

Сканирование сетевых служб

Техника при надлежащей фильтрации легитимных сценариев демонстрирует хорошую конверсию. Обнаружение атак на данном этапе еще позволяет организовать эффективное реагирование.

T1046 39,39%

Угадывание пароля

Старый добрый перебор пароля до сих пор популярен, особенно для сервисов, доступных из Интернета. В локальных сетях это эффективный способ обнаружения атаки.

T1110.001 33,44%

Специальные возможности

Специальные возможности, как правило, используются подразделениями ИТ для смены пароля локального администратора, однако фиксировались и случаи применения этой техники злоумышленниками.

T1546.008 31,14%

Исследование сетевых подключений

Техника выполняется с использованием штатных инструментов ОС, однако на практике применяется нечасто, тем более на рабочих станциях обычных пользователей, поэтому в 2022 году также показала относительно высокую конверсию.

T1049 22,82%

Исследование конфигурации сети

Получение сетевой конфигурации скомпрометированного узла — легитимная операция, однако в реальных атаках она работает как эффективный индикатор, поскольку довольно редко используется реальными пользователями.

T1016 22,47%

Эксплуатация удаленных служб

Как и в 2021 году, высокая конверсия подтверждает успешность компрометации сетей через сетевой периметр в 2022 году.

T1210 21,20%

Существующие учетные записи

Обычно в реальных инцидентах злоумышленники используют легитимные учетные записи, т.к. создание новых — крайне заметная операция. Высокая конверсия демонстрирует эффективность профилирования работы учетных записей с использованием машинного обучения.

T1078 18,53%

Несанкционированное использование ресурсов

Подавляющее большинство таких атак связано с применением криптомайнеров. Это распространенная проблема в корпорациях, однако не всегда можно с уверенностью сказать, что послужило причиной: успешная внешняя атака или деятельность инсайдера.

T1496 16,93%

Техники с наибольшим вкладом в России и СНГ

Техника	Вклад
T1204: Выполнение с участием пользователя	22,55%
T1566: Фишинг	17,82%
T1210: Эксплуатация удаленных служб	16,22%
T1565: Манипуляции с данными	9,65%
T1587: Разработка собственных средств	9,36%
T1071: Протоколы прикладного уровня	8,55%
T1588: Подготовка необходимых средств	7,48%
T1003: Получение дампа учетных данных	7,04%
T1021: Удаленные службы	6,81%
T1078: Существующие учетные записи	5,63%

Обнаружение на основе вердиктов решений класса XDR и продуктов для защиты конечных точек

В рамках сервиса MDR мы не регистрируем инцидент после каждого срабатывания продуктов. Однако дополнительное контекстное обогащение в совокупности с вердиктом продукта может быть основанием для старта расследования. Ввиду использования высокотехнологичных поставщиков телеметрии, вердикты продуктов по-прежнему остаются наиболее частыми и достаточно точными событиями безопасности, приводящими к обнаружению серьезных инцидентов.

Общий вклад	61%
Средняя конверсия	26%

Популярные сценарии

Телеметрия Обогащение

Срабатывание COB

Срабатывание сетевой COB (как в составе KATA, так и в составе компонента продукта для защиты конечных точек); в объеме мониторинга отсутствует источник атаки, поэтому проверить вероятное ложное срабатывание нет возможности.

Вердикт COB

Сетевые настройки хостов в мониторинге

Получение вредоносного вложения по почте

Срабатывание продукта на конечной точке на почтовое вложение.

Вердикт продукта

Получение почтового вложения

Закрепление в памяти

Срабатывание продукта на область памяти.

Вердикт продукта

Срабатывание «песочницы»

Срабатывание «песочницы» в составе KATA, и для объекта нет точного вердикта продукта для защиты конечной точки.

Вердикт «песочницы»

Вердикты по объекту от других продуктов

Попытка доступа на вредоносный URL

Попытка обращения к URL с плохой репутацией.

Вердикт продукта **HTTP-соединение**

DNS-запрос **Репутация URL**

Вердикт продукта, связанный с APT

Список релевантных точных и неточных вердиктов*.

