ГАРДА

Активное реагирование на сетевые киберинциденты

Лучшие мировые практики и современные тренды NDR

Октябрь 2025

Изменения ландшафта киберугроз стали причиной значительно возросшей актуальности продуктов класса NDR (Network Detection and Response)

Киберугрозы эволюционируют быстрее, чем когда-либо. Злоумышленники научились обходить традиционную защиту периметра и незаметно перемещаться внутри корпоративных сетей. Использование NDR-решений позволяет организациям **раньше обнаруживать сложные сетевые угрозы, горизонтальное перемещение злоумышленников внутри сети, сокращать время реакции на инциденты, минимизировать ущерб и интегрировать защиту с существующей инфраструктурой.**

В основе концепции NDR лежит глубокий анализ всего сетевого трафика, который с применением методов искусственного интеллекта и машинного обучения позволяет выявить даже самые сложные продвинутые угрозы. Не менее важной составляющей решений этого класса являются различные встроенные инструменты для реагирования на инциденты, такие как автоматическая блокировка атак и обогащение других компонентов ИБ инфраструктуры (например, SIEM, SOAR, XDR).

Фактически NDR — это современный этап развития устаревшего с 2020 года (согласно Gartner Market Guide for Network Detection and Response) класса решений NTA (Network Traffic Analysis).

Современные NDR-решения эффективно выявляют широкий спектр угроз в сетевом трафике:

внедрение вредоносного ПО

горизонтальное перемещение в сети (lateral movement)

изучение служб Active Directory (Active Directory Enumeration)

целевые атаки APT-группировок, атаки нулевого дня (zero-day атаки)

аномальное поведение (в сравнении с моделями нормального поведения на базе реального трафика)

DNS-туннелирование (по частоте и объему коммуникаций)

Command and Control-трафик (трафик связи зараженного хоста с центром управления, C2-трафик, детектируется по частоте и объему коммуникаций)

активность ботнетов

утечка данных (data exfiltration)

необычные заголовки HTTP и сертификаты SSL/TLS

использование доменных имен, сгенерированных DGA (Domain Generation Algorithm)

сканирование портов и другие техники разведки

DDoS-атаки

использование паролей в открытом виде

использование уязвимых протоколов и понижение версии шифрования

атаки на учетные записи протоколов: LDAP, KERBEROS, SSH, RDP, HTTP, FTP, SQL и других

подозрительный RDP трафик, удаленное исполнение файлов

криптомайнинг

На российском рынке классы NTA и NDR ошибочно принимаются за следующее поколение IDS (Intrusion Detection System) с возможностями для расследований или надстройку IDS и потокового антивируса над песочницей. Но такой подход не позволяет детектировать неизвестные угрозы, модификации известных угроз и атаки в шифрованном трафике внутри легальных приложений.

Основополагающим методом детектирования угроз в NDR является машинное обучение и продвинутая аналитика, позволяющая выявлять те атаки, которые остаются незамеченными для IDS и потоковых антивирусов.

Согласно исследованию IDC MarketScape: Worldwide Network Detection and Response 2024 Vendor Assessment, решения класса NDR применяют концептуальные принципы SIEM к анализу сетевого трафика, используя потоки данных для обнаружения аномалий, свидетельствующих о потенциальной активности злоумышленников. Под аномалиями понимаются отклонения от прогнозируемых значений или состояний, сформированных поведенческих профилей нормального поведения хостов (baseline) на основе данных сетевого трафика с последующим детектированием отклонений от прогнозируемых значений или состояний. Для детектирования таких аномалий могут использоваться поведенческий анализ, машинное обучение и продвинутые аналитические возможности.

Решения класса NDR согласно Magic Quadrant for Network Detection and Response 2025 должны обладать следующей функциональностью:

Поддерживать физические или виртуальные сенсоры, совместимые с on-premise и облачными сетями, для анализа сырого трафика или сетевой телемерии (Netflow, IPFIX)

Анализировать сетевой трафик север-юг (трафик при пересечении периметра) и восток-запад (трафик при горизонтальном перемещении внутри сети)

Моделировать нормальный профиль сетевого трафика и детектировать аномальную активность, отличающуюся от профиля, поддерживать технологии детектирования на основе поведенческого анализа (несигнатурные технологии), включая машинное обучение и продвинутую аналитику для выявления сетевых аномалий

