TADVISER
Государство. Бизнес. ИТ

Результаты совместного исследования TAdviser и Positive Technologies

Рынок SIEM в России

август-октябрь 2023
Москва

Цели и задачи исследования

В ходе настоящего исследования планировалось изучить спрос на SIEM[1]-системы в России, оценить требования к ним пользователей, а также выявить возможные ограничения спроса или драйверы и перспективы развития этих решений в России.

Методика

Формат работ:
- кабинетное обследование,
- опрос целевых респондентов (телефонные интервью).

Для выполнения задач исследования было проведено анкетирование экспертов, представляющих средний (от 250 до 3000 сотрудников) и крупный бизнес (от 3000 сотрудников и более).

Определение объема рынка, долей вендоров и прогнозы роста SIEM подготовлены на основе экспертных оценок авторов исследования, а также анализа данных известных аналитических агентств, в том числе информации об отгрузках открытых конкурсов торговых площадок.

Выборка

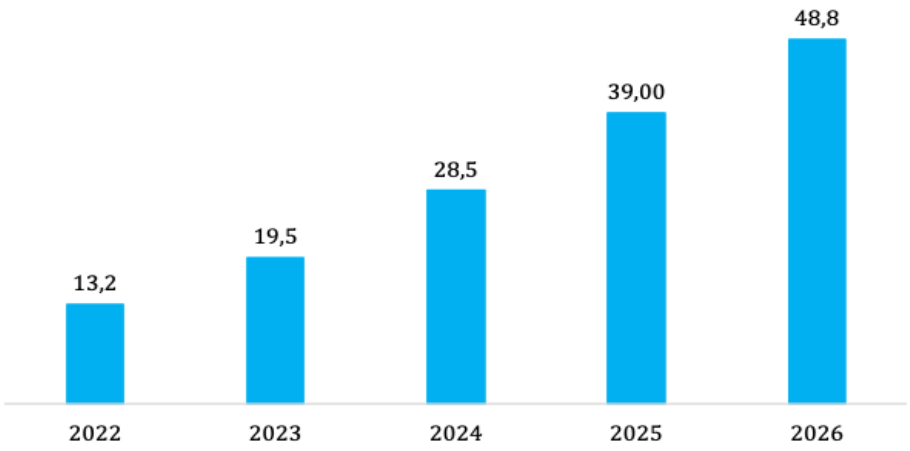
В опросе участвовали руководители ИТ и ИБ (CIO/CTO/CISO и другие специалисты, отвечающие за развитие ИБ функции) из компаний, представляющих отрасли: ТЭК, финансы, промышленность, телеком, ИТ, ритейл, транспорт, госсектор, образование, здравоохранение. Всего было опрошено 100 организаций.

[1] Security Information and Event Management – системы мониторинга событий информационной безопасности и управления инцидентами.

Рынок SIEM в России 2023: объем и динамика

Объем сегмента SIEM-систем в России по итогам 2022 года составил[2], по данным TAdviser, 13,2 млрд руб. (рост +30%). Этот рынок сохранит высокую динамику и в 2023 году – на уровне 47%. После двухлетнего всплеска темпы будут постепенно замедляться и вновь ускорятся к 2026 году. Усиление динамики будет обусловлено плановым периодом обновления или очередным этапом замены ранее установленных систем на фоне продолжающегося роста киберугроз.

Прогноз развития рынка SIEM в России, млрд руб.



Источник: TAdviser, 2023

Для сравнения, глобальный рынок SIEM-систем вырос в 2021 году на 20% по данным отчета Gartner и составил $4,1 млрд. Агентство IDC давало за тот же период более высокую оценку в $5,2 млрд (+16,6%). Такую динамику обуславливал рост числа киберугроз на фоне сохранения формата удаленной работы и распространения подхода BYOD (bring your own device) для рабочих задач, а также ввиду постепенного восстановления экономики после COVID-19.

[2]Определение объема рынка, долей вендоров и прогнозы роста SIEM проводилось на основе экспертных оценок авторов исследования, а также анализа данных известных аналитических агентств, в том числе информации об отгрузках открытых конкурсов торговых площадок

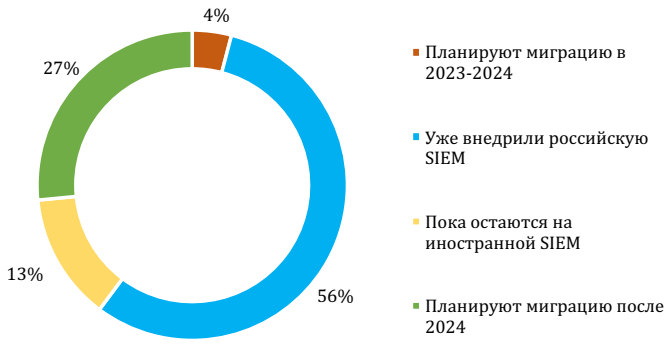
Российский рынок SIEM к настоящему моменту достаточно зрелый. Как показало исследование TAdviser, 97% опрошенных российских организаций сегодня используют SIEM. Эти системы обеспечивают решение комплексных задач ИБ (обнаруживать, расследовать атаки, реагировать на инциденты) и помогают эффективно противостоять расширяющемуся ландшафту киберугроз. Использование же SIEM-системы российской разработки отвечает регуляторным требованиям в части импортозамещения. Большинство опрошенных - специалисты крупных и средних предприятий, которые попадают под действие указа № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры РФ» (госорганизации, госкорпорации, субъекты КИИ, системообразующие предприятия), а также №187-ФЗ «О безопасности критической информационной инфраструктуры» (КИИ). Последний предписывает, в частности, что к 2025 гг. на российский софт должны перейти предприятия энергетики и финансовой сферы, а также полностью завершить импортозамещение ИТ-решений компании с госучастием и органы власти.

