Ценность Kaspersky Symphony для бизнеса

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Введение

Данный документ поясняет актуальность построения процессов по выявлению сложных кибератак, а также отвечает на ряд вопросов:

- В чём ценность решений класса XDR для бизнеса?
- Как аргументировать выделение бюджета на Kaspersky Symphony XDR?
- Какие преимущества от внедрения Kaspersky Symphony XDR получит организация?

Сегодня успех деятельности любой компании напрямую зависит от надежной защиты ее активов, стабильности бизнес-процессов и безопасности ИТ-инфраструктуры, 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 участников профессионального сообщества ИТ-директоров GlobalCIO | DigitalExperts «Актуальные подходы к обеспечению кибербезопасности», ключевыми факторами для выделения бюджета на ИБ-решения являются: необходимость соблюдения требований регуляторов, усложнение ландшафта угроз, расширение и усложнение существующей IT-инфраструктуры, которая требует защиты.

Ключевые факторы для выделения бюджета на ИБ

22%

Необходимость соответствия требованиям регуляторов

22%

Усложнение ландшафта угроз

21%

Расширение и усложнение существующей IT-инфраструктуры

13%

Желание высшего руководства усилить существующую защиту

10%

Факт случившегося индицента с ощутимым уроном

9% / **2%**

Необходимость повышения автоматизации и высвобождения ИБ-ресурсов / Другое

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.

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** — их деятельность направлена в первую очередь на получение финансовой выгоды. Проводят как массовые, так и целевые атаки с применением самых разных методов для достижения своей цели: от технических и программных средств, утилит и ПО до социальной инженерии.
- **Конкурирующие компании** — похищают конфиденциальные данные или даже пытаются совершить саботаж. Обычно используют услуги наемных исполнителей. Эти исполнители специализируются на кибершпионаже, разрабатывают собственные инструменты и продают свои услуги тому, кто больше заплатит.
- **Хактивисты** — нацелены на достижение политической, социальной или религиозной справедливости (в их понимании). Заявляют о своих благих целях, изобретательны, используют сложный инструментарий и представляют серьезную проблему для любой организации, привлекшей их внимание.
- **Государственные органы** — государственные 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.

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.

Растущая угроза

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 их ценность для бизнеса?

Основным камнем преткновения при защите бюджета ИБ-департамента для формирования защиты от современных киберугроз становятся инвестиции в построение защиты от потенциальных инцидентов. Наиболее популярный аргумент тех, кто принимает решение: такие атаки могут не произойти, а деньги будут потрачены.

Организации редко проецируют на себя инциденты, затронувшие другие компании, и склонны считать, что комплексные угрозы и связанные с ними 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 измеримых результатов от внедряемых систем и хотят видеть реальные факты, указывающие на необходимость инвестирования.

3 основных подхода для обоснования инвестиций:

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

1 Анализ рисков

Возможные последствия для ключевых отраслей

Финансовые структуры

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

Государственные услуги

- манипуляции с 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
- манипуляции с веб-ресурсами для использования в фишинговых атаках
- использование скомпрометированной инфраструктуры (устройств/интернета вещей) при DDoS-атаках

Энергоснабжение и коммунальные услуги

- манипуляции с 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.

Последствия целевой атаки для организации

- Компрометация данных
- Кража денежных средств
- Утрата критически важных данных
- Ухудшение репутации
- Кража коммерческой тайны
- Потеря конкурентного преимущества
- Повреждение ИТ-инфраструктуры
- Утрата доверия клиентов
- Прерывание основных бизнес-процессов
- Уменьшение занимаемой доли на рынке
- Недоступность сервисов для пользователей
- 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 понимание возможных последствий столкновения с целевыми атаками, напротив, повышается. Почему так происходит? К сожалению, основным обоснованием выделения бюджета на усиление существующей защиты зачастую остается факт уже случившегося инцидента с ощутимым ущербом, который вполне можно измерить.

Что происходит, когда компанию атакуют?

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 2021 году IT Security Economics, в 2021 году компании в России теряли больше всего денег в результате целевых атак.

Один такой киберинцидент наносил крупному бизнесу ущерб в среднем в размере 695 тысяч долларов США. С таргетированными атаками (когда злоумышленники целенаправленно атакуют конкретную компанию: проводят разведку и подбирают инструменты для нападения, исходя из характеристик жертвы) в 2021 году столкнулись 35% организаций в России. Компании также теряли деньги вследствие других видов киберинцидентов. В числе наиболее дорогостоящих для крупного бизнеса — электронные утечки данных из внутренних систем, утечки, вызванные атаками вредоносного ПО и несоблюдением внутренних политик информационной безопасности.

Самый большой ущерб от киберинцидентов в 2021 году для российского бизнеса был связан с целевыми атаками.

Средняя сумма расходов крупной компании в России в результате целевой атаки

$ 695 000

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.

Стоимость минимизации риска

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 некоторое представление.

Формула расчета окупаемости инвестиций в ИБ (ROI):

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

Рассчитайте окупаемость инвестиций

Используя эту формулу и представленные усредненные значения убытков в результате одного инцидента, можно произвести необходимый расчет.

Большая часть затрат на защиту – это стоимость лицензий и требуемого оборудования, расходы на персонал и стоимость технической поддержки.

Материальный ущерб – это убытки от одного инцидента, умноженные на количество инцидентов, например, за год.

Не стоит забывать, что ценность, которую обеспечивают решения класса XDR (Extended Detection and Response), например Kaspersky Symphony XDR, 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 Kaspersky Symphony XDR, 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.

2

Анализ временных затрат

Факторы снижения стоимости утечки данных

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

В ходе опроса «Лаборатории Касперского» в 2021 году IT Security Economics было выявлено несколько факторов, которые могут помочь предприятиям снизить стоимость утечки данных:

Быстрое обнаружение атак, направленных на организацию

Потери меньше на 32%

Финансовые потери были на 32% меньше 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 финансовый ущерб на 28% меньше, 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%

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

Время является одним из самых дефицитных ресурсов при расследовании инцидентов и реагировании на инциденты: быстро принятые сотрудниками ИБ меры противодействия уменьшают шансы атакующих достичь цели.

Рассмотрим 2 важных временных критерия:

а Время обнаружения

б Время реагирования

Время обнаружения

По данным аналитического отчета «Лаборатории Касперского» за 2021 год «Реагирование на компьютерные инциденты», время обнаружения первых признаков зависит от типа атаки в зависимости от ее длительности:

1

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.

2

Атаки средней длительности

Атаки длительностью несколько дней

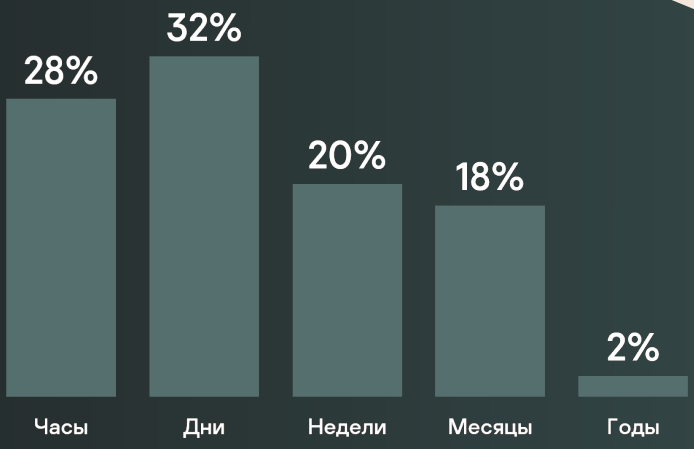
В подавляющем большинстве случаев эти атаки направлены непосредственно на хищение денежных средств. Как правило, злоумышленники добиваются поставленной цели в течение недели.

3

Длительные атаки

Атаки длительностью более нескольких недель

Данная активность почти всегда направлена на хищение 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 происходит в случае быстроразвивающихся атак, таких как как шифровальщики, с очевидными последствиями.

