Ценность Kaspersky Symphony для бизнеса

kaspersky активируй будущее

Введение

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). Напряженность цифрового ландшафта, а также усложнение требования законодательства требуют от организаций внедрения эффективной стратегии защиты от комплексных угроз и целевых атак и учета требований регуляторов.

Современные реалии ИБ

Было

Усложняется ландшафт угроз

Киберпреступники совершенствуют свои методы, применяют технологии ИИ, организация и проведение кибератак становится отдельной индустрией с развитым разделением труда

Расширяется поверхность атак и точек входа для злоумышленников

Развитие и внедрение новых технологий в бизнес-процессы, а также масштабное изменение цепочек поставок несут новые специфические киберриски

Усиливаются требования регуляторов

Особенно в отношении обеспечения защиты КИИ и персональных данных

+ Добавилось

Наступила эра хактивизма и целевой кибераграссии

Кибератаки на российские компании стали агрессивнее, размывается их мотивация, готовые инструменты для проведения кибератак становятся доступнее

Больше уязвимостей

Из-за полного ухода ряда ИБ-вендоров или приостановки обновлений их решений компании вынуждены срочно искать им замену и корректировать стратегию ИБ

Активная фаза импортонезависимости

Полным ходом идет замещение иностранных технологий. Есть ниши, в которых отечественные решения появились относительно недавно

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

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

Ключевые факторы для выделения бюджета на ИБ

- Усложнение ландшафта угроз
- Необходимость соответствия требованиям регуляторов
- Расширение, усложнение, трансформация существующей ИТ-инфраструктуры
- Необходимость повышения автоматизации процессов, высвобождения ресурсов ИБ-специалистов
- Факт случившегося киберинцидента

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.

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

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.

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 инструменто
- 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 обоснования инвестиций:

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

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

Анализ рисков

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
- Ухудшение репутации
- Утрата критически важных данных
- Кража денежных средств
- 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 различным оценкам, средние потери одной российской организаций от киберугроз могут составлять более $ 200000 в год. Для крупных компаний потери только от одной пропущенной целевой атаки могут превышать эту цифру, а верхняя планка не ограничена и доподлинно неизвестна, так как далеко не все инциденты становятся публичными.

В последние несколько лет доля критичных киберинцидентов — атака с участием человека или вирусных заражений, оказывающих серьезное воздействие на бизнес — в среднем составляет почти 10% от всех фиксируемых кибератак ежегодно. При этом процент целевых атак среди критичных инцидентов всех типов составил почти четверть (24,7%)[1].

Также, согласно аналитическому отчету Kaspersky Incident Response за 2023 год, главными проблемами для бизнеса, связанными с кибератаками, стали программы-вымогатели (Ransomware) и утечки данных.

Успешная атака с применением программ-вымогателей при определенных обстоятельствах способна остановить производственные и/или бизнес-процессы, нанести непоправимый ущерб ИТ-инфраструктуре, привести к потере критических данных. Каждое из этих возможных последствий приводит к необходимости выделения ресурсов на устранение и восстановление инфраструктуры, а также несет в себе потенциальную упущенную выгоду, например, от простоя бизнеса, штрафы, репутационные потери.

Последние два пункта особенно актуально для участившихся в последние годы случаев крупных утечек данных.

Общие сведения о значимых[2] утечках данных в российских компаниях в 2023 году[3]

133
факта утечек данных за 2023 год

2022 год	2023 год
141 факт утечек данных	**133** факта утечек данных
> 230 млн пользовательских данных	**> 310 млн** пользовательских данных
> 33 млн записей с паролями	**> 47 млн** записей с паролями

[1] Аналитический отчет Managed Detection and Response за 2023 год

[2] Значимая утечка данных — утечка данных, в результате которой было скомпрометировано более 5000 строк пользовательских данных или которая получила резонанс в СМИ

[3] С января по октябрь 2023 года

Помимо репутационных потерь ужесточаются и регуляторные требования к защите персональных данных.

30 мая 2025 года вступает в силу закон от 30.11.2024 г. 420-ФЗ, который вносит поправки в КоАП РФ, ужесточающие ответственность для операторов персональных данных.