Поскольку импортозамещение остается одной из приоритетных национальных задач, российские компании активно запускают проекты миграции с зарубежного софта, чтобы гарантировать стабильную работу в условиях санкционных ограничений и соблюсти требования законодательства. В сфере ИБ эти инициативы реализовывались и до 2022 года, что обусловило более высокий уровень проникновения российских разработок в этом сегменте и в целом – более высокий уровень зрелости решений (как показывают опросы TAdviser, именно последний фактор часто сдерживает импортозамещение программных продуктов в других нишах).

Фиксируемое в 2022-2023 гг. ускорение динамики роста рынка SIEM-систем обусловлено также общим курсом на импортозамещение. По данным опроса TAdviser, в части SIEM более половины организаций-респондентов подтверждают, что к 2023 году уже внедрили (либо внедряют в настоящий момент) российские решения. Чуть более 10% пока продолжают использовать иностранные системы (речь идет о закупленных ранее лицензиях, которые остаются в собственности компаний, хотя уже без регулярных обновлений и поддержки со стороны вендоров). Почти треть запланировали миграцию после 2024 года, с учетом сформированных road map'ов импортозамещения ИТ (в

крупных организациях такие инициативы реализуются поэтапно и рассчитаны в среднем на 3-4 года).

Планы по замене решения/миграции на российскую SIEM

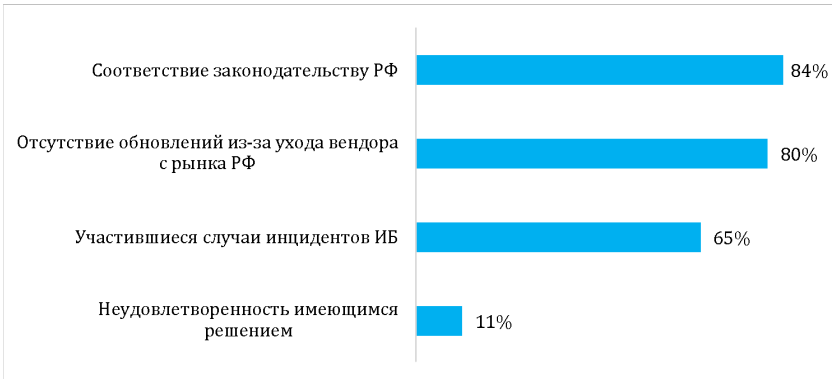


Источник: TAdviser, 2023

Основными стимулами к замене используемого иностранного решения на российскую SIEM респонденты называют необходимость соблюдения требований регулятора (84%), а также риски, связанные с отсутствием актуальных обновлений (80%) из-за ухода с российского рынка вендора используемой системы. Рост числа киберинцидентов отметили как триггер для проектов миграции 65% опрошенных.

Лишь 11% зафиксировали как причину замены неудовлетворенность ранее внедренными решениями от зарубежных вендоров.

Основные драйверы миграции на российскую SIEM



** - по данным респондентов, подтвердивших планы миграции в 2023-2024 гг, после 2024 г., а также ранее внедривших российское решение*

Источник: TAdviser, 2023

Подтверждая планы миграции после 2024 года, респонденты отмечают отсутствие пока понимания о наличии соответствующих бюджетов. Как правило, для таких закупок в крупных организациях используются статьи CAPEX, и в более 70% случаев они относятся к общему бюджету ИТ (при этом на их долю приходится до 10% ИТ-бюджета).

Более 70% респондентов считают, что их бюджет на SIEM в 2024 году увеличиваться не будет и сохранится на текущем уровне - на фоне в целом консервативного сегодня отношения бизнеса к расходам на ИТ (особенно в сегментах ТЭК, транспорт, промышленных предприятий, как показал ряд исследований TAdviser в 2023).