Вердикт продукта

Точный вердикт продукта на сервере

Срабатывание продукта для защиты конечных точек, установленного на сервере. Частный случай — срабатывание продукта на контроллере домена, на критичном сервере.

Вердикт продукта **Конфигурация продукта**

Список критичных серверов

Вредоносный URL в командной строке

В каком-либо поле (наиболее частый сценарий — командная строка, что и объясняет название сценария) любого события выделяется URL и проверяется по базе репутации.

Репутация URL

Создание известного инструмента

На файловой системе создается объект, который продуктом классифицируется как hack tool.

Вердикт продукта

Создание файла на файловой системе

Описание вердикта продукта

* Точный вердикт — обнаруженная продуктом активность точно вредоносна. Как правило, в этом случае продукт автоматически активно реагирует. Неточный вердикт или подозрительная активность — продукт обнаружил аномалию, но вероятность ложного срабатывания велика, поэтому активная реакция отсутствует, но оповещается команда MDR.

Обнаружение на основе событий ОС

События операционной системы при всей своей очевидности и доступности также предоставляют широкие возможности по обнаружению атак. Обогащенные данными об угрозах и скоррелированные с другими событиями EDR они демонстрируют высокую конверсию, а для ряда сценариев являются едва ли не единственным методом обнаружения.

Общий вклад	10%
Средняя конверсия	28%

Популярные сценарии

Телеметрия

Встроенная учетная запись была активирована

Встроенные учетные записи, такие как «Администратор» и (или) «Гость», были включены

События ОС: включение учетной записи

Сетевой вход известного инструмента

Обнаружены события сетевого входа от известного инструмента (kali, nmap и т.п.)

События ОС: вход, выход

Пользователь был добавлен в привилегированную группу

Зафиксировано добавление пользователя в привилегированную группу (Domain Admins, Enterprise Admins, Cert Publishers и т.п.)

События ОС: добавление члена группы

Успешный вход несуществующего пользователя

Зафиксирован успешный вход, однако при поиске учетной записи возникла ошибка «1332 (0x534) No mapping between account names and security IDs was done»

Событие ОС: вход

Запуск обфусцированного PowerShell-сценария

Основанный на машинном обучении анализ сценария выявил использование обфускации

События ОС: журнал команд PowerShell

Подозрительный входящий запрос на репликацию AD

Обращение с правами DS-Replication-Get-Changes, DS-Replication-Get-Changes-All к объекту класса Domain-DNS

События ОС: операция с объектом каталога

Подозрение на атаку DCShadow

Необходимые для DCShadow SPN были установлены для учетной записи компьютера

События ОС: изменение учетной записи компьютера

Запуск службы с системным процессом

Запускается служба, где в качестве исполняемого файла указана командная строка, содержащая cmd.exe, wmic.exe, bash.exe, mshta и т.п.

События ОС: запуск и установка службы

Установка подозрительной службы

В ОС устанавливается служба с подозрительным именем, содержащим winexesvc, dumpsvc, paexec, comspec и т.п.

События ОС: установка службы

Приложение

Тепловая карта тактик и техник MITRE ATT&CK

<0,5% <5% <10% >10%

TA0001: Initial Access

T1078: Valid Accounts	5,63%
T1091: Replication Through Removable Media	0,11%
T1133: External Remote Services	0,10%
T1189: Drive-by Compromise	0,35%
T1190: Exploit Public-Facing Application	2,14%
T1192: Spearphishing Link	0,05%
T1193: Spearphishing Attachment	0,69%
T1195: Supply Chain Compromise	0,02%
T1200: Hardware Additions	0,01%
T1566: Phishing	17,82%

TA0002: Execution

T1035: Service Execution	0,02%
T1047: Windows Management Instrumentation	1,04%
T1053.005: Scheduled Task	0,57%
T1053: Scheduled Task/Job	0,96%
T1059: Command and Scripting Interpreter	4,59%
T1064: Scripting	0,01%
T1086: PowerShell	0,02%
T1106: Native API	0,05%
T1129: Shared Modules	0,13%
T1203: Exploitation for Client Execution	0,20%
T1204: User Execution	22,55%
T1569: System Services	2,89%

