Ценность для бизнеса от внедрения платформы Kaspersky Anti Targeted Attack и Kaspersky EDR

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Введение

Данный документ поясняет актуальность построения процессов по выявлению сложных угроз и целевых атак, а также отвечает на ряд вопросов:

- В чем ценность для бизнеса от внедрения решений по противодействию сложным угрозам?
- Как аргументировать выделение бюджета на платформу Kaspersky Anti Targeted Attack (KATA) и Kaspersky EDR?
- Какие преимущества от внедрения этих решений получит организация?

Сегодня успешная деятельность любой компании напрямую зависит от надежной защиты ее активов, стабильности бизнес-процессов и безопасности ИТ-инфраструктуры, и особенно это актуально для объектов критической информационной инфраструктуры (КИИ). Постоянный рост числа и сложности киберугроз в эпоху глобализации информационной среды и необходимость соответствия нормативам регулирующих органов, стандартам банковской отрасли, GDPR и PCI DSS, а также соблюдения российского законодательства по безопасности КИИ требуют от организаций внедрения эффективной стратегии защиты от комплексных угроз и целевых атак и учета требований регуляторов.

Основные факторы инвестиций в кибербезопасность

По данным опроса о расходах на IT-безопасность среди менеджеров высшего звена ИТ и ИБ-департаментов "SANS 2020 IT Cybersecurity Spending Survey", ведущими факторами инвестиций в кибербезопасность на сегодняшний день являются: необходимость сокращения числа инцидентов и нарушений, соблюдение требований регуляторов, понимание необходимости идти в ногу с меняющимся и все более сложным ландшафтом угроз и выстраивания правильных процессов расследования, и реагирования на сложные инциденты.

69% Необходимость соответствия требованиям регуляторов

59% Сокращение числа инцидентов

57% Рост количества и сложности угроз

40% Выстраивание процессов расследования и реагирования

Атака — лишь вопрос времени

Любая организация, занимающая значительный сегмент рынка – потенциальная цель атак. Это касается даже небольших компаний: сегодня преступники проявляют и к ним интерес, а также используют как легкую промежуточную цель на пути к крупной добыче. А для лидеров рынка вероятность стать жертвой современной атаки возрастает еще больше.

Современные тенденции киберпреступности

Сегодня злоумышленники выбирают в качестве целей организации любого размера, сферы деятельности и уровня готовности к отражению угроз. Стоимость подготовки атак снижается, что подвергает риску большее число организаций. Для каждой компании найдется свой злоумышленник – и это всего лишь вопрос времени.

Сегодня наибольшую опасность для организаций представляют сложные угрозы и целевые атаки, включая комплексные угрозы уровня APT.

В отличие от обычного вредоносного ПО, сложные атаки осуществляются под контролем и управлением опытных киберпреступников. Злоумышленники стремятся закрепиться внутри корпоративного периметра и, оставаясь длительное время незамеченными, получить полный контроль над системами инфраструктуры.

Они адаптируют атаки на каждом этапе для обхода традиционных средств защиты, пытаются использовать уязвимости и все возможные точки проникновения в инфраструктуру. Разумеется, злоумышленники стремятся свести к минимуму затраты, используя наиболее дешевые средства атаки для максимальной финансовой отдачи.

Комплексная атака может также включать абсолютно базовые технологии и подходы. Мошенники способны, например, проникнуть в системы организации всего за несколько минут при относительно низких затратах, используя готовое многоцелевое вредоносное ПО — дешевое и простое. Помимо низкой стоимости, такие несложные инструменты обладают дополнительным преимуществом: они позволяют преступнику маскировать целенаправленные атаки под распространенные угрозы и таким образом успешно скрывать свои истинные намерения. Тенденция снижения цены на подобного рода вредоносное ПО и увеличение предложений от киберпреступных группировок неуклонно ведут к росту общего количества сложных атак.

Ситуация усугубляется и тем, что многие организации пытаются защититься от новейших угроз при помощи традиционных технологий безопасности, в то время как киберпреступники постоянно совершенствуют свои методы. Превентивные технологии изначально не разрабатывались для противодействия современным комплексным угрозам; они помогают выявить инциденты, однако зачастую не способны определить тот факт, что поступающие предупреждения могут быть составными частями более опасной и сложной схемы, которая может повлечь за собой огромный ущерб — как единовременно, так и в долгосрочной перспективе.

Кто организует атаки?

Киберзлоумышленники — продают данные тому, кто больше заплатит, или просто похищают деньги. Обычно создают инструменты для преступления сами или покупают их на черном рынке.

APT-группировки — направлены в первую очередь на получение финансовой выгоды. Проводят как массовые, так и частные атаки с применением широкого спектра мер для достижения своей цели: от технических и программных средств, утилит и ПО до социальной инженерии.

Конкурирующие компании — ищут конфиденциальные данные или даже пытаются совершить саботаж. Обычно оплачивают «услуги» наемных исполнителей. Эти исполнители – профессионалы кибершпионажа, разрабатывают собственные инструменты и продают свои «услуги» тому, кто больше заплатит.

Хактивисты — нацелены на достижение политической, социальной или религиозной (в их понимании) справедливости в соответствии с намерениями группы. Заявляют о своих благих целях, изобретательны, используют сложный инструментарий и представляют серьезную проблему для любой организации, привлекшей их внимание.

Правительственные органы — правительственные структуры во всем мире могут вести регулярную слежку за отдельными лицами, группами и компаниями, хотя и отрицают это. Их инструментарий может быть чрезвычайно изощренным, дорогостоящим и сложным для обнаружения.

Почему сегодня уже недостаточно традиционных средств защиты от сложных угроз?