Ответственность за нарушения в области защиты ПДн после вступления в силу 420-ФЗ 30 мая 2025 года

Невыполнение или несвоевременное выполнение оператором обязанности по уведомлению Роскомнадзора о случаях установления факта утечки ПДн Ст. 13.11 (ч. 11)	Должностные лица: штраф **400–800 тыс. ₽** Юрлица: штраф **1–3 млн ₽**
Утечка субъектов ПДн и/или уникальных идентификаторов Ст. 13.11 (ч. 12)	Должностные лица: штраф **200–600 тыс. ₽** Юрлица : штраф **3–15 млн ₽** (в зависимости от объема утечки)
Повторная утечка ПДн Ст. 13.11 (ч. 15)	Должностные лица: штраф **800 тыс.–1,2 млн ₽** Юрлица: **оборотный штраф** — от 1 до 3% от выручки за предшествующий календарный год, но **не менее 20 млн** и **не более 500 млн ₽**
Утечка информации, содержащей специальные категории персональных данных и/или биометрические данные, в случае если ранее были административные наказания за утечки ПДн разного рода Ст. 13.11 (ч. 18)	Должностные лица: штраф **1–2 млн ₽** Юрлица : **оборотный штраф** — от 1% до 3% от выручки за предшествующий календарный год, но **не менее 25 млн** и **не более 500 млн ₽**

Регуляторный хаб знаний в области кибербезопасности

Подробная информация о регулировании вопросов ИБ по отраслям и подбор решений для обеспечения соответствия

Подробнее

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

Анализ временных затрат

Факторы снижения стоимости инцидента

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

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.

Один из ключевых показателей эффективности зрелой ИБ-системы — продолжительность инцидента. Он представляет из себя сумму двух критериев:

1

Время обнаружения

Mean Time to Detect (MTTD)

Среднее время, необходимое организации для обнаружения нарушения безопасности или угрозы

2

Время реагирования

Mean Time to Respond (MTTR)

Среднее время, необходимое на реакцию и устранение обнаруженной угрозы

Аналитики «Лаборатории Касперского» в отчете Incident Response за 2023 год, разделили наблюдаемые атаки на три категории по их длительности:

Атаки длительностью до недели

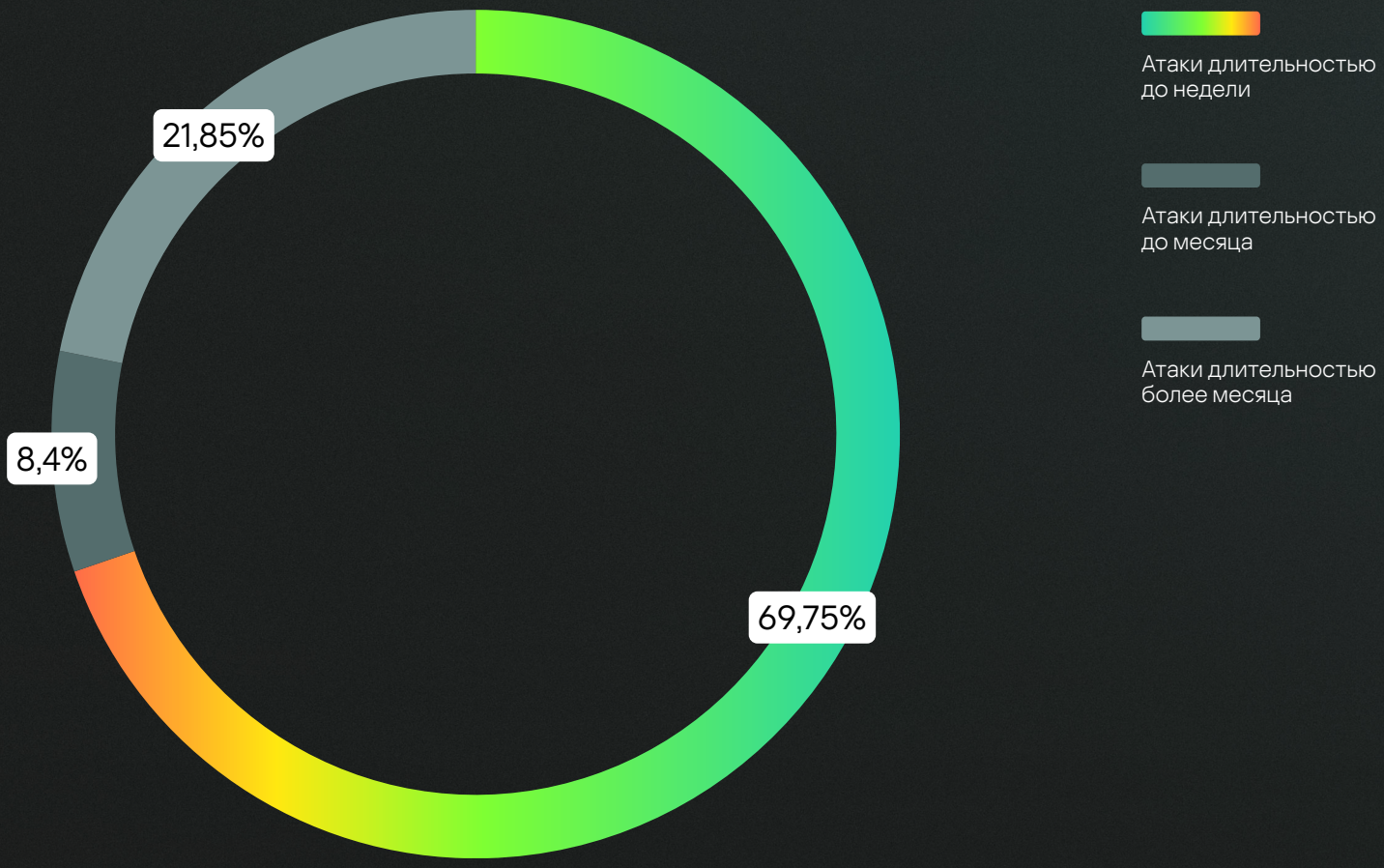
Масштабные быстрые атаки программ вымогателей на легкодоступные цели, представляющие большую проблему даже для организаций с развитой системой информационной безопасности. Такие инциденты связаны с общеизвестными и легко идентифицируемыми проблемами безопасности.