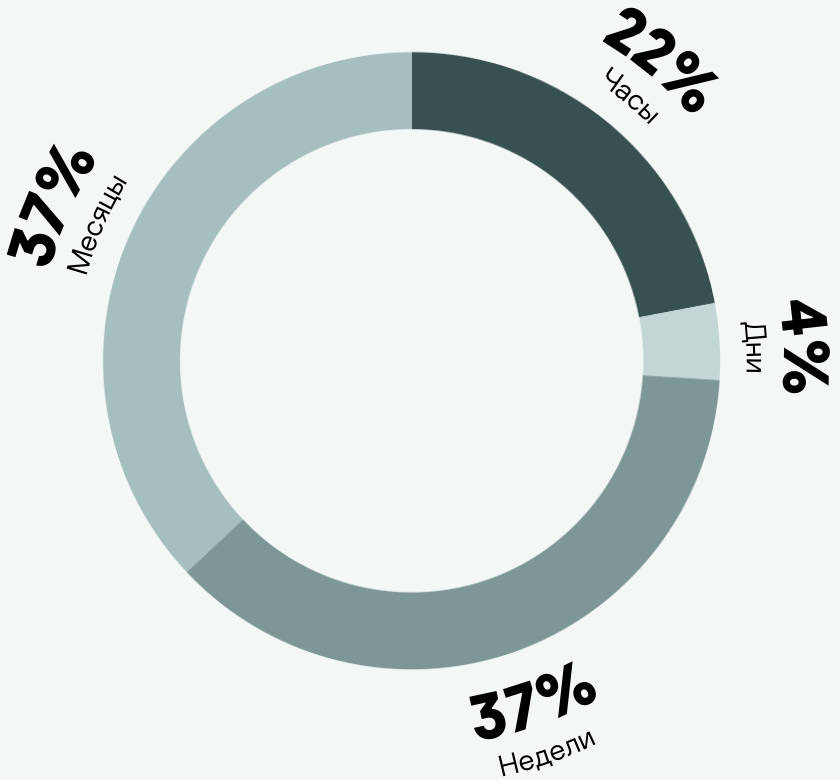
По данным отчета «Лаборатории Касперского», обнаружение атак без явных разрушительных признаков, средних по продолжительности и длительных, обычно занимает от нескольких дней до нескольких месяцев.

6

Время реагирования

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 России и стран СНГ, Европы и Азии, Южной и Северной Америки, Ближнего Востока и Африки.

Согласно данным отчета «Лаборатории Касперского» за 2021 год «Реагирование на компьютерные инциденты» продолжительность реагирования на атаку чаще всего варьировалась от нескольких недель до нескольких месяцев. Она в том числе определялась глубиной фактического проникновения злоумышленников в скомпрометированную сеть и количеством времени, прошедшего с момента первоначального взлома.



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.

Очевидно, что организации должны стремиться сократить время на обнаружение и реагирование, что должно привести к уменьшению риска успешной атаки, а также уменьшить 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 IT Security Economics в 2021 году, ключевым препятствием на пути противодействия сложным инцидентам остается: отсутствие квалифицированного технического персонала для реагирования на сложные киберинциденты

Дефицит кадров в сфере информационной безопасности усугубляется недостатком актуальных знаний у аналитиков в области 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
- Затронутые в ходе атаки системы
- Временные рамки атаки
- Вредоносные программы и инструменты, которые были использованы в процессе атаки
- Завершена атака или нет, то есть достиг ли атакующий своей цели

Такая работа требует высококлассных нишевых специалистов с обширными знаниями, чутьем и опытом в области анализа вредоносного ПО, цифровой криминалистики, взаимодействия с глобальными данными об угрозах и реагирования на инциденты. Специалисты должны уметь правильно интерпретировать данные, получаемые от средств защиты, видеть и извлекать 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 оценку информации и принятие критически важных решений: нужно ли продолжать расследование 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.

Использование сразу нескольких инструментов в работе также сопряжено с увеличением количества ручных операций и ожидаемо приводит к неэффективному использованию, перегрузке ИБ-служб и 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 действительно сложного инцидента и организации мер противодействия.

Рассчитайте затраты на разрешение инцидентов

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

XDR

Kaspersky Symphony

Использование ИБ-службой специализированного XDR-решения Kaspersky Symphony XDR — с 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.