Специфика подготовки целевых атак и их проведения:

- детальное изучение используемых средств защиты с целью их обхода;
- разработка уникального ПО и закрепление его в инфраструктуре цели;
- использование при атаках доверенных, но скомпрометированных объектов;
- применение легитимных инструментов;
- применение многовекторного подхода к проникновению;
- скрытность и устранение следов.

Технологические ограничения традиционных средств защиты:

- создавались в условиях другого ландшафта угроз;
- обнаружение направлено только на распространенные (несложные) угрозы, уже известные уязвимости и методы;
- нет технологий выявления комплексных атак, требующих анализа первопричин и дополнительного расследования;
- не собирают и не хранят данные для последующего ретроспективного анализа;
- нет наглядной визуализации и встроенного сопоставления данных;
- нет возможности обогащения обнаружений дополнительным контекстом из глобальной базы знаний об угрозах (Threat Intelligence) для расследования сложных инцидентов.

Обоснование выгод от внедрения и ценность для бизнеса

Как обосновать реальную выгоду от внедрения решений по противодействию сложным угрозам и показать ценность для бизнеса?

Основным камнем преткновения при защите бюджета ИБ-департамента для формирования защиты от современных киберугроз становится обоснование инвестиций в построение защиты от инцидентов, которые на момент бюджетирования являются все еще потенциальными. Среди наиболее популярных аргументов лиц, принимающих решения: «Не факт, что такие атаки произойдут, а деньги будут потрачены».

Организации редко проецируют на себя инциденты, затронувшие другие компании и склонны считать, что сложные угрозы и вытекающие последствия никогда их не коснутся. Однако сегодняшняя статистика подтверждает обратное: ни одна компания не застрахована от сложных атак и может стать целью в любой момент. Данные также демонстрируют, насколько дорогостоящими могут быть современные киберинциденты — как в репутационном, так и в денежном выражении.

Обосновать необходимость выделения бюджета на реализацию стратегии защиты от современных угроз — непростая задача. Несмотря на то, что уровень финансовых потерь в случае успешной кибератаки вероятнее всего превысит сумму требуемых инвестиций, лица, принимающие решения, по-прежнему настаивают на демонстрации реальных, измеримых результатов от внедряемых систем и хотят видеть более ощутимые показатели, указывающие на необходимость инвестирования.

В данном документе описаны 3 основных подхода для обоснования инвестиций:

1. **Анализ рисков**
2. **Анализ временных затрат**
3. **Требования регуляторов**

Анализ рисков

В чем состоит риск для ключевых отраслей?

Финансовые структуры

- несанкционированные транзакции
- атаки на банкоматы с похищением наличности
- кража персональных данных

Государственные услуги

- манипуляция данными
- шпионаж
- ограниченная доступность онлайн-услуг
- кража персональных данных
- действия хактивистов

Производство и высокие технологии

- шпионаж (производственные секреты)
- компрометация критически важных технологических процессов
- саботаж

Телекоммуникации

- атаки на корпоративных клиентов через телекоммуникационную инфраструктуру
- контроль выставления счетов
- манипуляция веб-ресурсами для использования в фишинговых атаках
- использование скомпрометированной инфраструктуры (устройств/интернета вещей) при DDoS-атаках

Энергоснабжение и коммунальные услуги

- манипуляции результатами расчетов
- атаки на технологические сети с нанесением физического ущерба

СМИ

- хактивизм
- компрометация веб-сайтов (взлом с целью замены страниц на фальшивые, фишинг)
- распространение атак на широкую аудиторию

Здравоохранение

- похищение информации о пациентах
- атаки на оборудование дистанционного оказания медицинских услуг

К чему приводят сложные угрозы и целевые атаки?

За сложными угрозами и целевыми атаками стоят профессионалы, для которых киберпреступления – способ заработка. Их единственная цель при выборе предприятия и организации атаки — извлечение максимальной прибыли. Ее они рассчитывают еще до начала атаки, учитывая сопутствующие расходы и потенциальный уровень вознаграждения.

В наши дни стоимость запуска эффективной кибератаки значительно снизилась, что вызвало бурный рост общего количества атак во всем мире.

Чем рискует организация при целевой атаке?

- компрометация данных
- утеря критичных данных
- кража коммерческой тайны
- уничтожение ИТ-инфраструктуры
- прерывание основных бизнес-процессов
- недоступность предлагаемых сервисов
- кража денежных средств
- ухудшение репутации
- потеря конкурентного преимущества
- утеря доверия клиентов
- уменьшение занимаемой доли на рынке
- прямые и косвенные денежные потери

Восприятие уровня риска

Интересный факт: до инвестирования в решение по защите от сложных угроз и целенаправленных атак компании находятся под высоким риском, при низком уровне его осознания и принятия. После развертывания специализированного решения риск значительно снижается, в то время как восприятие риска встречи со сложными инцидентами у этих организаций уже гораздо выше. Почему так происходит? К сожалению, основным обоснованием выделения бюджета на усиление существующей защиты зачастую остается факт уже случившегося инцидента с ощутимым ущербом, который вполне возможно измерить.

Когда компания подвергается кибератаке

операционные расходы мгновенно взлетают: пени, штрафы, страховые выплаты, приобретение нового ПО и обучение персонала.

Потери при реализации риска

По данным глобального исследования «Лаборатории Касперского» в 2020 году "IT Security Economics", средняя сумма расходов крупной компании в результате инцидентов, связанных с утечкой данных в 2020 году, составила **1 миллион 92 тысячи долларов** США.

В ходе этого опроса были проинтервьюированы 5266 респондентов из 31 страны, включая Россию и СНГ, заданы вопросы о состоянии IT-безопасности в их организациях, угрозах, с которыми они столкнулись, и расходах, понесенных в ходе ликвидации последствий атак.