Агрегировать алерты в инциденты безопасности для облегчения расследования угроз и предоставления возможностей автоматического или ручного реагирования для обработки детектов вредоносного сетевого трафика

Детектировать угрозы, используя собственные или внешние потоки Threat Intelligence

Поддерживать традиционные методы обнаружения, такие как сигнатуры системы обнаружения и предотвращения вторжений (IDPS), эвристика на основе правил или алерты на основе пороговых значений

Автоматически реагировать посредством сетевой изоляции хоста или блокировки сетевого трафика напрямую или с помощью интеграций с другими средствами защиты

Данные о сетевых потоках доставляются в NDR с помощью таких протоколов, как Netflow, SFlow, IPFIX, NSEL, Netstream и другие. Эти протоколы передают статистику метаданных сетевых соединений, но не включают их содержимое (payload, например, файлы, команды прикладных протоколов и другие). Обработка только статистики позволяет снизить нагрузку на сетевое оборудование и облегчить передачу данных в NDR.

Важно отметить, что сигнатурный анализ IDS и индикаторы компрометации Threat Intelligence были впервые отмечены Gartner как обязательные требования к детектированию в решениях класса NDR только в 2025 году. До этого Gartner подразумевал, что к этому классу могут относиться решения, использующие исключительно несигнатурные методы детектирования угроз.

Реагирование на события в NDR можно разделить на три типа

1

Автоматическое реагирование (active или automated response)

Этот тип реагирования может использовать автоматическое блокирование угроз посредством интеграции с другими решениями ИБ или блокировки соединений при работе в разрыве (inline). Для реагирования применяются политики или плейбуки. Плейбуки представляют собой автоматизированный сценарий реагирования, состоящий из нескольких шагов.

2

Ручное реагирование (manual response)

Подразумевает предоставление инструментов проактивного поиска угроз (threat hunting tools) и реагирования на инциденты — ручной запуск плейбуков или политик для блокирования. Threat hunting tools дают возможности для детального анализа сетевого трафика на уровне tcp-флагов и содержимого протоколов, интерактивные фильтры, возможности обогащения поисковых запросов, временную шкалу (timeline) для перемотки трафика или событий вперед или назад (playback), автоматический риск-скоринг инцидентов, рекомендации по реагированию и другие возможности.

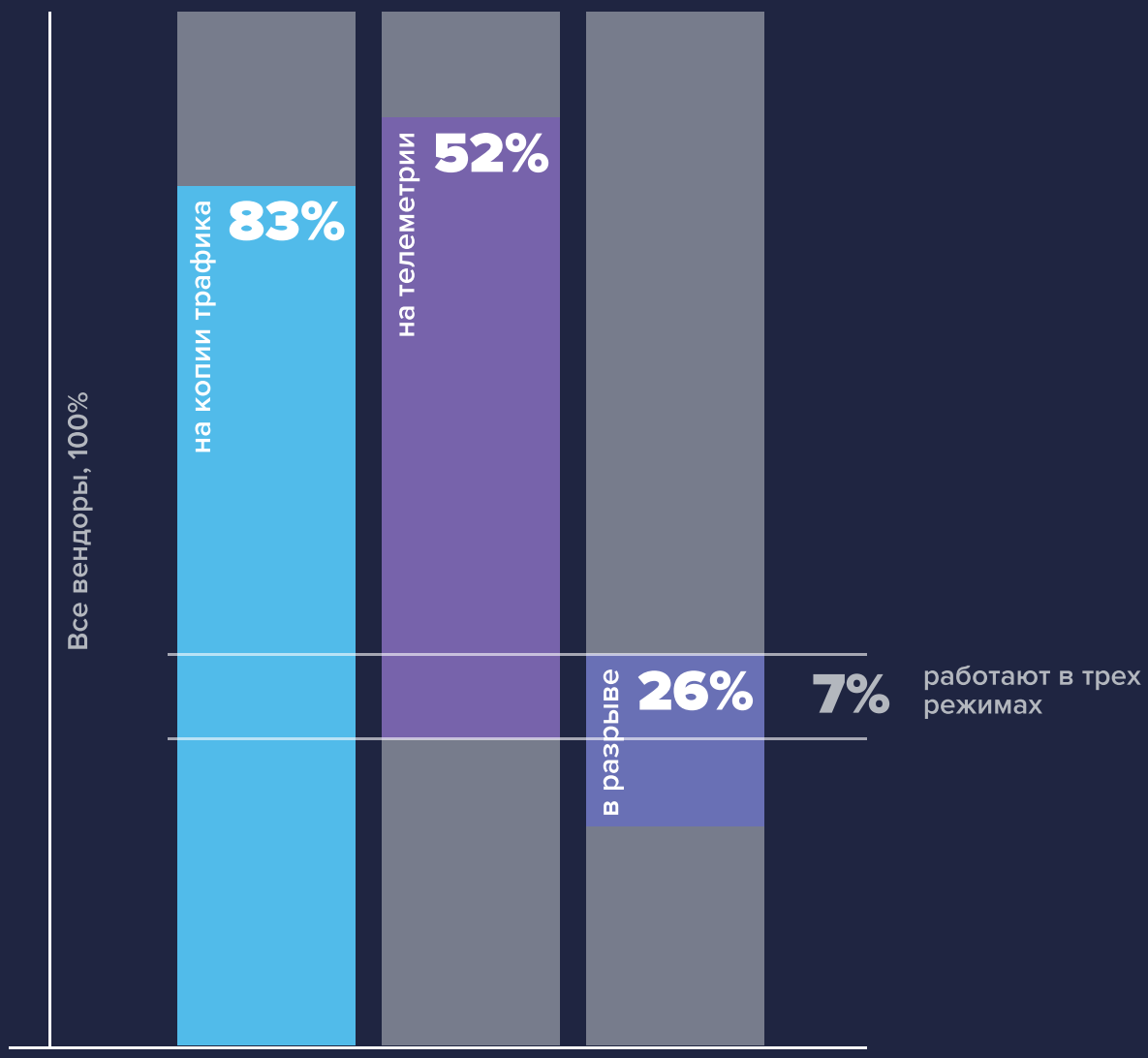
3

Интеграции или интероперабельность (Interoperability)

Возможности интеграций с другими решениями безопасности. В данном случае речь идет о возможности автоматической передачи данных и инцидентов в другие компоненты ИБ- и ИТ-инфраструктуры: SIEM, SOAR, Sandbox, Service Desk, системы мониторинга.

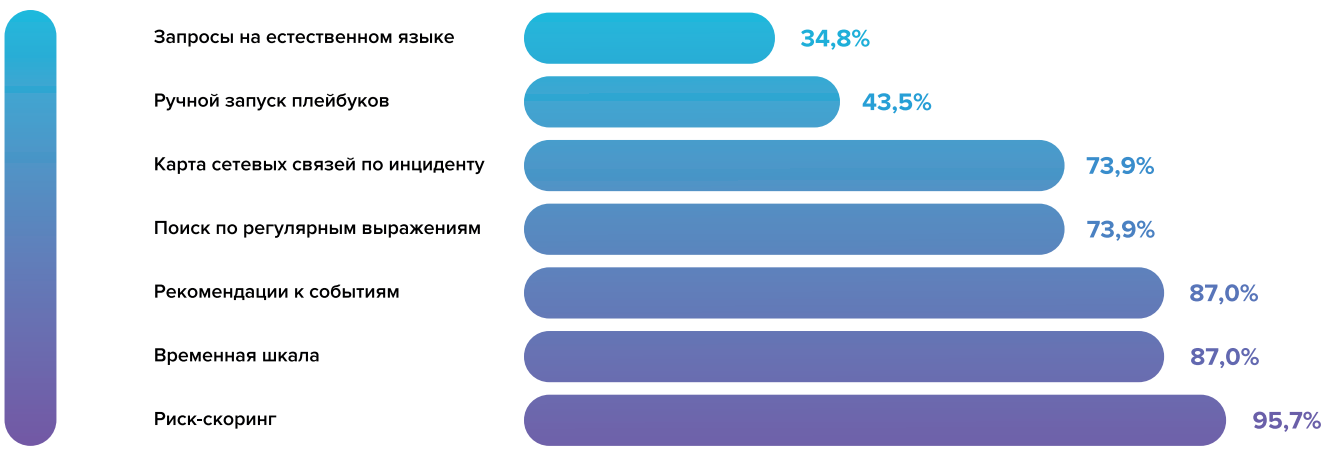
Возможности применения тех или иных сценариев реагирования напрямую зависят от режима работы с сетевым трафиком или сетевой телеметрией.