Формулы расчета времени, которое понадобится аналитикам для разрешения одного инцидента (без средств автоматизации):

1. 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**

2. 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. Составляющие расхода на одного аналитика:

- 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

Стоимость нормо-часа аналитика = **Затраты на аналитика в год**

52 недели × 5 рабочих дней × 8 часов

Расчет времени, необходимого аналитикам на разрешение одного инцидента с помощью дополнительного инструментария (с автоматизацией)

По данным статистики ведущих аналитических агентств и нашего опыта, решения по комплексному противодействию сложным угрозам, такие как Kaspersky Symphony XDR, способны сократить время обнаружения и реагирования за счет автоматизации действий и унификации до 50-60%.

Kaspersky Symphony XDR 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.

50-60%

Прогнозируемая экономия от автоматизации

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

Показатель эффективности Kaspersky Symphony XDR

$$1 - \frac{\text{Затраты на разрешение одного инцидента с автоматизацией} \times N + \text{Затраты на Kaspersky Symphony XDR}}{\text{Затраты на разрешение одного инцидента без автоматизации} \times N} \times 100\%$$

N — прогнозируемое количество инцидентов в год

3

Требования регуляторов

Минкомсвязь России

Реестр российского ПО

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

Сертификаты ФСБ и ФСТЭК России

«Лаборатория Касперского» прошла сертификацию в ФСТЭК и ФСБ России

Соответствие

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 российского законодательства относится:

- Использование решения, присутствующего в реестре российского ПО и имеющего сертификаты ФСБ и ФСТЭК России
- Проверка инфраструктуры на наличие получаемых от регуляторов индикаторов компрометации, проведение оперативных мер по реагированию и пр.
- Сбор и централизованное хранение данных, вердиктов и иной информации, связанной с произошедшими инцидентами, которые позволяют оказывать содействие специалистам ФСБ, предоставляя им необходимую информацию об обнаруженных угрозах
- Обязательства по информированию об инцидентах через передачу информации о кибератаках на КИИ в ГосСОПКА (Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак)

Единая концепция кибербезопасности

Корпоративная IT-безопасность

ФСТЭК ФСБ

ЦБ РФ СТО БР ИББС

GDPR PCI DSS

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.

Актуальные тенденции

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, требованиям законодательства по защите критической информационной инфраструктуры (КИИ).

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 о компьютерных инцидентах ФСБ РФ, а также ЦБ РФ, если организация 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.

Также субъекты КИИ со значимыми объектами КИИ обязаны соблюдать требования ФСТЭК по обеспечению их безопасности, выполнять предписания должностных лиц ФСТЭК об устранении нарушений в области 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 Kaspersky Symphony XDR, 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.

Решение «Лаборатории Касперского»

Kaspersky Symphony XDR помогает организациям соответствовать действующему законодательству в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов. Благодаря встроенному модулю ГосСОПКА решение полностью интегрировано с технической инфраструктурой НКЦКИ.

Платформа Kaspersky Symphony XDR формирует полную картину инцидента, автоматизирует процесс сбора данных и обеспечивает их централизованную запись и хранение для эффективного расследования многоступенчатых атак, в том числе в случае недоступности скомпрометированных рабочих мест или в случае, когда данные были зашифрованы в ходе атаки.

Всё в одном

Всесторонняя защита
с соблюдением требований
законодательства

О Kaspersky Symphony XDR

От безупречной защиты рабочих мест – к единой всеобъемлющей безопасности

Kaspersky Symphony XDR - это решение класс Extended Detection and Response (XDR), которое обеспечивает надежную защиту от кибератак и помогает соответствовать требованиям законодательства, в том числе благодаря встроенному модулю ГосСОПКА. В состав решения входит передовая защита рабочих мест, серверов, виртуальных машин, сетевого и почтового трафика, а также платформа, которая позволяет повысить киберграмотность сотрудников. Все элементы платформы взаимосвязаны между собой, дополняют друга и входят в одну лицензию.