Для 70% российских компаний вопрос защиты данных является главной проблемой, связанной с кибербезопасностью.

В среднем, в 2020 году прямые потери от инцидента, связанного с утечкой данных, составили **745 тыс. долларов** США во всем мире, а последующие затраты **347 тыс. долларов** США.

Средняя сумма расходов крупной компании в мире в результате утечки данных

$ 745 тыс. — прямые потери

$ 347 тыс. — последующие траты

Стоимость минимизации риска

Компании не должны ожидать прямых выгод от инвестиций в стратегию защиты от кибератак. Основная выгода здесь — это минимизация риска инцидентов, и потерь в случае их возникновения.

Подсчитать экономию при своевременной локализации сложной атаки нелегко, однако примерный подсчет возможных потерь на основе данных статистики по убыткам компаний из смежных областей из открытых источников вполне может помочь составить примерное представление.

Формула для расчета окупаемости инвестиций применительно к информационной безопасности:

$$\frac{\text{Возможный материальный ущерб} - \text{Совокупная стоимость владения}}{\text{Совокупная стоимость владения}} \times 100\%$$

Используя эту формулу и представленные усредненные значения по потерям организации за один инцидент, можно произвести необходимый расчет

Большинство затрат на решение складывается из стоимости лицензий и требуемого оборудования, расходов на персонал и стоимости технической поддержки.

Материальный ущерб складывается из стоимости одного инцидента, умноженного на их количество, например, за год.

Не стоит забывать, что ценность, которую обеспечивают решения по противодействию сложным угрозам и целевым атакам, такие как Kaspersky Anti Targeted Attack (KATA) и Kaspersky EDR, заключается в отсутствии затрат, которых удалось избежать, а не в получении прямых доходов.

Одной из целей инструментов защиты от APT-угроз и других сложных атак, в том числе платформы KATA и Kaspersky EDR, является усложнить проведение кибератак настолько, чтобы они стали практически невозможными или экономически нецелесообразными. Обычно в такие решения интегрирован целый ряд передовых технологий: чем больше уровней защиты и контролируемых потенциальных точек входа для атаки, тем выше вероятность обнаружения, сколько бы времени и денег злоумышленник ни тратил на подготовку.

Противодействие угрозам

Противодействие современным угрозам и сложным атакам требует налаженного процесса реагирования на инциденты — от сбора данных, обнаружения угроз, приоритизации, расследования до оперативной нейтрализации угрозы.

Анализ временных затрат

2

При возникновении инцидента от сотрудников, ответственных за ИБ, требуются быстрые и точные шаги, которые позволят максимально снизить ущерб от инцидента.

В ходе опроса «Лаборатории Касперского» в 2020 году "IT Security Economics" было выявлено несколько факторов, которые могут помочь предприятиям снизить стоимость утечки данных:

Быстрое обнаружение

потери ниже **на 32%**

Финансовые потери были на 32% ниже на предприятиях, которые смогли обнаружить нарушение почти мгновенно и предпринять необходимые меры по нейтрализации угрозы, по сравнению с теми, которые сделали это в течение недели или более.

Своевременное раскрытие информации об утечке

ущерб меньше **на 28%**

В среднем, предприятия, которые добровольно информируют свою аудиторию о нарушении, несут на 28% меньше финансовый ущерб, чем в ситуациях, когда их клиенты и другие заинтересованные стороны узнают новости об утечке данных из средств массовой информации.

Использование современных технологий

стоимость ниже **на 53%**

Стоимость утечки данных снижается на 53% для организаций, которые используют современные технологии и своевременно обновляют ПО.

Время является одним из самых дефицитных ресурсов при расследовании и реагировании на инциденты, а скорость мер реагирования, предпринятых сотрудниками ИБ, уменьшает шансы для атаки достичь своих целей.

Рассмотрим два важных временных критерия:

2.1 **Время обнаружения**

2.2 **Время реагирования**

Время обнаружения

2.1

По данным аналитического отчета «Лаборатории Касперского» за 2020 год «Реагирование на компьютерные инциденты», время обнаружения первых признаков зависит от типа атаки, относящейся к одной из трех категорий по длительности:

Быстрые атаки

Атаки длительностью менее суток.

В основном, это инциденты, связанные с заражением шифровальщиками. Ввиду большой скорости развития, эффективное противодействие данным атакам возможно только превентивными методами. В некоторых случаях была замечена задержка между первичной компрометацией и началом активных действий со стороны атакующего, вплоть до недели.

Атаки средней длительности

Атаки, развивающиеся несколько дней.

В подавляющем большинстве случаев эти атаки направлены непосредственно на хищение денежных средств. Как правило, злоумышленники добиваются поставленной цели в течение недели.