Распределение NDR-решений согласно режимам работы с сетевым трафиком



Анализ копии сетевого трафика является самым популярным методом анализа данных сети, его поддерживают подавляющее большинство вендоров (83%).
При этом более половины решений (52%) работают с сетевой телеметрией (Netflow и аналоги), что уверенно доказывает достаточность такого типа данных для детектирования угроз. Режим работы «в разрыв» (inline) поддерживает менее трети решений (26%), что указывает на ограничения в его применении. Большинство решений поддерживают несколько режимов работы, отдельные могут поддерживать сразу три режима, но таких представителей совсем немного, менее 7%.

Возможности ручного реагирования



Более 70% вендоров поддерживают 5 основных возможностей ручного реагирования:

- риск-скоринг,
- временную шкалу,
- рекомендации к событиям,
- поиск по регулярным выражениям,
- карту сетевых связей по инциденту.

Данный факт свидетельствует о том, что большинство игроков рынка NDR достигли значительного уровня зрелости в решении соответствующих задач.

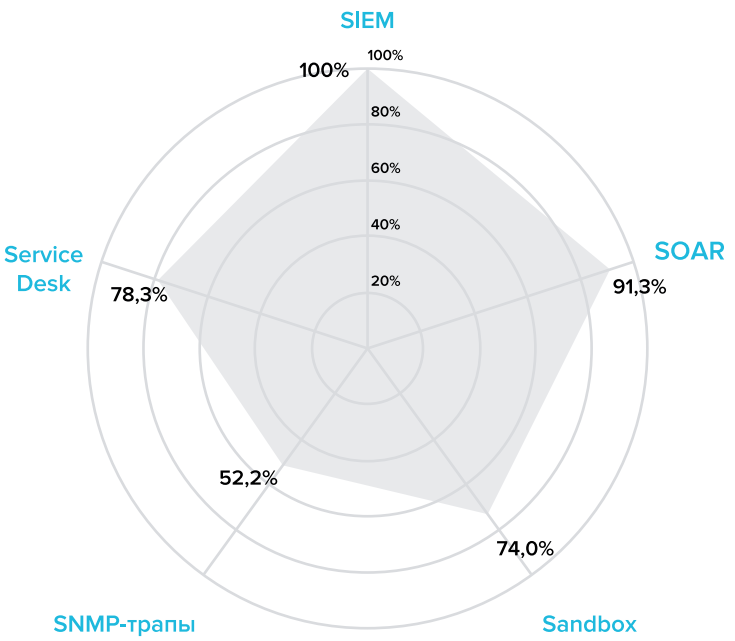
Риск-скоринг подразумевает автоматическую оценку решением уровня критичности обнаруженного инцидента. Она может быть реализована как статически, через предустановленные значения в детектирующей логике, так и динамически, с применением машинного обучения для оценки уровня уверенности в точности детектирования и критичности потенциального эффекта от инцидента.

Обработка запросов на естественном языке на данный момент является инновационной технологией и пока не получила массового применения. Для обработки подобных запросов используются технологии NLP (Natural Language Processing) или ограниченные возможности искусственного интеллекта (LLM).

Ручной запуск плейбуков становится базовой технологией, которая в ближайшем будущем вероятно станет основой для ручного реагирования в NDR.

Интеграция

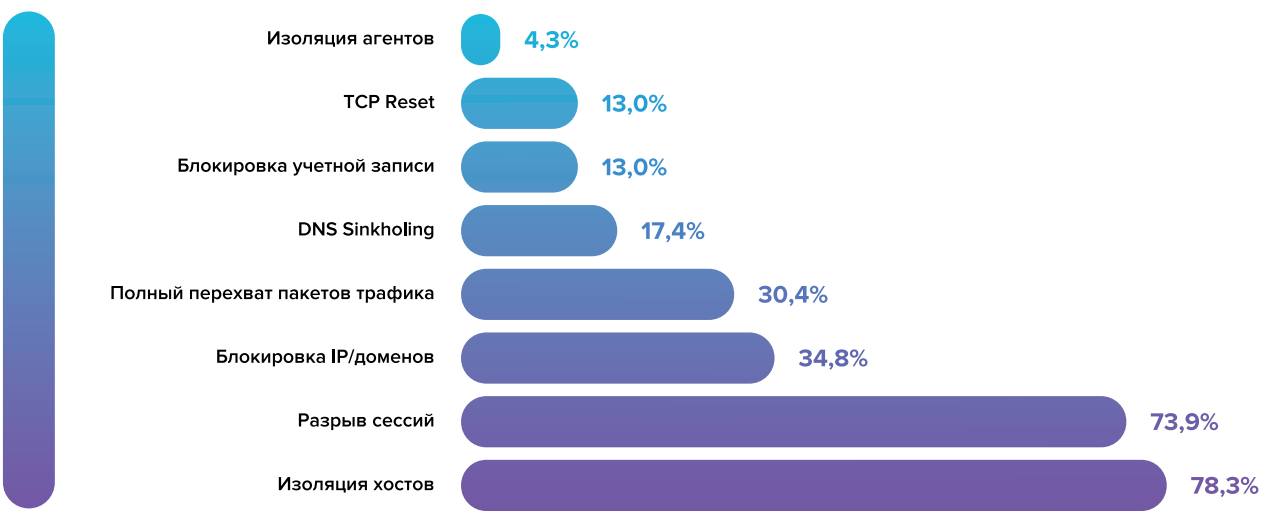
Интеграционная экосистема (поддержка в %)



Анализируя данные о возможностях интеграции решений класса NDR, можно выделить следующие мировые тренды:

- абсолютным стандартом де-факто стала интеграция с системами SIEM и SOAR, что демонстрирует стремление к комплексности и централизации управления кибербезопасностью;
- широкое распространение получили функции извлечения файлов из сетевого трафика и отправка их на анализ в песочницу (Sandbox), их также поддерживают большинство решений;
- около половины решений используют генерацию snmp-трапов как средство оповещений.

Автоматическое реагирование



Наиболее распространенными видами автоматического активного реагирования являются сетевая изоляция хостов/подсетей и разрыв сессий. Данный тип блокировки используется для изоляции скомпрометированных хостов, направлен на сдерживание угрозы и предотвращение ее распространения внутри сети. Техническая реализация обеспечивается интеграцией с NGFW, NAC, EDR-агентами.

Чуть менее трети проанализированных решений поддерживают полную запись сетевого трафика при срабатывании детектирующей логики (full packet capture). Данный показатель отражает существенное отличие в подходах к сбору сетевых данных на глобальном и российском рынках: в международной практике запись полной копии сетевого трафика не является стандартной опцией по умолчанию. Более того, некоторые платформы не записывают даже непрерывную статистику сетевых соединений, ограничиваясь фиксацией только трафика, относящегося к детектируемым аномалиям или инцидентам. Такой подход демонстрирует компромисс между оптимизацией ресурсов хранения и глубиной последующего расследования и анализа.

Технологии автоматизации реагирования

Поддержка плейбуков для реагирования

26,1%
Не поддерживают плейбуки

73,9%
Поддерживают плейбуки

Поддержка AI-расследований

65,1%
Не поддерживают AI-расследования

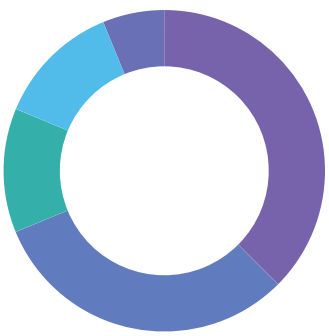
34,9%
Поддерживают AI-расследования

Поддержка плейбуков для расследования и блокировки

26,0%
Поддерживают плейбуки для расследования

74,0%
Поддерживают плейбуки для блокировки

Распределение AI-технологий для расследований и снижения ложных срабатываний



37,5%
AI Analyst

31,3%
AI Triage

12,5%
AI Investigations

12,5%
AI Search Assistant

6,2%
AI Prioritization

Большинство решений используют плейбуки для блокировок. Самые продвинутые продукты поддерживают автоматизацию расследований с помощью плейбуков.

Использование плейбуков для автоматизации расследований практически всегда подразумевает применение технологий искусственного интеллекта. При этом важно отметить, что под искусственным интеллектом в абсолютном большинстве решений понимается машинное обучение (Machine Learning, ML). Генеративный искусственный интеллект используется в единичных случаях и ограниченных сценариях — для обработки запросов на естественном языке.

AI-технологии для автоматизации расследований

AI Investigations — функция автоматизированного расследования инцидентов с поддержкой анализа цепочек событий и скоринга уверенности при детектировании цепочек горизонтального перемещения.

AI Analyst — расширенная версия AI Investigations с поддержкой внешних запросов на обогащение данных по событиями (запросы к различным репутационным базам и базам IoC), опционально может поддерживать автоматическую эскалацию инцидентов и генерацию отчетов на различных этапах анализа.

AI Search Assistant — инструмент для построения поисковых запросов с использованием естественного языка.

AI Triage — функция автоматической приоритизации инцидентов на основе динамической оценки их критичности с учётом контекста и потенциального воздействия.

AI Prioritization — функция автоматической категоризации и ранжирования объектов (триаж учетных записей и хостов) на основе расчетного риск-индекса, уровня критичности и уверенности в потенциальной компрометации.

Плейбуки для проведения расследований на текущий момент являются инновацией, в отличие от плейбуков для блокирования.

Большинство решений, поддерживающих плейбуки для расследований, базируются на применении технологий искусственного интеллекта. Важно подчеркнуть, что в мировой практике под ИИ чаще всего подразумевается именно машинное обучение, а использование наиболее продвинутых функциональных возможностей реализовано в модуле «ассистент».

Ведущие NDR-платформы достигли такого уровня зрелости, что способны обеспечивать полный цикл обработки инцидентов — от детектирования угрозы и ее автоматического блокирования до фиксации результата и последующего закрытия инцидентов без необходимости вмешательства человека.

Анализ реагирования на российском рынке

Рынок специализированных решений для реагирования на инциденты в сетевом трафике в настоящий момент находится в стадии активного развития. На российском рынке преобладают IDS-системы с различными надстройками, опирающиеся на сигнатурные методы детектирования. Эти системы часто ошибочно воспринимаются как платформы анализа сетевого трафика (NTA) или обнаружения и реагирования (NDR). Применение несигнатурных методов детектирования является визионерским, и практически не используется, в отличие от сигнатурного анализа. В России NDR остается инновационным классом решений несмотря на то, что в мире уже фактически стал общепринятым стандартом безопасности. Этим отчасти обусловлено минимальное проникновение современных инструментов автоматического реагирования на инциденты.

- По мере развития сегмента и роста понимания рынком ключевых задач, которые позволяют решить технологии NDR, можно ожидать расширения возможностей реагирования на инциденты, прежде всего ручного реагирования. Стоит отметить достаточно развитое на российском рынке направление интеграций с другими СЗИ, такими как SIEM и песочница, предназначенных для обогащения контекста анализа. Данная тенденция во многом обусловлена стратегией созданиях сквозных интеграций в рамках моновендорных экосистем информационной безопасности.

- Технологии автоматизации реагирования, как с точки зрения блокирования атак, так и с точки зрения автоматического расследования, на данный момент практически отсутствуют на российском рынке ввиду описанных выше причин.

- К факторам, стимулирующим развитие, можно отнести кратно возросшее количество атак, использующих горизонтальное перемещение в инфраструктуре атакуемой организации.

Общие выводы

Доминирование устаревших сигнатурных IDS и медленное внедрение мировых стандартов для NDR-решений сдерживает развитие современных средств автоматического реагирования на инциденты в России.

- Анализ копии сетевого трафика и сетевой телеметрии являются самыми популярными методами интеграции с инфраструктурой, оказывающими влияние на методы автоматического реагирования.

- Решения класса NDR чаще всего используют сетевые и агентские средства защиты для автоматической блокировки скомпрометированных хостов.

- Инструменты проактивного поиска и реагирования на угрозы унифицированы для большинства решений, включая ручной запуск плейбуков для блокировки.

- Несколько наиболее зрелых продуктов используют искусственный интеллект для автоматизации работы аналитиков: задач динамического риск-скоринга, триажа, расследований инцидентов и автоматических блокировок.

Методология

Исследование проводилось в апреле-июле 2025 года на основе анализа открытых источников и отчетов аналитических агентств Gartner, KuppingerCole, GigaOm, QKS group, IDC и других. В ходе работы над исследованием были изучены продукты класса NDR 23 вендоров.

Критерии отбора решений для анализа были сформированы на основе комбинированных требований к NDR-платформам, установленных ведущими мировыми аналитическими агентствами.

Из выборки были исключены семь продуктов, позиционируемых как NDR-решения, но не соответствующих данному классу, так как их основу составляет анализ логов, а не сетевого трафика или сетевой телеметрии, либо они требуют для работы установки других решений, например, XDR или APT-платформы.

Авторы

Станислав Грибанов, эксперт по продуктам информационной безопасности, автор блога «Кибербезопасность и продуктовая экспертиза для бизнеса»

Ксения Крупкина, эксперт по продуктовому маркетингу в направлении сетевой безопасности