Планы изменения бюджета на SIEM в 2024

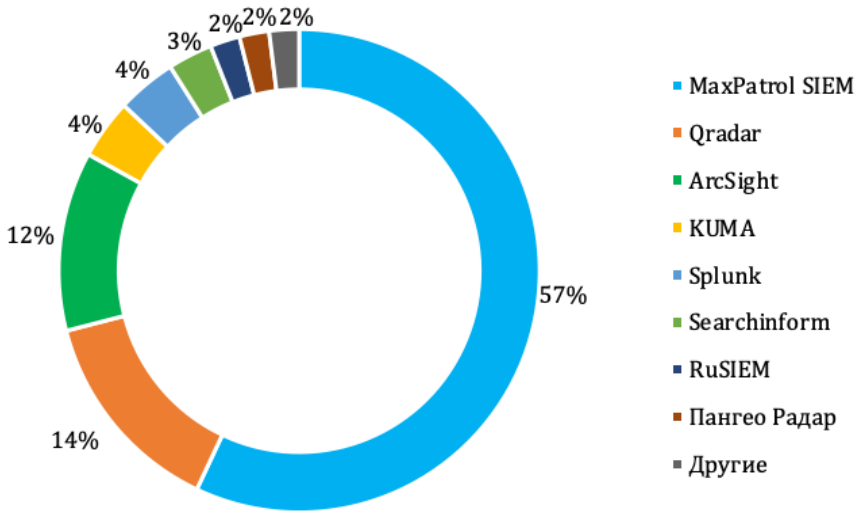
Источник: TAdviser, 2023

Ключевые игроки российского рынка SIEM

Позиции российских поставщиков SIEM с 2022 года существенно укрепились ввиду массового ухода зарубежных вендоров с отечественного рынка. Доля локальных производителей выросла с 40% в совокупных затратах клиентов до более 50% в 2022 году и, на фоне снижения доли зарубежных продуктов, превысит 70% к 2024 г.

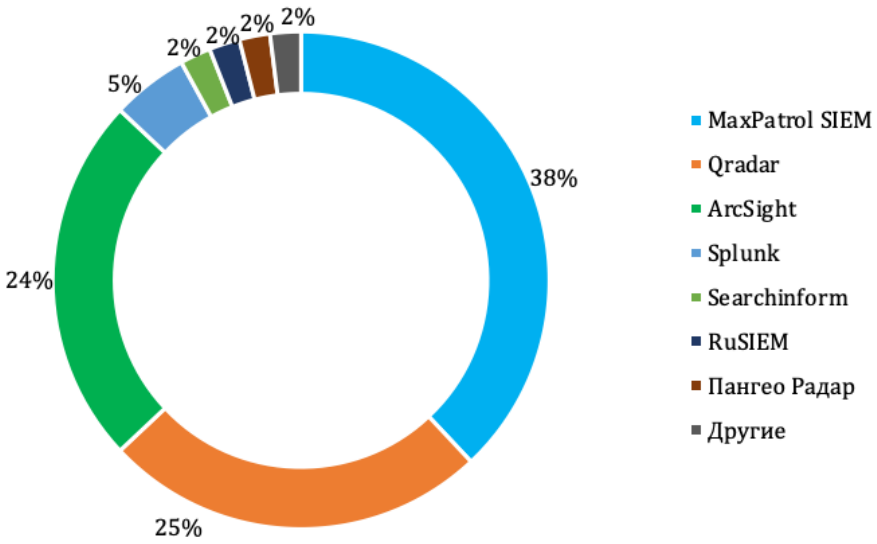
Среди поставщиков SIEM, по данным закупочных площадок и экспертных оценок TAdviser в 2022 году лидируют Positive Technologies (57%), Qradar (14%), ArcSight (12%).

Структура российского рынка SIEM по долям вендоров в 2022 году



Источник: TAdviser, экспертная оценка[3]

Структура российского рынка SIEM по долям вендоров в 2021 году



Источник: TAdviser, экспертная оценка[4]

[3] Определение объема рынка, долей вендоров и прогнозы роста SIEM проводилось на основе экспертных оценок авторов исследования, а также анализа данных известных аналитических агентств, в том числе информации об отгрузках открытых конкурсов торговых площадок

[4] Определение объема рынка, долей вендоров и прогнозы роста SIEM проводилось на основе экспертных оценок авторов исследования, а также анализа данных известных аналитических агентств, в том числе информации об отгрузках открытых конкурсов торговых площадок

Основные технологические тренды развития SIEM в мире и в России

По оценкам Gartner, в рамках продуктового развития SIEM-системы движутся в сторону многофункциональности: к 2025 году 75% глобальных вендоров будут предлагать клиентам консолидированные решения SIEM + (IRP[5]+SOAR[6]+TIP[7]), где IRP+SOAR+TIP будет сливаться в TDIR[8] (threat detection and incident response).

Соответственно, поддержка интеграции SIEM со сторонними решениями SOAR, UEBA, TIP (либо их наличие в самом решении) становится определяющей по критерию completeness of vision магического квадранта Gartner.

Также усиливается фокус разработчиков на решение задач сбора контекстных данных и обеспечения прозрачности ИТ-инфраструктуры за счет развития функции asset management, отмечают в Gartner.

По данным исследования Gartner, на глобальном рынке SIEM сегодня доминируют облачные решения (SaaS) – благодаря скорости и простоте развертывания, масштабируемости и гибкости. Тренд миграции SIEM-решений в облако будет сохраняться, а решения on-premise компании будут выбирать при условии необходимости выполнения требований зарубежных регуляторов.