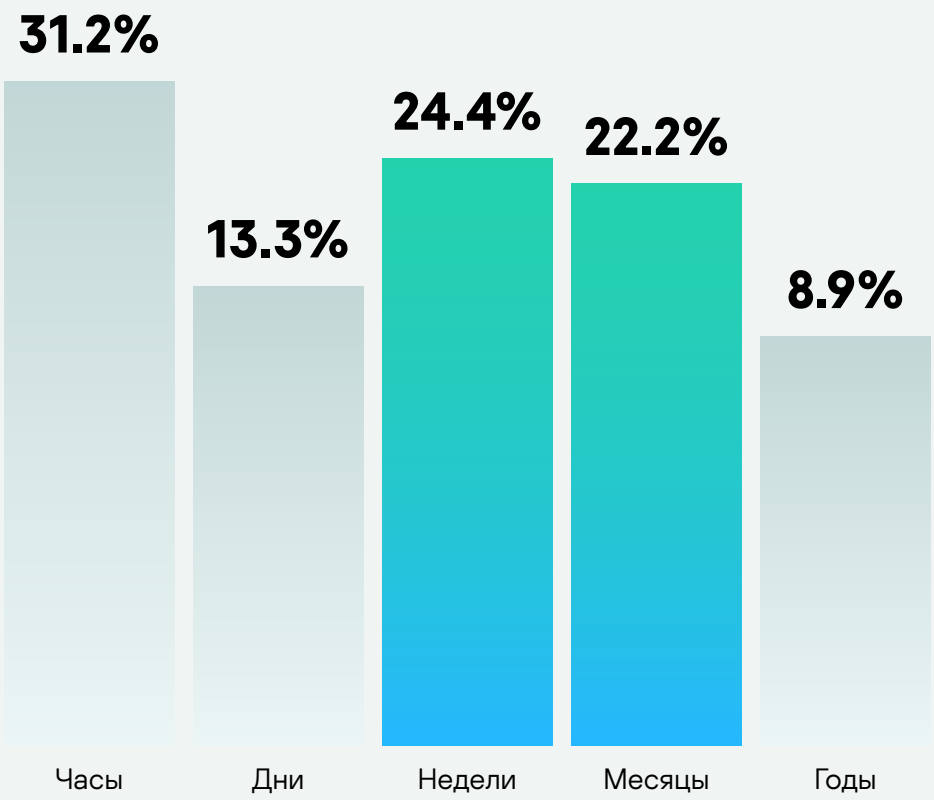
Длительные атаки

Атаки длительностью более нескольких недель.

Данная активность почти всегда направлена на похищение конфиденциальных данных. Для таких атак характерно чередование активных и пассивных фаз. Интересно, что суммарная продолжительность активных фаз в среднем близка к атакам средней длительности.

Обнаружение атак в течение нескольких часов чаще всего свойственно быстроразвивающимся атакам, таким как шифровальщики, с очевидными последствиями.

В соответствии с отчетом, обнаружение атак без явных разрушительных признаков, средних по продолжительности и длительных атак обычно занимает **от нескольких недель до нескольких месяцев.**



Время реагирования

2.2

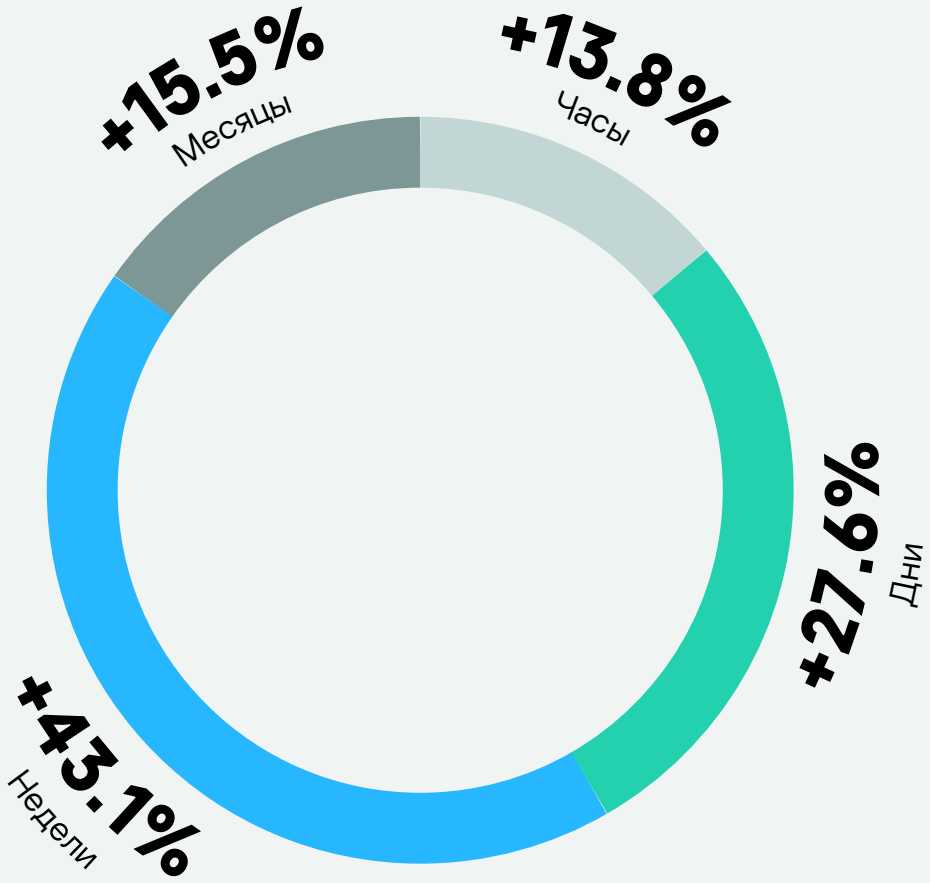
Предоставленные данные в отчете «Реагирование на компьютерные инциденты» по времени реагирования на инциденты основаны на данных реальных расследований, проведенных командой Global Emergency Response Team, занимающейся цифровой криминалистикой и реагированием на инциденты, в которую входят эксперты из Европы, Латинской Америки, Северной Америки, России и Ближнего Востока.

Это означает, что приведенные значения могут отличаться и в большую сторону, если организация выбирает путь самостоятельного реагирования на инциденты, не обладая необходимой экспертизой и/или специализированными инструментами.