Атаки длительностью до месяца

Из-за использования программ вымогателей многие такие атаки неотличимы от более быстрых. Многие случаи, помещенные в эту группу, характеризуются значительным промежутком времени между первоначальным доступом и последующими этапами атаки.

Атаки длительностью более месяца

Сменяющие друг друга активные и пассивные фазы нерегулярной продолжительности. Длительность активных фаз примерно такая же, как в предыдущей группе (средняя).



Аналитический отчет «Incident Response за 2023 год»

Содержит информацию о кибератаках, расследованных 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

Ежегодный аналитический отчет Managed Detection and Response

Освещает результаты анализа инцидентов, выявленных командой Центра мониторинга и реагирования на инциденты (SOC1) «Лаборатории Касперского» в 2023 году

Скорость обнаружения киберугроз

Современные технологии помогают сократить скорость обнаружения киберугроз в среднем до 39 минут, согласно отчету Managed Detection and Response за 2023 год. Столько времени занимали все этапы обнаружения вплоть до реагирования у команды SOC «Лаборатории Касперского» в рамках предоставления сервиса «управляемой защиты» Kaspersky MDR.

Этот показатель может варьироваться в зависимости от сложности кибератак, технических возможностей ИБ-команды и наличия других ресурсов.

Среднее время реагирования

Среднее время реагирования на разные типы атак, согласно отчету Incident Response за 2023 год, составило от 40 до 46 часов.

Время реагирования также зависит от комплексности угрозы, количества точек входа, которые эксплуатировали злоумышленники, агрессии атаки. В последние годы заметно участились случаи инцидентов, в которых цель нападавших заключалась не в потенциальном получении финансовой выгоды, а в банальном уничтожении данных и причинения максимального ущерба инфраструктуре.

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

Сегодня ИБ-специалисты сталкиваются с необходимостью:

- Выполнения сложных задач в условиях нехватки квалифицированных кадров и экспертизы
- Ручного разбора и анализа большого числа инцидентов
- Эксплуатации средств ИБ, которые не взаимодействуют друг с другом и управляются из разных консолей
- Принятия решений без использования средств наглядного централизованного представления информации

Согласно глобальному опросу «Лаборатории Касперского», 41% современных компаний сталкиваются с дефицитом квалифицированных кадров в сфере ИБ. В первую очередь отмечается нехватка экспертов по угрозам информационной безопасности и аналитиков вредоносного ПО (по 39%), SOC-аналитиков (35%), специалистов по анализу защищенности и экспертов по сетевой безопасности (33%), а также TI-аналитиков (Threat Intelligence) — 32%

Человеческие ресурсы

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:

1. Начальный вектор атаки
2. Временные рамки атаки
3. Затронутые в ходе атаки системы
4. Размер ущерба, нанесенного атакой
5. Вредоносные программы и инструменты, которые были использованы в процессе атаки
6. Завершена атака или нет, то есть достиг ли атакующий своей цели

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

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.