Это комплексное решение помогает ИБ-службам отражать продвинутые кибератаки на всех уровнях значительно быстрее и с меньшими усилиями благодаря оптимально настроенной автоматизации защитных действий, кросс-продуктовому взаимодействию, использованию достоверной аналитики о киберугрозах и многоуровневому контролю потенциальных точек входа злоумышленников.

Сильные стороны Kaspersky Symphony XDR

Фундаментальная защита

Включена технология EDR в синергии с EPP, которая защищает более 60 миллионов корпоративных рабочих мест по всему миру

Аналитика

Включена признанная лучшей в мире аналитика об угрозах по результатам Forrester Wave: External Threat Intelligence Services 2021

Киберграмотность

Включена платформа, которая повышает киберграмотность рядовых сотрудников

Взаимодействие

Тесное взаимодействие включенных элементов, кросс-продуктовые сценарии и четкие планы по наращиваю функциональности.

Гибкость

Гибкость сетевой защиты: Netflow, анализ сетевого трафика, загрузка IDS&APT-фидов в сторонние инструменты. Интеграция с различными ИБ-решениями сторонних поставщиков

Соответствие требованиям

Решение помогает обеспечить соответствие требованиям регуляторов (например, в сфере безопасности объектов КИИ), в том числе благодаря встроенному модулю ГосСОПКА

Расширенные возможности защиты

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, значительно сокращая количество времени и сил, которые сотрудникам службы ИБ приходится тратить на защиту от угроз повышенной сложности.

- Включена функциональность платформы Threat Intelligence и потоки данных об угрозах
- Включено повышение осведомленности сотрудников
- Включен модуль ГосСОПКА для автоматического взаимодействия с НКЦКИ

Kaspersky Symphony XDR позволяет:

- Снизить риски информационной безопасности
- Повысить продуктивность и качество работы сотрудников служб ИТ и ИБ
- Сократить трудозатраты высококвалифицированных кадров
- Обеспечить помощь в соответствии с требованиями внутренних политик безопасности и внешних регулирующих органов
- Сократить количество рутинных ручных операций при противодействии сложным угрозам
- Сократить прямые потери от целенаправленных действий злоумышленников

«Лаборатория Касперского» активно участвует в независимых тестированиях и взаимодействует с ведущими аналитическими агентствами. Наши технологии и продукты признаны во всем мире и удостоены многочисленных международных наград.

Международное признание

MITRE | ATT&CK®

Качество обнаружения подтверждено оценкой MITRE ATT&CK. «Лаборатория Касперского» показала высокую эффективность обнаружения ключевых техник, применяемых на основных этапах проведения современных целевых атак

Gartner peerinsights customers' choice 2020™

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

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

Исследовательская компания Radicati Group назвала «Лабораторию Касперского» ведущим игроком в отчете Advanced Persistent Threat (APT) Protection – Market Quadrant, 2021

FORRESTER®

«Лаборатория Касперского» признана лидером по результатам исследования Forrester Wave: External Threat Intelligence Services (Внешние услуги по анализу угроз), 2021

SE Labs AAA December 2021 ADVANCED SECURITY (EDR)

«Лаборатория Касперского» получила в 2021 году высшую оценку AAA за EDR по итогам теста Enterprise Advanced Security от SE Labs

IDC

«Лаборатория Касперского» признана ключевым игроком в области защиты конечных устройств для бизнеса по версии IDC MarketScape

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE

В независимом тесте ICSA Labs: Advanced Threat Defense «Лаборатория Касперского» показала 100%-ное обнаружение угроз, не допустив ни одного ложного срабатывания

Инвестируйте в безопасное будущее

Инвестиции и регулярная переоценка процессов, связанных с информационной безопасностью, необходимы, чтобы опережать все более частые кибератаки и свести к минимуму возможные финансовые потери.

Заключение

Всё чаще руководители участвуют в процессе принятия решений, связанных с информационной безопасностью. Это способствует выделению большего количества денег на IT-безопасность и повышению 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 по сравнению 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 было учтено при планировании бюджета на информационную безопасность, чтобы подготовиться к следующему поколению киберинцидентов.

www.kaspersky.ru