Сегодня ИБ-специалисты сталкиваются с необходимостью:

- выполнения сложных задач в условиях нехватки квалифицированных кадров и экспертизы;
- ручного разбора и анализа большого числа инцидентов;
- принятия решений без использования средств наглядного централизованного представления информации;
- эксплуатации средств ИБ, которые не взаимодействуют друг с другом и управляются из разных консолей.

Согласно данным отчета «Лаборатории Касперского» за 2020 год «Реагирование на компьютерные инциденты», время, необходимое для принятия мер по реагированию на инцидент (от расследования инцидента до финальных действий по нейтрализации угрозы), чаще всего варьировалось **от нескольких дней до нескольких недель.** И, в том числе, определялось глубиной фактического проникновения злоумышленников в скомпрометированную сеть и количеством времени, прошедшим с момента первоначального взлома.



Очевидно, что **организации должны стремиться сократить время на обнаружение и реагирование**, что приведет к уменьшению риска успешной атаки, а также сократит временные, ресурсные и, соответственно, денежные затраты на восстановление после инцидента. В том числе организации должны учитывать тот факт, что неосторожные действия в рамках процесса реагирования на инциденты без достаточных экспертных знаний в этом вопросе могут спровоцировать злоумышленника произвести оперативные действия по сокрытию следов, что значительно затруднит процесс расследования и реагирования на инцидент или даже сделает его невозможным.

Согласно опросу "SANS 2019 Incident Response Survey: It's Time for a Change", основными ключевыми препятствиями на пути эффективного реагирования на инциденты остаются:

57% случаев

нехватка ресурсов и знаний

48% случаев

отсутствие бюджета на инструменты по противодействию сложным угрозам

Дефицит кадров в сфере информационной безопасности усугубляется недостатком знаний у аналитиков в вопросе противодействия сложным угрозам, отсутствием зачастую необходимого контекста для понимания серьезности оповещений от различных точечных ИБ-систем и усталостью от количества рутинной работы, требующей большой концентрации внимания.

При расследовании инцидента специалистам требуется определить:

- начальный вектор атаки
- размер ущерба, нанесенного атакой
- вредоносные программы и инструменты, которые были использованы в процессе атаки
- завершена атака или нет, то есть достиг ли атакующий своей цели
- затронутые в ходе атаки системы
- временные рамки атаки и пр.

Такая работа требует высококлассных нишевых специалистов с обширными знаниями, чутьем и опытом в области анализа вредоносного ПО, цифровой криминалистики, опытом взаимодействия с глобальными данными об угрозах и реагирования на инциденты. Специалисты должны уметь правильно интерпретировать данные, получаемые от средств защиты, увидеть и извлечь важную информацию из общего потока данных и обогащать получаемую информацию дополнительным контекстом. К сожалению, большинство сотрудников в роли аналитиков не достаточно обучены или перегружены рутинными задачами. Вместе с тем, эти сотрудники несут ответственность за просмотр информации и принятие критически важных решений: «Нужно ли продолжать это расследовать или нет?».

Для организаций, не использующих специализированные решения, обнаружение сложных угроз, включая сбор, хранение и анализ данных, а также проведение различных действий на этапах расследования и реагирования без применения средств автоматизации может оказаться крайне трудозатратным занятием.

Использование сразу нескольких инструментов в работе также сопряжено с увеличением количества ручных операций и ожидаемо приводит к неэффективному использованию, перегрузке ИБ-служб и к дополнительным затратам.

Автоматизация

Аналитики компаний тратят большое количество времени на рутинные операции, которые необходимы и важны, но могут быть автоматизированы. Автоматизация таких задач позволит организациям не только сэкономить дорогостоящее рабочее время аналитика, но и снизить их загрузку, позволив сосредоточиться на анализе и мерах по противодействию действительно сложным инцидентам.

Использование ИБ-службой специализированного комплекса Kaspersky Anti Targeted Attack и Kaspersky EDR — с единым веб-интерфейсом, поддержкой полного пакета функциональных возможностей, необходимых для всего цикла обработки сложных инцидентов, и максимально автоматизированными процессами — позволяет значительно сократить время на обнаружение и реагирование на сложные инциденты.

Для проведения дальнейших расчетов по возможным затратам на разрешение инцидентов, можно взять три усредненных варианта суммарного времени разрешения инцидента без использования специализированных средств, учитывая в том числе возможное разнообразие атак, с которыми могут столкнуться организации.

15 дней

30 дней

90 дней

Формулы для расчета времени, затраченного аналитиками при разрешении одного инцидента (без средств автоматизации)

При использовании сторонних услуг по реагированию на инцидент

Затраты на разрешение одного инцидента без автоматизации = **Время на разрешение инцидента** × **Стомость услуги по реагированию на инцидент**

При самостоятельном реагировании на инцидент без помощи специализированных средств

Затраты на разрешение одного инцидента без автоматизации = **Время на разрешение инцидента** × **Стоимость нормо-часа аналитика** × **Количество требуемых аналитиков**

Компании могут сделать примерный расчет на год, расходы на одного аналитика складываются:

- рыночная зарплата сотрудника с необходимой квалификацией
- премии и оплата переработок
- отчисления в фонды – 30 % от зарплаты
- обучение – до 10-15 % от зарплаты в год
- НДФЛ – 13 % от зарплаты

Стоимость нормо-часа аналитика

$$\text{Стоимость нормо-часа аналитика} = \frac{\text{Затраты на аналитика в год}}{52\ \text{недели} \times 5\ \text{рабочих дней} \times 8\ \text{часов}}$$

Расчет времени, затраченного аналитиками при разрешении одного инцидента с помощью дополнительного инструментария (с автоматизацией)

Прогнозируемая экономия от автоматизации

50-60%

По данным статистики ведущих аналитических агентств и нашего опыта, решения по противодействию сложным угрозам, такие как Kaspersky Anti Targeted Attack (KATA) и Kaspersky EDR способны сократить время обнаружения и реагирования за счет автоматизации действий и унификации до 50-60%.