Kaspersky Symphony XDR

Комплексное решение

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.

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

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 = 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 = Время на разрешение инцидента × Стоимость нормо-часа аналитика × Количество требуемых аналитиков

Минцифры 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

Основные решения «Лаборатории Касперского» имеют сертификаты ФСТЭК и ФСБ России

Безопасная разработка

«Лаборатория Касперского» первой в России прошла сертификацию процессов безопасной разработки и получила сертификат №1 в ФСТЭК России о соответствии процессов безопасной разработки программного обеспечения требованиям ГОСТ Р 56939. Сегодня требование соответствию ГОСТ Р 56939 уже включается во все проводимые заказчиками тендеры, оно прописано в документах всех значимых отраслей, таких как банковская сфера, КИИ, транспорт, медицина

Единая концепция кибербезопасности

Соответствие всем требованиям корпоративной ИТ-безопасности

- ФСБ
- ФСТЭК
- ЦБ РФ
- СТО БР ИББС
- GDPR
- PCI DSS

Требования регуляторов

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.

Ключевые аспекты современных законодательных требований

Только отечественные решения

Полный запрет для ряда организаций использования СЗИ и сервисов по информационной безопасности, происходящих из недружественных стран.

Указ Президента РФ от 01.05.2022 N 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

Сертифицированное ПО

Использование решений, присутствующих в Реестре российского ПО Минцифры РФ и имеющего сертификаты ФСБ и ФСТЭК России, в т.ч. в цепочке поставок.

Проверка инфраструктуры

на наличие получаемых от регуляторов (в т.ч. отраслевых) 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).

Защита персональных данных

Соблюдение требований по сбору, хранению ПДн, обращению с ними и их защите.

Актуальные тенденции

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, 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.

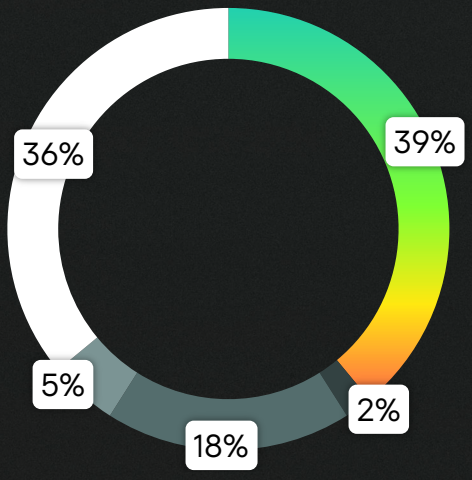
Субъекты КИИ с незначимыми/значимыми объектами КИИ обязаны незамедлительно информировать о компьютерных инцидентах ФСБ РФ, а также ЦБ РФ, если организация относится к финансовой сфере, и оказывать содействие должностным лицам ФСБ в обнаружении, предупреждении и ликвидации последствий компьютерных атак,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

Закрытие ключевых требований с помощью решений «Лаборатории Касперского»

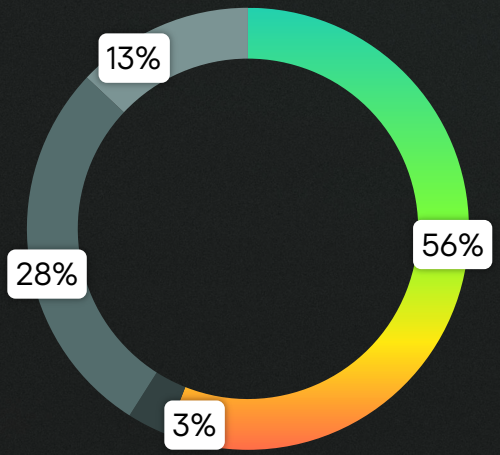
Меры защиты информации в информационных системах[1]

Процент закрытия требований решениями «Лаборатории Касперского»

С учетом организационных мер



Без учета организационных мер



Организационные меры, штатное ПО, резервирование

Kaspersky Symphony XDR (KES, KSC, KATA, KEDR, KUMA, KASAP, KSMG, KWTS)

Другие решения Kaspersky (DDoS Protection, Scan Engine, Тренинги)