TA0003: Persistence

T1037: Boot or Logon Initialization Scripts	0,02%
T1060: Registry Run Keys / Startup Folder	0,05%
T1098: Account Manipulation	5,35%
T1100: Web Shell	0,01%
T1136: Create Account	0,06%
T1137: Office Application Startup	0,07%
T1158: Hidden Files and Directories	0,02%
T1176: Browser Extensions	0,05%
T1197: BITS Jobs	0,04%
T1205.001: Port Knocking	0,01%
T1505: Server Software Component	0,56%
T1542: Pre-OS Boot	0,03%
T1543: Create or Modify System Process	0,31%
T1546: Event Triggered Execution	1,49%
T1547: Boot or Logon Autostart Execution	2,29%
T1554: Compromise Client Software Binary	0,02%
T1556: Modify Authentication Process	0,16%
T1574: Hijack Execution Flow	0,20%

TA0004: Privilege Escalation

T1055: Process Injection	1,56%
T1068: Exploitation for Privilege Escalation	0,23%
T1134: Access Token Manipulation	0,13%
T1484.001: Group Policy Modification	0,01%
T1548.002: Bypass User Account Control	0,10%

TA0005: Defense Evasion

T1014: Rootkit	0,15%
T1027: Obfuscated Files or Information	0,73%
T1036: Masquerading	2,16%
T1070: Indicator Removal	0,40%
T1073: DLL Side-Loading	0,01%
T1112: Modify Registry	0,65%
T1140: Deobfuscate/Decode Files or Information	0,08%
T1207: Rogue Domain Controller	0,44%
T1218: System Binary Proxy Execution	0,86%
T1220: XSL Script Processing	0,01%
T1222: File and Directory Permissions Modification	0,05%
T1497: Virtualization/Sandbox Evasion	0,10%
T1550: Use Alternate Authentication Material	0,16%
T1553: Subvert Trust Controls	0,15%
T1562: Impair Defenses	0,50%
T1564: Hide Artifacts	0,52%
T1600: Weaken Encryption	0,07%
T1620: Reflective Code Loading	0,81%

TA0006: Credential Access

T1003: OS Credential Dumping	7,04%
T1040: Network Sniffing	0,10%
T1056: Input Capture	0,31%
T1110: Brute Force	1,78%
T1187: Forced Authentication	0,01%
T1212: Exploitation for Credential Access	0,10%
T1539: Steal Web Session Cookie	0,02%
T1552: Unsecured Credentials	0,71%
T1555: Credentials from Password Stores	0,52%
T1557: Adversary-in-the-Middle	0,06%
T1558: Steal or Forge Kerberos Tickets	1,73%
T1606: Forge Web Credentials	0,01%
T1649: Steal or Forge Authentication Certificates	0,01%

TA0007: Discovery

T1007: System Service Discovery	0,35%
T1012: Query Registry	0,31%
T1016: System Network Configuration Discovery	0,30%
T1018: Remote System Discovery	0,52%
T1033: System Owner/User Discovery	0,68%
T1046: Network Service Discovery	0,52%
T1049: System Network Connections Discovery	0,30%
T1057: Process Discovery	0,02%
T1069: Permission Groups Discovery	0,48%
T1082: System Information Discovery	0,05%
T1083: File and Directory Discovery	0,07%
T1087: Account Discovery	0,72%
T1135: Network Share Discovery	0,06%
T1201: Password Policy Discovery	0,01%
T1482: Domain Trust Discovery	0,51%
T1482: Domain Trust Discovery	0,05%
T1615: Group Policy Discovery	0,35%

TA0008: Lateral Movement

T1021: Remote Services	6,81%
T1076: Remote Desktop Protocol	0,02%
T1080: Taint Shared Content	0,01%
T1210: Exploitation of Remote Services	16,22%
T1534: Internal Spearphishing	2,63%
T1563: Remote Service Session Hijacking	0,06%
T1570: Lateral Tool Transfer	0,30%

TA0009: Collection

T1005: Data from Local System	0,07%
T1039: Data from Network Shared Drive	0,04%
T1113: Screen Capture	0,10%
T1119: Automated Collection	0,09%
T1125: Video Capture	0,06%
T1560: Archive Collected Data	0,06%

TA0010: Exfiltration

T1020: Automated Exfiltration	0,06%
T1029: Scheduled Transfer	0,01%
T1030: Data Transfer Size Limits	0,01%
T1041: Exfiltration Over C2 Channel	0,03%
T1048: Exfiltration Over Alternative Protocol	0,02%
T1567: Exfiltration Over Web Service	0,04%

TA0011: Command and Control

T1001: Data Obfuscation	0,01%
T1071: Application Layer Protocol	8,55%
T1090: Proxy	0,22%
T1095: Non-Application Layer Protocol	0,90%
T1102: Web Service	0,06%
T1104: Multi-Stage Channels	0,01%
T1105: Ingress Tool Transfer	1,15%
T1219: Remote Access Software	0,13%
T1568: Dynamic Resolution	0,13%
T1571: Non-Standard Port	0,07%
T1572: Protocol Tunneling	0,17%
T1573: Encrypted Channel	0,01%

TA0040: Impact

T1485: Data Destruction	1,12%
T1486: Data Encrypted for Impact	1,20%
T1487: Disk Structure Wipe	0,01%
T1489: Service Stop	0,07%
T1490: Inhibit System Recovery	0,01%
T1492: Stored Data Manipulation	0,01%
T1493: Transmitted Data Manipulation	0,01%
T1496: Resource Hijacking	1,86%
T1498: Network Denial of Service	0,02%
T1499: Endpoint Denial of Service	0,04%
T1561: Disk Wipe	2,16%
T1565: Data Manipulation	9,65%

TA0042: Resource Development

T1583: Acquire Infrastructure	0,17%
T1584: Compromise Infrastructure	0,06%
T1586: Compromise Accounts	0,01%
T1587: Develop Capabilities	9,36%
T1588: Obtain Capabilities	7,48%
T1608: Stage Capabilities	0,96%

TA0043: Reconnaissance

T1589: Gather Victim Identity Information	0,02%
T1590: Gather Victim Network Information	0,20%
T1592: Gather Victim Host Information	0,01%
T1595: Active Scanning	0,85%
T1598: Phishing for Information	0,85%

О компании

«Лаборатория Касперского» — международная компания, работающая в сфере информационной безопасности с 1997 года. Глубокие экспертные знания и многолетний опыт компании лежат в основе защитных решений и сервисов нового поколения, обеспечивающих безопасность бизнеса, критически важных инфраструктур, государственных органов и рядовых пользователей. Обширное портфолио «Лаборатории Касперского» включает в себя передовые продукты для защиты конечных устройств, а также ряд специализированных решений и сервисов для борьбы со сложными и постоянно эволюционирующими киберугрозами.

Сервисы кибербезопасности

- Kaspersky Managed Detection and Response
- Kaspersky Incident Response
- Kaspersky Digital Forensics and Malware Analysis
- Kaspersky Targeted Attack Discovery
- Kaspersky Security Assessment
- Kaspersky SOC Consulting
- Kaspersky Cybersecurity Training

Международное признание

«Лаборатория Касперского» активно участвует в независимых тестированиях и взаимодействует с ведущими аналитическими агентствами.

Наши технологии признаны во всем мире и удостоены многочисленных международных наград и признаний.

MITRE | ATT&CK®

AV comparatives

Quadrant Knowledge Solutions

FORRESTER®

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

5000+
квалифицированных специалистов работают в компании

50%
сотрудников — это RnD-специалисты

35
ведущих мировых экспертов в области кибербезопасности

9
центров прозрачности

400 000+
вредоносных объектов мы обнаруживаем каждый день

240 000+
компаний по всему миру мы оберегаем от киберугроз

650+ млн
кибератак было остановлено нашими решениями в 2022 году

#kaspersky
#активируйбудущее

Свяжитесь с нами

По вопросам работы сервисов и в случае необходимости оказания экстренной помощи с расследованием инцидентов:

services@kaspersky.com

www.kaspersky.ru