Платформа KATA с Kaspersky EDR позволяет обеспечить максимальный уровень автоматизации операций и унификации процессов по обнаружению, расследованию и реагированию на инциденты и наглядного представления информации. Это позволяет ИБ-специалистам выполнять ежедневные задачи более эффективно, не тратя времени на ручную работу, которая может быть автоматизирована.

Затраты на разрешение одного инцидента с автоматизацией = **Затраты на разрешение одного инцидента без автоматизации** × (100% − **Прогнозируемая экономия от автоматизации, %**)

Показатель эффективности платформы KATA и Kaspersky EDR

$$\text{Показатель эффективности платформы KATA и Kaspersky EDR} = \left[1 - \frac{\text{Затраты на разрешение одного инцидента с автоматизацией} \times N + \text{Затраты на платформу KATA и Kaspersky EDR}}{\text{Затраты на разрешение одного инцидента без автоматизации} \times N} \right] \times 100\%$$

N — прогнозируемое количество инцидентов в год

Минкомсвязь России

Реестр российского ПО

«Лаборатория Касперского» является отечественным разработчиком средств информационной безопасности и ее решения внесены в единый реестр российского ПО.

Источник: reestr.minsvyaz.ru

Сертификат ФСТЭК России

Платформа Kaspersky Anti Targeted Attack имеет сертификат ФСТЭК России, который удостоверяет, что решение является программным средством автоматизированного анализа защищенности и обнаружения уязвимостей автоматизированных систем и средств вычислительной техники, обрабатывающих информацию, не содержащей сведений, составляющих государственную тайну, соответствует требованиям по безопасности информации, установленным в документе «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2018) - по 4 уровню доверия.

Сертификаты ФСБ России:

- Платформа Kaspersky Anti Targeted Attack имеет сертификат ФСБ России на соответствие требованиям к средствам обнаружения компьютерных атак класса В и может использоваться в автоматизированных информационных системах, обрабатывающих информацию, не содержащую сведений, составляющих государственную тайну.
- Платформа Kaspersky Anti Targeted Attack соответствует требованиям ФСБ России к антивирусным средствам класса Д и может использоваться для защиты информации, содержащей сведения, составляющие государственную тайну.

Требования регуляторов

Необходимость следования рекомендациям и требованиям действующего законодательства порождает вопрос — при чем здесь возврат инвестиций? Все просто – определенные требования регуляторов обязательны для выполнения, и им необходимо следовать во избежание проблем и возможных убытков, связанных с несоответствием таким требованиям.

Сегодня к требованиям законодательства можно отнести:

- **использование решения, присутствующего в реестре российского ПО и имеющего сертификаты ФСБ и ФСТЭК России;**
- **сбор и централизованное хранение данных, вердиктов и иной информации, связанной с произошедшими инцидентами, которые позволяют оказывать содействие специалистам ФСБ России, предоставляя им необходимую информацию об обнаруженных угрозах;**
- **обязательства по информированию об инцидентах;**
- **проверка инфраструктуры на наличие получаемых от регуляторов индикаторов компрометации и проведения оперативных мер по реагированию и пр.**

ЕДИНАЯ КОНЦЕПЦИЯ КИБЕРБЕЗОПАСНОСТИ

Соблюдение требований

Соблюдение норм действующего законодательства и выполнение обязательств по уведомлению о нарушениях и оперативному предоставлению необходимой информации о произошедших компьютерных инцидентах требуют от организаций четкого построения процессов по расследованию и реагированию на инциденты.

В идеале, организациям необходимо следовать актуальной тенденции слияния формальных требований с фактической IT-безопасностью. Это означает, что необходимо подбирать такие инструменты по защите от сложных угроз, которые в дополнение к своей основной функции должны учитывать специфику различных организаций и помогать обеспечивать соответствие нормативам внешних регулирующих органов, стандартам банковской отрасли, требованиям ЦБ РФ, требованиям к защите персональных данных при их обработке в информационных системах персональных данных (ИСПДн), PCI DSS, GDPR и, конечно же, требованиям законодательства по защите критической информационной инфраструктуры (КИИ) и пр.

Организации, на которые распространяются требования ФСБ и ФСТЭК в рамках 187-ФЗ уже в какой-то степени ознакомлены с ними и понимают меры ответственности за нарушения 187-ФЗ.

Субъекты КИИ с незначимыми/значимыми объектами КИИ обязаны незамедлительно информировать ФСБ о компьютерных инцидентах, в том числе и ЦБ РФ, если организация также относится к финансовой сфере, и оказывать содействие должностным лицам ФСБ в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов.

Платформа **Kaspersky Anti Targeted Attack и Kaspersky EDR** помогают организациям соответствовать действующему законодательству в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов, предоставляя данные об инцидентах оперативно и в полном объеме.

Платформа **Kaspersky Anti Targeted Attack и Kaspersky EDR** формирует полную картину инцидента, автоматизирует процесс сбора данных и обеспечивает их централизованную запись и хранение для эффективного расследования многоступенчатых атак, в том числе при недоступности скомпрометированных рабочих мест или в случаях, когда данные были зашифрованы в ходе атаки.

Также субъекты КИИ с значимыми объектами КИИ обязаны соблюдать требования ФСТЭК по обеспечению их безопасности, выполнять предписания должностных лиц ФСТЭК об устранении нарушений в части соблюдения требований к обеспечению безопасности значимого объекта КИИ. А также реагировать на компьютерные инциденты в порядке, утвержденном ФСБ, принимать меры по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ.