Узконаправленные решения

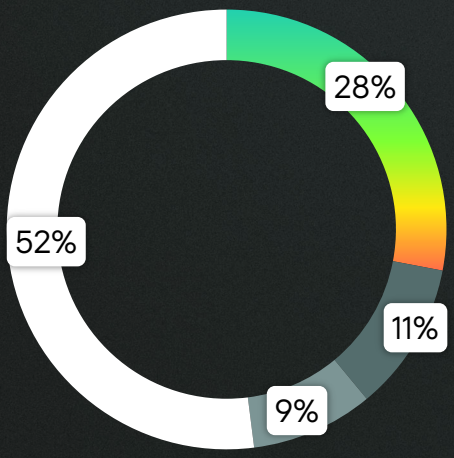
Межсетевые экраны

[1] В соответствии с Приказом ФСТЭК №17

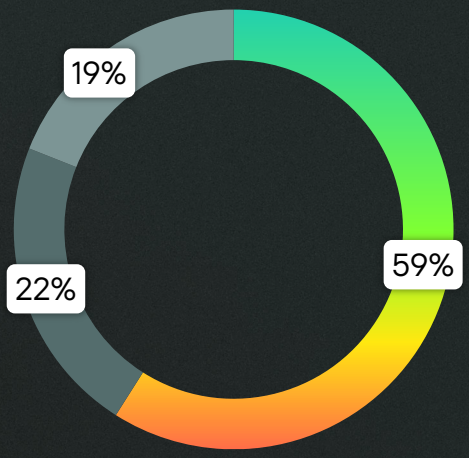
Меры защиты информации в автоматизированных системах управления[1]

Процент закрытия требований решениями «Лаборатории Касперского»

С учетом организационных мер



Без учета организационных мер



Организационные меры, штатное ПО, резервирование

Kaspersky Symphony XDR (KES, KSC, KATA, KEDR, KUMA, KASAP, KSMG, KWTS)

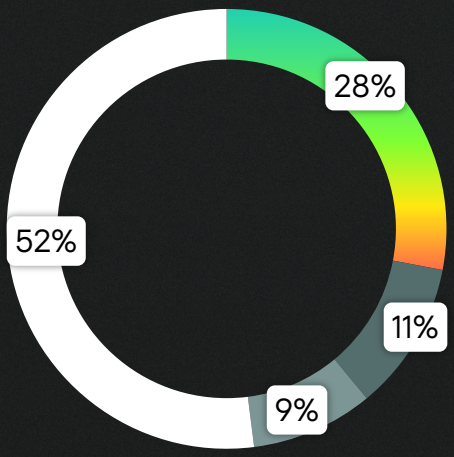
Узконаправленные решения

Межсетевые экраны

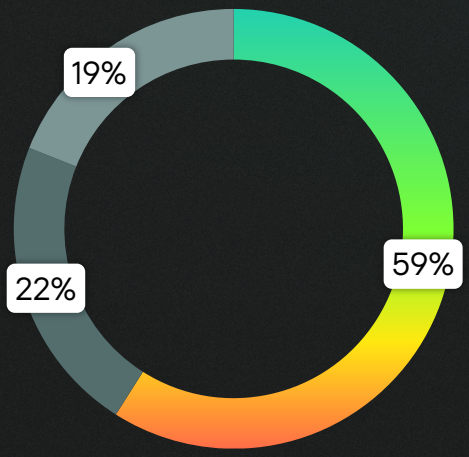
Меры защиты информации значимых объектов критической информационной инфраструктуры[2]

Процент закрытия требований решениями «Лаборатории Касперского»

С учетом организационных мер



Без учета организационных мер



Организационные меры, штатное ПО, резервирование

Kaspersky Symphony XDR (KES, KSC, KATA, KEDR, KUMA, KASAP, KSMG, KWTS)