В то же время выбор облачной SIEM определяется в целом активностью использования компанией-клиентом облачных сервисов для ведения бизнеса.

---

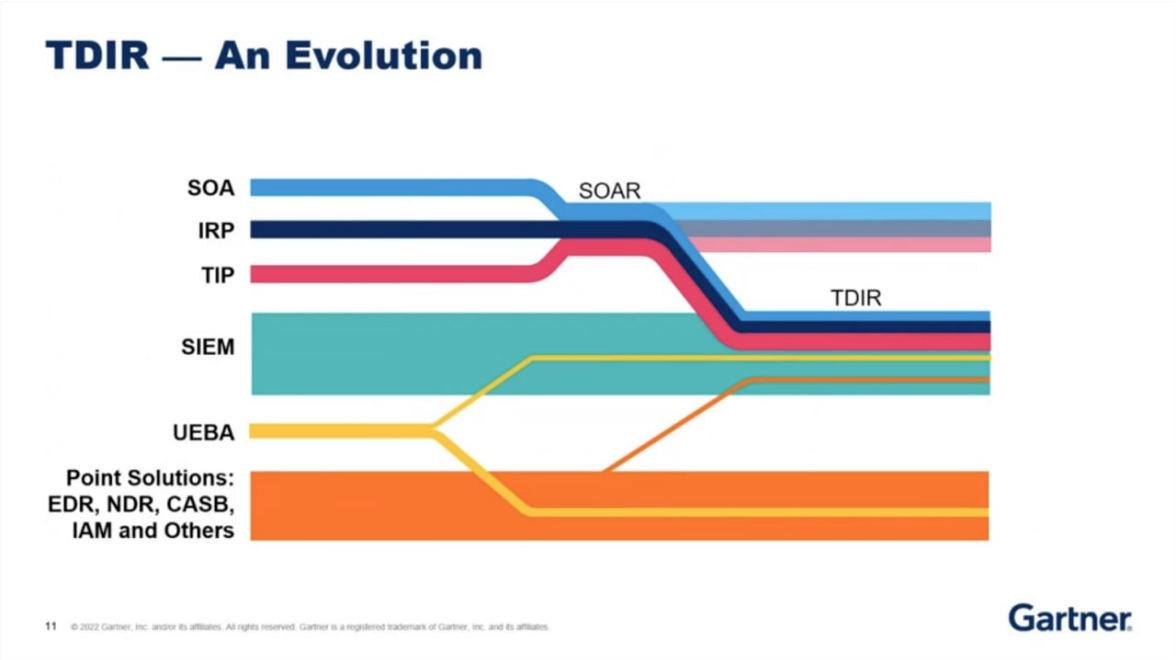
[5] IRP (Incident Response Platform) - платформа реагирования на инциденты

[6] SOAR (Security Orchestration, Automation and Response) - средства оркестровки (управления) систем безопасности

[7] TIP (Threat Intelligence Platform) - платформа для работы с данными киберразведки

[8] TDIR (Threat Detection and Incident Response)- средства обнаружения угроз и реагирования на инциденты

Траектория развития SIEM решений по версии Gartner



В Топ-5 технологических трендов рынка SIEM компания Positive Technologies включает на ближайшие 2-3 года следующие:

1. Автоматическую адаптацию коробочной экспертизы под инфраструктурные особенности заказчика;
2. Синергию анализа событий с уровня конечных точек, приложений, трафика и СЗИ;
3. Поведенческий анализ на базе технологий ML, AI – обработку событий с учетом контекста и знаний о шаблонах поведения атакующих;
4. SIEM в облаке и для облака - использование облаков как источника данных и формата предоставления сервиса, в том числе, развитие MSSP функционала;
5. Автоматизация взаимодействия со смежными ИБ системами.

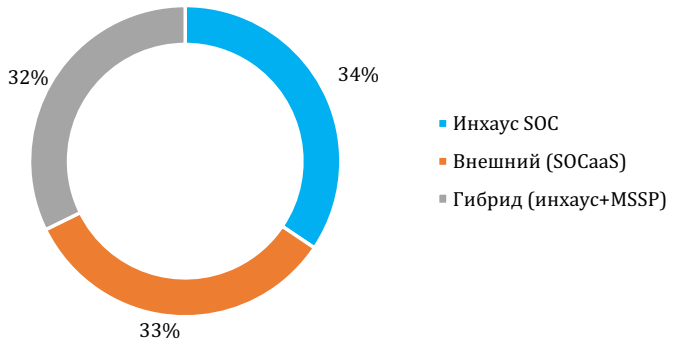
Обозначенные технологические тренды будут стимулировать повышение качества работы с SIEM и обеспечат прозрачность управление инфраструктурой. А за счет автоматизации сократится объем ручной работы операторов при мониторинге и реагировании на инциденты.

Проникновение сервисной модели в потреблении решений ИБ

96% опрошенных подтверждают наличие в своих организациях SOC. У более трети из них речь идет об инхаус центрах – как правило, их развивают крупные компании с развитыми функциями ИБ. Еще примерно треть таких организаций используют гибридный подход, когда технологический стек разворачивается инхаус, при этом управление осуществляет MSSP, закрывая таким образом (отчасти) дефицит кадров на этом рынке.

Именно отсутствие специалистов внутри, вместе с недостаточно проработанными или с не вполне зрелыми процессами, указывают среди основных причин, тормозящих создание SOC в ряде организаций.

Использование SOC в российских организациях

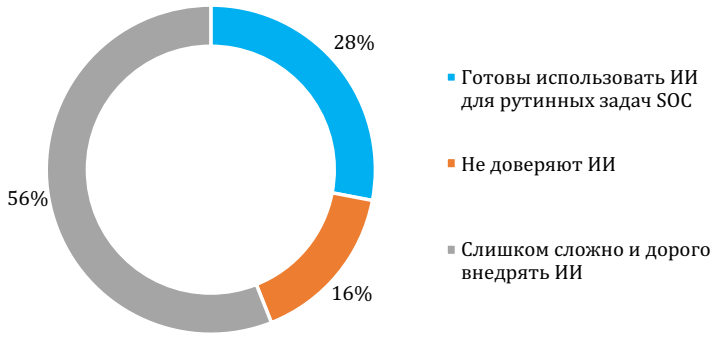


Источник: TAdviser, 2023

У почти 90% опрошенных ядром SOC служит решение SIEM.

Более трети респондентов хотели бы заменить рутинную работу своих операторов SOC, внедрив технологии искусственного интеллекта и машинного обучения (AI/ML). Однако более половины пока воздержались бы от такого шага ввиду высокой, по их внутренней оценке, стоимости и сложности таких проектов на текущем этапе развития и проникновения технологий. В том числе часть респондентов смущает и недостаточная экспертиза поставщиков для реализации таких проектов для задач конкретного бизнеса.

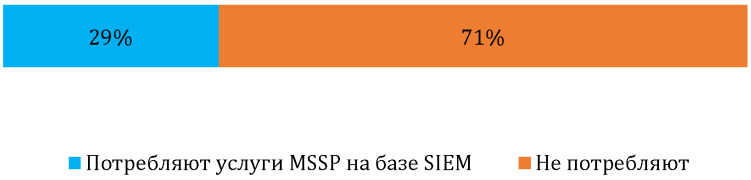
Перспективы использования ИИ для задач SOC



Источник: TAdviser, 2023

Около трети респондентов подтверждают потребление услуг провайдеров MSSP на базе SIEM решений. В частности, речь идет об услугах подключения источников (более 70%), сервисе реагирования (около 60%), а также о разработке правил корреляций (45%).

Потребление услуг MSSP на базе SIEM решения



Источник: TAdviser, 2023

Планируют переходить на модель потребления услуг ИБ от MSSP на базе SIEM более 10% опрошенных. Такие сдержанные прогнозы связаны, в том числе, с пока недостаточно высоким уровнем доверия к MSSP и вообще к облачной модели предоставления услуг (здесь, в том числе, сказались последствия прошлогодних «отключений» российских заказчиков от внешних сервисов вендорами из западных стран).

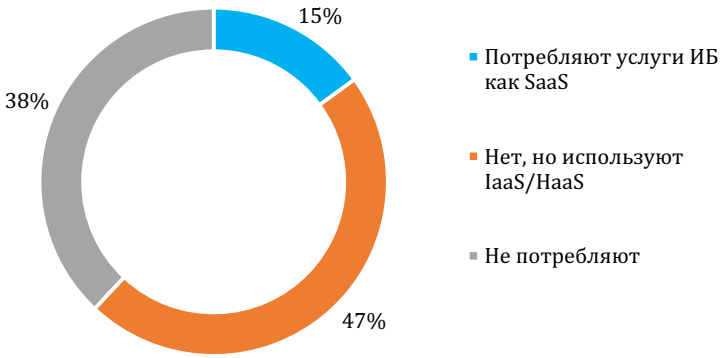
Планы потребления услуг MSSP на базе SIEM решения

** - по данным респондентов, не потребляющих услуг MSSP на базе SIEM в настоящий момент*

Источник: TAdviser, 2023

К настоящему моменту используют продукты ИБ как сервис только 15% опрошенных компаний. При этом 47% подтвердили практику использования инфраструктурных сервисов из облака IaaS (либо HaaS). Более трети респондентов в целом воздерживаются от облачных решений в сфере ИБ.

Использование продуктов ИБ как сервис

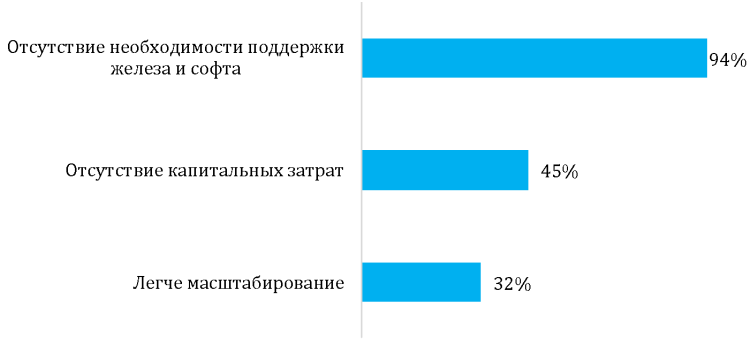


Источник: TAdviser, 2023

Тем не менее, среди тех, кто пока не потребляет ИБ продукты по сервисной модели, более трети все же планируют переходить на такую модель (36%). Основным стимулом здесь становится возможность обойти таким образом другую прошлогоднюю проблему – сложности, высокую стоимость и длительные сроки при закупке оборудования, по-прежнему сохраняющие актуальность на отечественном рынке. 94% указывают отсутствие необходимости в поддержке железа и софта собственными силами как

основной фактор выбора модели SaaS. Также для 45% важна возможность оптимизировать, либо сократить за счет перехода в облако капитальные затраты.

Факторы выбора модели SaaS для потребления услуг ИБ



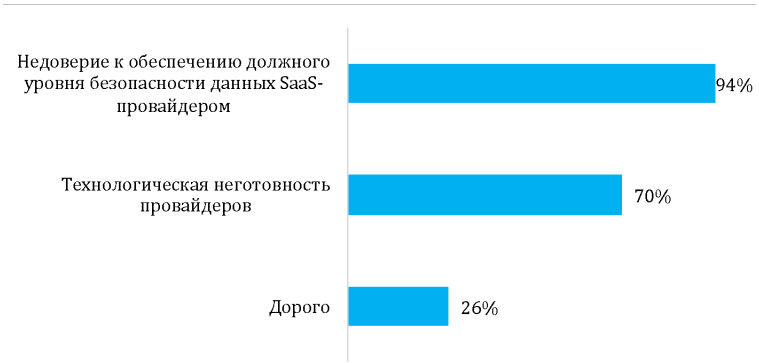
** - по данным респондентов, планирующих переход на SaaS модель потребления решений ИБ*

Источник: TAdviser, 2023

В то же время и недоверие к обеспечению должного уровня безопасности данных со стороны SaaS-провайдера сохраняется – этот фактор доминирует среди тех респондентов, кто по-прежнему отказывается переходить в облако (94%). Еще 70% из них указывают как сдерживающий фактор технологическую неготовность провайдеров к предоставлению стабильного, бесшовного и удобного в потреблении сервиса.

На результатах сказывается также географическая распределенность крупных компаний – по данным исследования, а также предыдущих опросов TAdviser в 2023 г., для них по-прежнему критична, в свете перехода в облако, негарантированная стабильность каналов во всех регионах присутствия в стране.

Сдерживающие факторы потребления услуг ИБ по модели SaaS

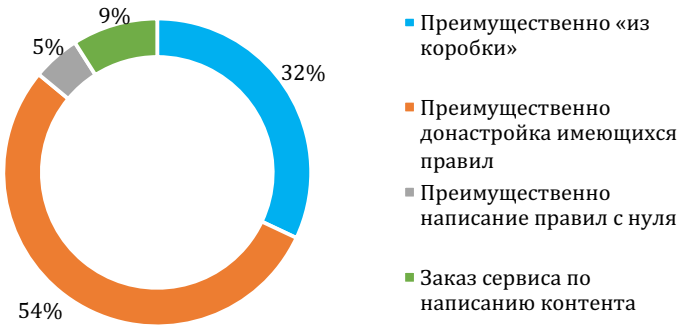


** - по данным респондентов, не планирующих переход на SaaS модель потребления решений ИБ*

Источник: TAdviser, 2023

При работе с контентом в SIEM более половины опрошенных ориентируются на донастройку имеющихся правил. При этом более трети планируют работать преимущественно «из коробки» - на базе внешней экспертизы от вендора. Большинство опрошенных заказчиков избегают как написания правил с нуля, так и заказа такого сервиса у внешнего поставщика.

Основные подходы к работе с контентом в SIEM



Источник: TAdviser, 2023

Спрос и ожидания от SIEM-систем

При выборе решения SIEM российский крупный и средний бизнес ориентируется в первую очередь на постоянно обновляемые правила для обнаружения актуальных угроз (83%), на возможность реагировать на события безопасности прямо из SIEM (65%) и на удобство интерфейса для оператора/аналитика ИБ (64%).

Более 50% обращают также внимание на поддержку мультитенантности[9] и на гибкость архитектуры. Еще более 40% заинтересованы в возможности быстрого старта, а также использовании поведенческой аналитики, AI и ML.

[9] Мультитенантность - возможность изолированно обслуживать разных пользователей (подписчиков) в рамках одного сервиса (инсталляции или развертывания)

Ключевые факторы при выборе решения SIEM. Первого приоритета

Источник: TAdviser, 2023

Среди других приоритетных факторов, которые учитываются при выборе SIEM, респонденты отметили наличие технической поддержки (97%), а также стоимость решения (88%).

Почти половина считают важным эффективное использование вычислительных ресурсов – в том числе, на фоне общих сейчас проблем с их расширением. Со 2 квартала 2022 года многие компании испытывают сложности с закупкой оборудования после ухода с российского рынка западных поставщиков. С дефицитом вычислительной техники сталкиваются в том числе и дата-центры.

С учетом запуска параллельного и «серого» импорта сроки поставок могут достигать до 9 (и более) месяцев, при значительном росте цен. Выделить и согласовать иногда в разы увеличившиеся суммы на такие закупки заказчикам становится сложнее – бизнес не готов к такому увеличению нагрузки на CAPEX.

Факторы выбора решения SIEM. Второго приоритета

Источник: TAdviser, 2023

Необходимость качественной техподдержки (а качество здесь определяется, в основном, в сравнении с ранее знакомой практикой западных вендоров) указывают как одну из основных сложностей при настройке и эксплуатации SIEM почти 90% респондентов. Значимость этого фактора обостряется и дефицитом кадров – как внутри компании, так и на рынке в целом (его отмечают 81%).

Для почти 70% опрошенных проблемой в таких проектах остается необходимость выделять вычислительные ресурсы на фоне явного дефицита оборудования и непонятных перспектив по возможностям увеличения мощностей.

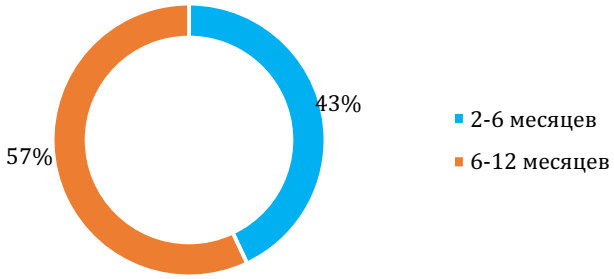
Основные сложности при настройке и эксплуатации SIEM

Источник: TAdviser, 2023

Оптимальным сроком внедрения SIEM-системы (с учетом ее развертывания, подключения источников, написания необходимых правил корреляций) более половины опрошенных считают до 12 месяцев. Более 40% компаний хотели бы уложиться с таким проектом до полугода.

В то же время, никто из опрошенных респондентов не считает оптимальным выход внедрения за рамки одного года. Также нет и сверхоптимистичных ожиданий быстрого старта за 1-2 месяца – с учетом достаточно масштабных инфраструктур у большинства организаций-респондентов и сложившегося опыта реализации проектов ИТ/ИБ.

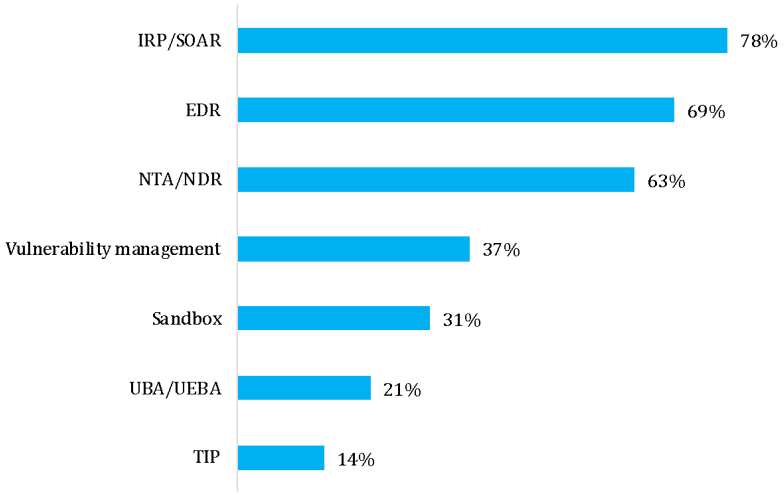
Оптимальный срок внедрения SIEM-системы



Источник: TAdviser, 2023

В контексте единой экосистемы с SIEM компании в первую очередь выделяют такие продукты для интеграции, как IRP/SOAR (78%), EDR (69%) и NTA/NDR (63%). Более трети отмечают также необходимость интеграции с Sandbox.

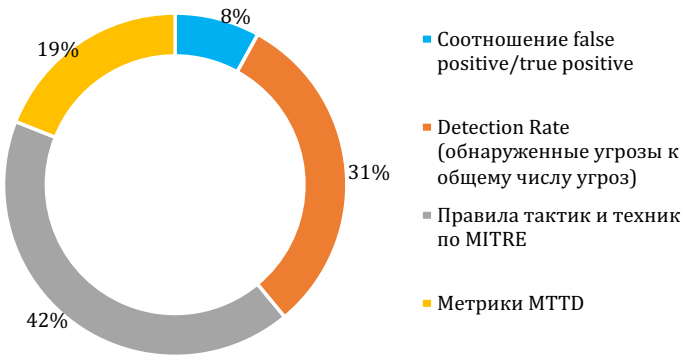
Основные продукты для интеграции в единую экосистему с SIEM



Источник: TAdviser, 2023

Эффективность работы SIEM большинство опрошенных организаций (61%) считают возможным оценивать через метрики – MTTD, а также правила тактик и техник по MITRE. К Detection Rate (обнаруженные угрозы к общему числу угроз) апеллируют еще более трети респондентов.

Подходы к оценке эффективности работы SIEM



Источник: TAdviser, 2023

При подходе к измерению эффективности использования SOC большинство заказчиков-респондентов (83%) ориентируются в первую очередь на соответствие требованиям регулятора (количество найденных нарушений, скорость реакции на запросы от

аудиторов и т.д). На втором месте – устоявшиеся и знакомые по опыту взаимодействия с зарубежными вендорами метрики типа MTTD/MTTR (76%).

Характерно, что никто из опрошенных не указал подхода к оценке ROCI (Return On Cyber Investments) – в значительной мере потому, что в российских организациях такой показатель в принципе мало распространен и почти не рассчитывается официально.

Подходы к оценке эффективности использования SOC

Источник: TAdviser, 2023

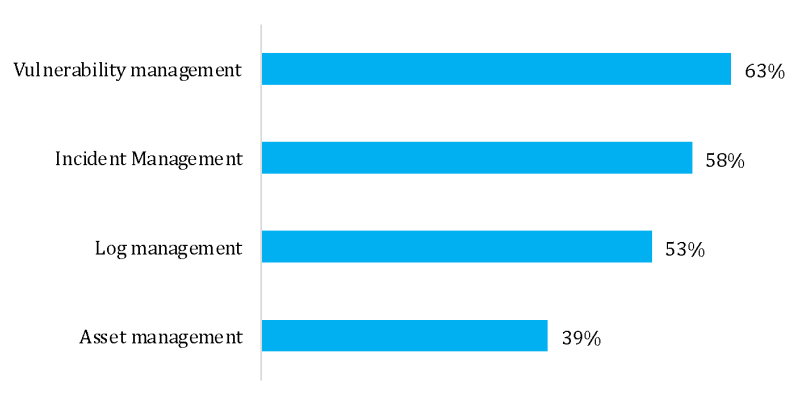
По итогам внедрения SIEM почти все опрошенные организации рассчитывают на своевременное обнаружение попыток нарушения киберустойчивости и инцидентов, ведущих к недопустимым событиям (97%). Более чем для половины важно также получение актуальной обновляемой экспертизы для защиты своей инфраструктуры.

Ожидаемые результаты от внедрения SIEM

Источник: TAdviser, 2023

Более 60% опрошенных считают, что для задач ИТ-отдела могут быть полезными такие функции SIEM системы, как Vulnerability management (63%), Incident Management (58%) и Log management (53%).

Оценка полезности функций SIEM для задач службы ИТ



Источник: TAdviser, 2023

Основные выводы

Рынок SIEM в России сохраняет позитивную динамику и продолжит расти до 2027 года. Его драйверами остаются растущие киберугрозы, усиливающиеся кибератаки на российские организации, а также потребность в импортозамещении зарубежных систем ввиду ужесточения законодательства и усиление внимания регуляторов к использованию отечественного ПО.

97% крупных и средних организаций, опрошенных TAdviser в 3 кв. 2023 года, уже используют SIEM-систему. С учетом общего курса на импортозамещение более половины организаций-респондентов к 2023 году уже внедрили (56%), либо внедряют сейчас (27%) российские решения. Еще треть запланировали миграцию на отечественные SIEM-системы после 2024 года.

При выборе решения SIEM опрошенные представители российского крупного и среднего бизнеса ориентируется в первую очередь на постоянно обновляемые правила для обнаружения актуальных угроз (83%), возможность реагировать на события безопасности прямо из SIEM (65%), а также на удобство интерфейса для пользователя системы - оператора или аналитика ИБ (64%).

Более 50% респондентов при выборе SIEM-системы обращают внимание на гибкость архитектуры. Еще более 40% заинтересованы в возможности быстрого старта, а также в использовании поведенческой аналитики, AI и ML. В контексте построения единой экосистемы с SIEM опрошенные компании выделяют интеграцию с IRP/SOAR (78%), EDR (69%) и NTA/NDR (63%).

По итогам внедрения SIEM почти все опрошенные организации рассчитывают на своевременное обнаружение инцидентов, ведущих к недопустимым событиям (97%), а также на получение актуальной обновляемой экспертизы для защиты своей инфраструктуры (59%).

Сервисная модель до последнего времени не получила широкого распространения при потреблении ИБ продуктов в России. Сегодня используют услуги провайдеров MSSP на базе SIEM решений около трети респондентов TAdviser. В целом уровень доверия к облачной модели предоставления услуг в сегменте ИБ пока невысокий - компании беспокоятся о безопасности и доступности своих данных. Однако сложившееся осторожное отношение к облакам уже сегодня может быть пересмотрено ввиду необходимости решения проблем, связанных с дефицитом оборудования и персонала на фоне потребности в обеспечении качественной техподдержки. Более трети респондентов, пока не потребляющих ИБ продукты по сервисной модели, планируют переход на нее в ближайшее время. Почти все из них указывают отсутствие необходимости в поддержке железа и софта собственными силами как основной фактор выбора модели SaaS.