Субъекты КИИ должны соблюдать требования по обеспечению безопасности значимых объектов КИИ РФ. А это означает, что должны применяться соответствующие технологии для выстраивания этой защиты.

Большая часть мер обеспечения безопасности значимых объектов покрывается решениями «Лаборатории Касперского», в том числе платформой Kaspersky Anti Targeted Attack и Kaspersky EDR, которые взаимодействуют между собой на глубоком уровне, что исключает интеграционные проблемы и необходимость, например, разворачивания нескольких агентов для защиты рабочих мест и серверов и т. п.

О Kaspersky EDR и платформе Kaspersky Anti Targeted Attack

Корпоративные рабочие места, где тесно взаимосвязаны данные, пользователи и корпоративные системы — важнейшая часть сети с позиций бизнеса, а также с точки зрения IT-безопасности.

При проведении комплексных кибератак рабочие места остаются основной мишенью злоумышленников. Чтобы защитить их и не дать злоумышленникам использовать конечные устройства для проникновения в инфраструктуру, необходимо усилить существующую систему безопасности. Полный цикл защиты рабочих мест, от автоматического блокирования угроз до быстрого реагирования на сложные инциденты, предполагает использование превентивных технологий наряду с расширенными возможностями защиты.

Передовая линия обороны — начиная с рабочих мест

Kaspersky EDR обеспечивает полный обзор всех рабочих мест в корпоративной сети и визуализацию каждой стадии расследования, предоставляет эффективное обнаружение угроз и мощный инструмент анализа первопричин. Процесс расследования подкрепляется ретроспективным анализом, а обнаружения сопоставляются с базой знаний MITRE ATT&CK. Это позволяет эффективно идентифицировать тактики и техники злоумышленников. Кроме того, продукт обеспечивает проактивный поиск угроз и доступ к порталу Kaspersky Threat Intelligence. С помощью этих инструментов эксперты смогут воссоздать всю последовательность действий злоумышленников, обнаружить самые изощренные атаки и быстро принять эффективные контрмеры.

Централизованное управление инцидентами в рамках всей инфраструктуры рабочих мест и поддержка широкого спектра действий по реагированию из единой веб-консоли позволяют компаниям обеспечить непрерывность рабочих процессов. Быстрое и точное сдерживание угроз и устранение инцидентов в распределенных инфраструктурах предоставляется благодаря централизации автоматизированных процессов, которые оптимизируют работу ИБ-отдела. При этом не нужны дополнительные ресурсы, исключаются простои, а производительность не снижается.

Переход на комплексную стратегию защиты

Почему организациям необходимо защищать при помощи передовых инструментов не только рабочие места, но и сеть, применять наиболее продвинутые детектирующие технологии и иметь полную картину происходящего в инфраструктуре? Как уже отмечалось, целевые атаки управляются и контролируются высококвалифицированными профессиональными киберпреступниками, которые нацелены на заражение максимального числа значимых элементов инфраструктуры организации и часто комбинируют множество различных приемов в рамках одной спланированной атаки.

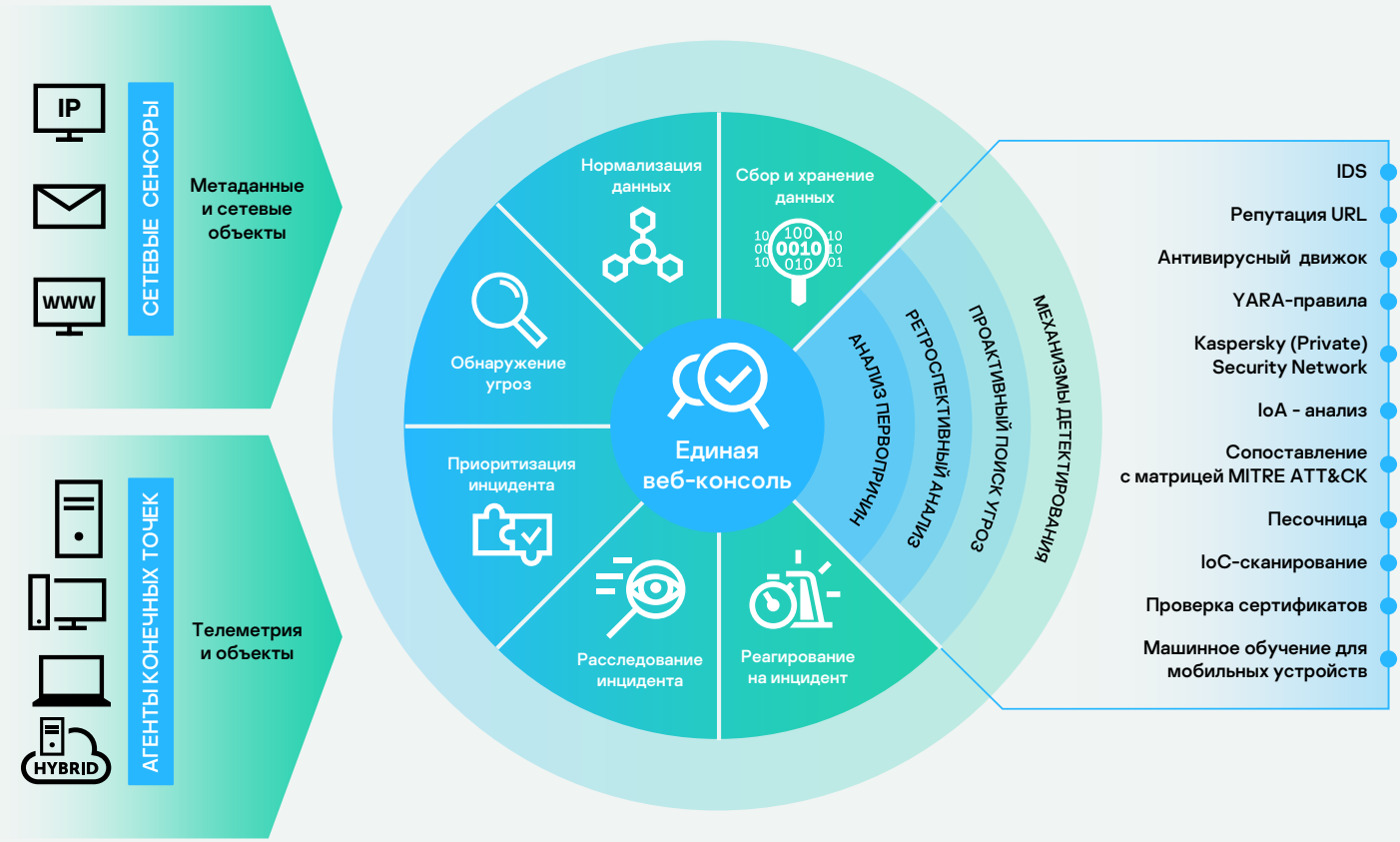
Платформа Kaspersky Anti Targeted Attack, усиленная возможностями Kaspersky EDR, обеспечивает передовую защиту от комплексных угроз и целевых атак в едином решении. Это решение полностью интегрировано с Kaspersky Security для бизнеса, а также с Kaspersky Security для почтовых серверов и Kaspersky Security для интернет-шлюзов для автоматического ответа на сложные угрозы на уровне сети. Полная визуализация данных, возможность проведения глубинного анализа сетевого трафика, эмуляция угроз при помощи продвинутой песочницы и мощные технологии EDR – все это делает расследование и реагирование на инциденты более быстрыми, точными и эффективными.

Совместимость

Kaspersky EDR может входить в состав платформы Kaspersky Anti Targeted Attack, благодаря чему возможности EDR совмещаются с функциями обнаружения продвинутых угроз на уровне сети.

Платформа Kaspersky Anti Targeted Attack объединяет возможности передового обнаружения на уровне сети и технологии EDR – Kaspersky EDR.

Специалисты по IT-безопасности получают в едином решении все инструменты, которые позволят выявлять угрозы на всех уровнях развития целевой атаки, проводить анализ первопричин и проактивный поиск угроз, а также оперативно и централизованно реагировать на сложные инциденты, позволяя значительно сократить количество времени и сил, которые сотрудникам службы ИБ приходится тратить на защиту от угроз повышенной сложности.



Анализ сетевого трафика

Мониторинг активности конечных точек

Централизованное хранилище данных и вердиктов

Глобальная аналитика угроз

Платформа KATA с Kaspersky EDR позволяют:

- сократить прямые потери от целенаправленных действий злоумышленников
- повысить продуктивность и качество работы сотрудников служб ИТ и ИБ
- сократить трудозатраты высококвалифицированных кадров
- обеспечить помощь в соответствии требованиям внутренних политик безопасности и внешних регулирующих органов
- сократить количество рутинных ручных операций при противодействии сложным угрозам
- снизить риски информационной безопасности

Международное признание

Оценка аналитических агентств

«Лаборатория Касперского» стала победителем **Gartner Peer Insights Customers' Choice** в категории EDR-решения, 2020 год.

Исследовательская компания Radicati Group назвала «Лабораторию Касперского» **ведущим игроком в отчете "Advanced Persistent Threat (APT) Protection – Market Quadrant, 2020".**

По результатам исследования 2020 SPARK Matrix от Quadrant Knowledge Solutions решение **Kaspersky EDR было признано технологическим лидером на рынке EDR-решений.**

Независимые тесты

В независимом тесте ICSA Labs: Advanced Threat Defense (3 квартал 2019 года) платформа Kaspersky Anti Targeted Attack показала **100% результат обнаружения угроз, не допустив ни одного ложного срабатывания.**

SE Labs протестировала эффективность платформы Kaspersky Anti Targeted Attack против широкого спектра кибератак и **присвоила решению рейтинг AAA.**

Качество обнаружения подтверждено оценкой MITRE ATT&CK

Решение Kaspersky EDR прошло тестирование MITRE ATT&CK (Раунд 2), показав высокую эффективность обнаружения ключевых техник, применяемых на основных этапах проведения современных целевых атак.

Подробнее: kaspersky.com/MITRE

Заключение

Все чаще руководители участвуют в процессе принятия решений, связанных с информационной безопасностью. Это влечет за собой рост соответствующих бюджетов и повышение уровня готовности компании к управлению инцидентами. Таким образом, в организациях любых размеров крайне важно добиться заинтересованности высшего руководства.

По данным нашего последнего исследования, доля бюджетов, выделяемых на информационную безопасность, практически не изменилась в сравнении с прошлым годом. Возможно, организации пока не торопятся с инвестициями в ИБ, обдумывая свои дальнейшие шаги. Но учитывая то, что риск стать жертвой атаки непрерывно растет, компаниям любых размеров стоит более тщательно выверять, все ли необходимые расходы были учтены при планировании бюджета на информационную безопасность, чтобы подготовиться к следующему поколению киберинцидентов. Инвестиции и регулярный пересмотр процессов, связанных с информационной безопасностью, необходимы, чтобы опережать растущую частоту кибератак и свести к минимуму возможные финансовые потери.

Kaspersky
Anti Targeted
Attack

Узнать больше

Kaspersky
Endpoint Detection
and Response

Узнать больше

www.kaspersky.ru