Узконаправленные решения

Межсетевые экраны

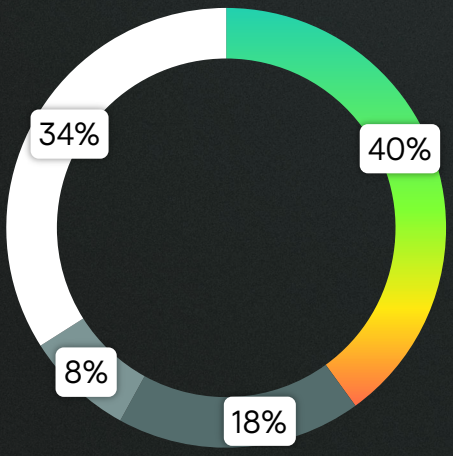
[1] В соответствии с Приказом ФСТЭК №31

[2] В соответствии с Приказом ФСТЭК №239

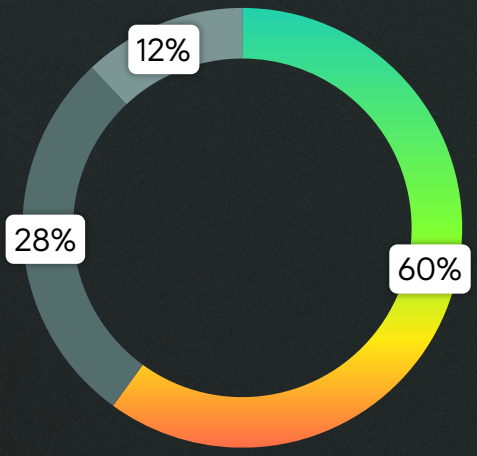
Меры по обеспечению безопасности персональных данных[1]

Процент закрытия требований решениями «Лаборатории Касперского»

С учетом организационных мер



Без учета организационных мер



Организационные меры, штатное ПО, резервирование

Kaspersky Symphony XDR (KES, KSC, KATA, KEDR, KUMA, KASAP, KSMG, KWTS)

Узконаправленные решения

Межсетевые экраны

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.

[1] В соответствии с Приказом ФСТЭК №21

Kaspersky Symphony XDR

Kaspersky Symphony XDR

Kaspersky Symphony XDR — решение класса XDR (eXtended Detection and Response) для всеобъемлющей кибербезопасности корпоративных ИТ-инфраструктур. С Kaspersky Symphony XDR специалисты по ИТ-безопасности получают в едином решении передовые инструменты и технологии, которые позволят выявлять кибератаки на всех этапах их развития, проводить анализ первопричин и проактивный поиск угроз, а также оперативно и централизованно реагировать на сложные инциденты.

Решение обеспечивает надежную защиту от кибератак и помогает соответствовать требованиям законодательства, в том числе благодаря встроенному модулю ГосСОПКА, полностью интегрированному с технической инфраструктурой НКЦКИ. 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.

Все в одном

Всесторонняя защита с соблюдением требований законодательства

От безупречной защиты рабочих мест — к единой всеобъемлющей безопасности

Преимущества построения всеобъемлющей защиты с Kaspersky Symphony XDR

Технологии, получившие признание

Входящие в решение продукты и сервисы являются обладателями различных наград, их эффективность ежегодно подтверждается независимыми тестовыми лабораториями и аналитическими агентствами.

Комплексное решение

Единое предложение для защиты всей инфраструктуры с технологиями EPP, EDR, Sandbox, NTA, Threat Intelligence и другими, объединенное с собственной SIEM-системой, которая позволяет решению быстро встраиваться в существующую ИБ-систему.

Соответствие требованиям

Продукты в составе Kaspersky Symphony XDR входят в Реестр отечественного ПО. Решение помогает обеспечить соответствии требованиям регуляторов в вопросах ИБ, в том числе благодаря встроенному модулю ГосСОПКА.

Опыт и знания экспертов

Решение включает ряд запатентованных технологий и разработано на основе аналитических данных об APT-атаках, полученных глобальным центром исследования и анализа угроз «Лаборатории Касперского» (GReAT). Уникальная экспертиза и богатый международный опыт позволяют компании предоставлять пользователям актуальную высококачественную аналитику о киберугрозах.

Удобное лицензирование

Базовый уровень Symphony XDR Core для гибкого и поэтапного построения ИБ-системы.

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

Участие в тестированиях

«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 ENGENUITY | ATT&CK® Evaluations

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

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

FORRESTER®

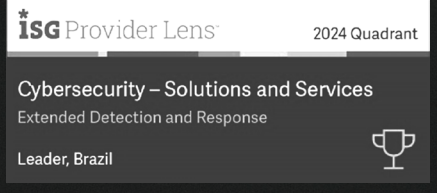
«Лаборатория Касперского» признана лидером по результатам исследования Forrester Wave: External Threat Intelligence Services (Внешние услуги по анализу угроз)

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

Все 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.

Kaspersky Symphony XDR

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее