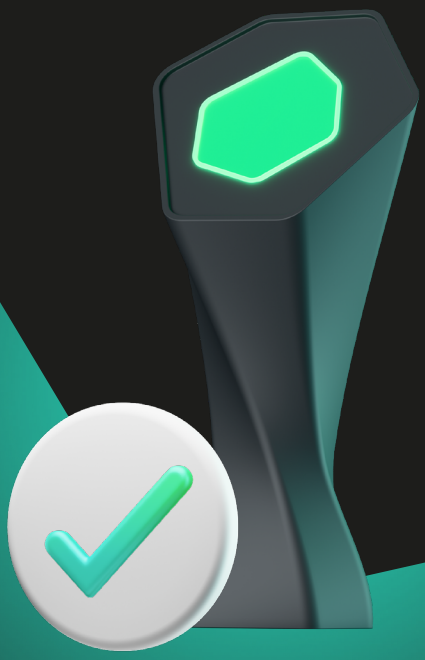
kaspersky



Как оптимизировать процессы SOC, создавая эффективные сценарии реагирования

Вступление: что такое сценарий реагирования (и чем он не является)

Сценарии многих атак, которые приходится расследовать команде SOC, рано или поздно повторяются – подобно волнам, снова и снова набегающим на берег. На первый взгляд они кажутся уникальными, но на деле могут происходить по одной и той же схеме. Сценарии реагирования – это пошаговые инструкции по устранению конкретных типов инцидентов, которые упрощают работу аналитиков с однотипными угрозами.

В стрессовой ситуации, когда каждая минута на счету, сценарии реагирования помогают аналитику действовать уверенно и последовательно. Сценарий и план реагирования на инциденты – это не одно и то же. План реагирования охватывает более масштабные организационные процессы, определяет роли и политики. Он разрабатывается на базе корпоративной стратегии безопасности и предусматривает, например, порядок уведомления регулирующих органов об инциденте, но при этом в нем нет четких практических указаний, которые нужны аналитику во время реагирования.

Сценарий представляет собой пошаговое руководство по реагированию на сложные угрозы определенной категории, которым аналитики могут уверенно пользоваться при расследовании аналогичных атак. Это существенно сокращает сроки реагирования и снижает риски. Без таких сценариев аналитикам пришлось бы разрабатывать тактики реагирования на основе общей стратегии безопасности прямо в разгар инцидента. И если не удастся верно определить следующий шаг, команда может оказаться в тупике и упустить драгоценное время.

При наличии сценариев наряду с планом реагирования специалисты SOC могут реализовывать стратегические цели через конкретные действия. План определяет, кто за что отвечает и зачем это нужно, а сценарий описывает, как реализовать план на практике. Вместе эти два инструмента повышают устойчивость компании к повторяющимся угрозам.

Последовательность имеет значение: от плана реагирования к средствам обнаружения и сценариям

Сценарии реагирования разрабатываются в строго определенном логическом порядке. Прежде всего, нужно сформировать план реагирования при участии IT-отдела, специалистов по управлению рисками и других ответственных лиц. Если от инцидента пострадают системы, люди или репутация компании, каждая группа будет ответственна за принятие определенных мер реагирования, поэтому важно, чтобы эти действия были согласованными.

Следующий шаг – подготовить средства обнаружения. В конце концов, от сценария будет мало толку, если вы не можете обнаружить инцидент. Однако это не означает, что достаточно создать небольшой набор правил детектирования и на этом успокоиться. Не имея полного представления об угрозах, аналитики не готовы эффективно реагировать на инциденты, а значит – защищать компанию.

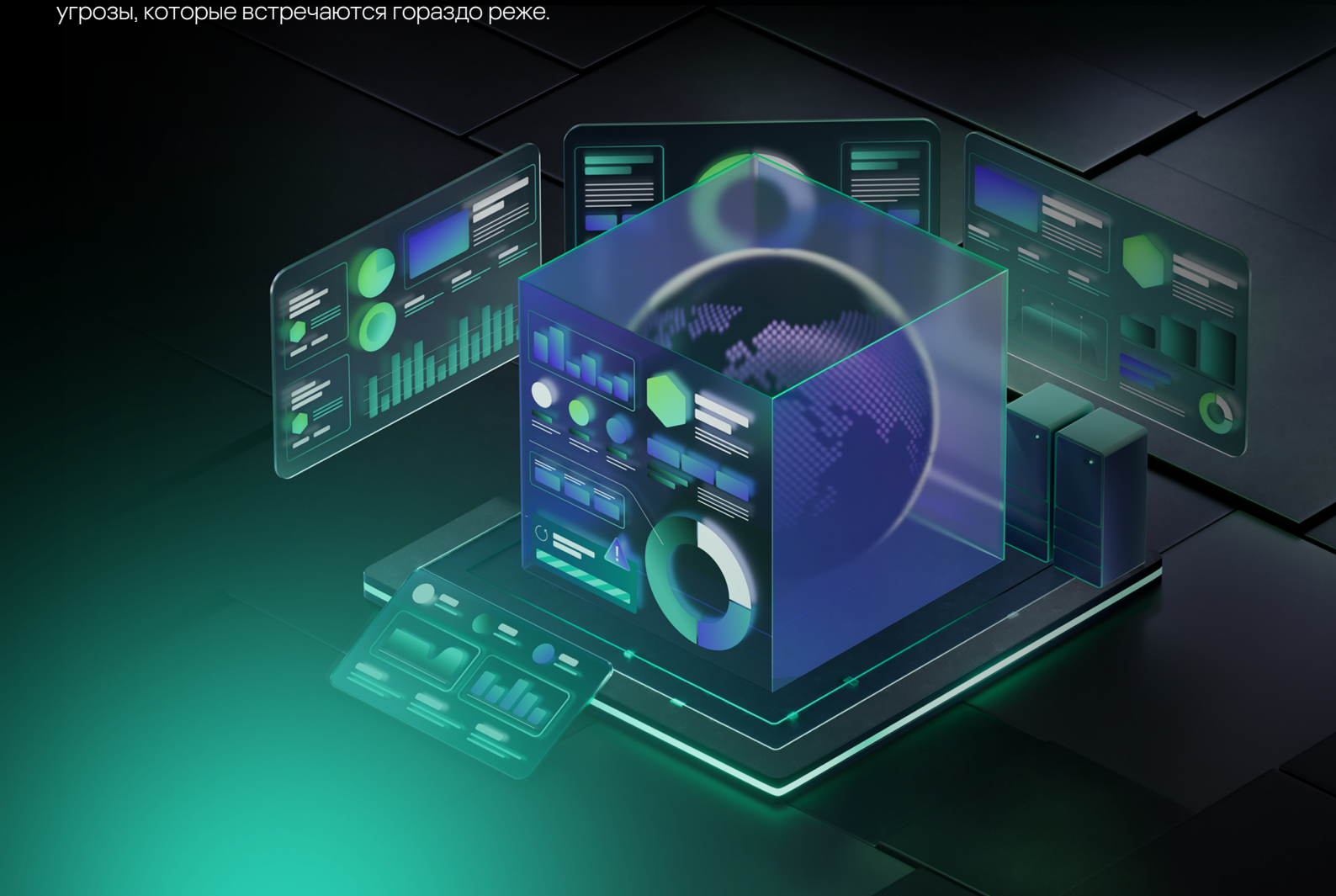
> К разработке сценариев реагирования следует приступать только после тщательного анализа возможностей доступных средств обнаружения. Вам не нужно сразу расписывать сценарии реагирования на угрозы, которые вы все равно пока не можете обнаружить.

Андрей Тамойкин, эксперт «Лаборатории Касперского» по кибербезопасности

Начать следует с разработки сценариев реагирования на инциденты, которые ваша команда может распознать с высокой степенью достоверности. Осваивая новые категории инцидентов, вы можете создавать новые сценарии. Это логичный подход, обеспечивающий баланс между готовностью команды к противодействию атакам и реалистичной оценкой ситуации:

- План реагирования определяет общую схему ответных мер.
- Возможности обнаружения дают представление об угрозах, с которыми вы можете справиться.
- Сценарии реагирования трансформируют ваши возможности в конкретные действия.

По мере расширения возможностей обнаружения растет и библиотека сценариев, и со временем SOC начинает эффективно реагировать не только на знакомые и ожидаемые угрозы, но и на более сложные угрозы, которые встречаются гораздо реже.



Кому и зачем нужны сценарии реагирования?

Сценарии реагирования повышают продуктивность SOC в целом, однако их основная задача – обеспечить согласованность и эффективность действий в повседневной работе. Это структурный подход, который устраняет потребность в обсуждении каждого последующего действия и экономит время специалистов, – и для современных SOC, которым изо дня в день приходится обрабатывать все больше данных об эволюционирующих угрозах, это особенно важно.

Что касается отдельных специалистов, сценарии больше всего пригодятся аналитикам, поскольку они содержат перечень четких инструкций и алгоритмов, которые следует использовать в том или ином случае. Иными словами, при получении оповещения аналитики могут следовать проверенным процедурам, не строя догадок и не изобретая велосипед. При таком подходе повышается уверенность специалистов, а новые или неопытные аналитики могут быстрее стать продуктивными членами команды. (Для понимания ситуации приведем статистику: 46% специалистов по ИБ признались, что начали чувствовать себя уверенно на своей первой работе в этой сфере лишь более чем через год с момента трудоустройства.)

> Оптимизация процессов реагирования повышает общую эффективность SOC, но все же максимум преимуществ получают аналитики.

Андрей Тамойкин, эксперт «Лаборатории Касперского» по кибербезопасности

Сценарии реагирования также снижают стресс, связанный с принятием решений. Зная четкий порядок действий, специалисты могут избежать умственного перенапряжения во время длительной смены или стремительно развивающегося инцидента. В результате меры реагирования будут приниматься быстрее и более предсказуемо. Со временем этот подход повысит общую надежность процессов в SOC и руководители смогут сосредоточиться на развитии стратегии и повышении устойчивости компании к угрозам.

Постоянное совершенствование и пересмотр сценариев

Сценарий быстро потеряет свою ценность, если его не корректировать. Угрозы эволюционируют, появляются новые инструменты, а эксперты накапливают практический опыт. Сценарии реагирования должны быть согласованы с текущими процессами, технологическими возможностями и целями компании, поэтому их следует пересматривать регулярно – в идеале не менее одного раза в год.

> Практически все функции SOC требуют непрерывного совершенствования – и сценарии не исключение.

Андрей Тамойкин, эксперт «Лаборатории Касперского» по кибербезопасности

Не менее важно пересматривать сценарии после некоторых событий. Каждое изменение в алгоритмах обнаружения и инфраструктуре, а также масштабные инциденты требуют корректировки соответствующего сценария. Именно в таких ситуациях пробелы в системе защиты и возможные пути улучшения становятся очевидными. Обновление сценариев реагирования в ответ на такие события позволяет SOC не просто восстановиться после инцидента, но и стать сильнее.

В организациях, где сценарии пересматриваются не только планово, но и после каждого значимого события, процессы реагирования развиваются вместе с SOC, а сами сценарии становятся все более надежным и эффективным инструментом.

Что такое «хорошо» – и как это измерить

Эффективные сценарии реагирования не только содержат четкие инструкции, легко применимые на практике, но и позволяют достичь измеримых результатов. Существуют показатели, позволяющие оценить, работает ли сценарий так, как было задумано. Одним из ключевых показателей является среднее время классификации оповещений. Оно отражает, насколько быстро аналитики определяют, является ли оповещение ложным или истинным. Это важно, чтобы распределять ресурсы рационально. Качество классификации можно оценить по уровню ложноположительных и ложноотрицательных срабатываний. Слишком частые ложноположительные срабатывания приводят к напрасной трате времени, а ложноотрицательные означают, что угрозы остались незамеченными.

> Среднее время классификации – один из ключевых показателей: мы должны проверять инциденты в максимально сжатые сроки.

Андрей Тамойкин, эксперт «Лаборатории Касперского» по кибербезопасности

Еще один важнейший показатель – среднее время реагирования. Он помогает оценить, насколько быстро SOC может локализовать инцидент и предоставить рекомендации по устранению последствий. Чем выше этот показатель, тем выше риск для защищаемых систем. Чем он ниже, тем эффективнее работает команда.

Эффективная автоматизация сценариев

Важным показателем является уровень автоматизации. Соотношение числа ручных и автоматизированных операций в рамках одного сценария показывает, есть ли в нем пространство для оптимизации или он уже достаточно эффективно организован.

Однако, несмотря на очевидные преимущества автоматизации, ее не следует закладывать в сценарий изначально. В основе любого сценария реагирования должны лежать тщательно протестированные ручные операции. Автоматизировать процесс нужно поэтапно и только после того, как вы убедитесь в его надежности. Базовое обогащение данных позволяет быстрее получить контекстную информацию, а оркестрация задач обеспечивает согласованное использование инструментов. При этом важные решения должны принимать живые люди – аналитики.

> Лучше разработать сценарии с ручными процессами реагирования, чем не иметь их вовсе.

Андрей Тамойкин, эксперт «Лаборатории Касперского» по кибербезопасности

Полная автоматизация возможна только в хорошо знакомых сценариях с низким уровнем риска. Действия с масштабными последствиями, такие как изоляция критически важных для бизнеса хостов или удаление учетных записей, требуют подтверждения человеком. В подобных случаях бездумная автоматизация принесет еще больше вреда, чем сама угроза. Здесь важно найти баланс: автоматизация должна снимать со специалистов бремя рутинной работы, но важные решения всегда принимает аналитик. При правильной реализации этого подхода ведущая роль останется за специалистами, а технологии повысят их продуктивность.

Область применения и структура сценариев

Область применения сценариев определяется категориями инцидентов, которые SOC обнаруживает с высокой достоверностью. Обычно таких категорий бывает от 20 до 30. Для каждой из них разрабатывается отдельный сценарий реагирования с ветвлениями, учитывающими возможные варианты развития инцидента. Эффективный сценарий объединяет ключевые этапы, общие для всех типов инцидентов, такие как классификация и сдерживание, и специализированные меры, направленные на нейтрализацию конкретных угроз, например вирусов или бэкдоров. Такой подход обеспечивает четкую последовательность выполнения действий с учетом ситуации.

> Нам не нужен сценарий реагирования на бэкдор. Нам нужен сценарий реагирования на заражение вредоносным ПО – с отдельными инструкциями по реагированию на бэкдоры, если это необходимо в вашей ситуации.

Андрей Тамойкин, эксперт «Лаборатории Касперского» по кибербезопасности

В небольших SOC за разработку и утверждение сценариев обычно отвечает руководитель отдела. В более крупных SOC эксперт по исследованию угроз или профильный специалист анализирует актуальность и необходимость каждого сценария, в том числе в контексте доступных возможностей обнаружения, тем самым обеспечивая эффективность библиотеки сценариев в целом.

Практическое внедрение: базовый фундамент и непрерывный рост

При внедрении сценариев реагирования начинайте с малого, например с обычных чек-листов для нескольких задач, которые вы выполняете во время реагирования на самые распространенные инциденты. С появлением новых технологий и возможностей дополняйте библиотеку сценариев новыми категориями инцидентов и автоматизируйте процессы там, где это действительно необходимо. Главное – развивать ваш набор сценариев вместе с потенциалом SOC.

> Не тратьте на сценарий больше времени, чем он поможет сэкономить.

Андрей Тамойкин, эксперт «Лаборатории Касперского» по кибербезопасности

Не нужно тратить время на создание сложных или теоретических сценариев, которые вряд ли когда-нибудь пригодятся вам на практике. Хотя подход к их созданию надо адаптировать к меняющимся условиям, сценарии всегда должны соответствовать реальным потребностям вашей команды, быть понятными и удобными в использовании.

Выводы

Эффективное реагирование на инциденты начинается с правильной подготовки: сначала разрабатывается план реагирования, затем выполняется анализ средств обнаружения, и только потом команда приступает к созданию сценариев. Для оценки эффективности нужно использовать четкие показатели, такие как среднее время классификации, среднее время реагирования, уровень ложноположительных и ложноотрицательных срабатываний и уровень автоматизации.

Сценарии реагирования должны постоянно дорабатываться – рекомендуется пересматривать их регулярно, а также после каждого существенного изменения инфраструктуры или набора инструментов. Автоматизация ускоряет процессы и повышает их эффективность, но важнейшие решения должен принимать человек.

Лучше всего начинать с простых сценариев, проверять их эффективность и развивать библиотеку сценариев по мере развития потенциала SOC.

О «Лаборатории Касперского»

«Лаборатория Касперского» – международная компания, работающая в сфере информационной безопасности и защиты конфиденциальности данных с 1997 года. Глубокие экспертные знания и многолетний опыт компании лежат в основе защитных решений и сервисов нового поколения, обеспечивающих безопасность бизнеса, критически важных инфраструктур, государственных учреждений и рядовых пользователей, защищая миллиарды устройств от новейших угроз и целевых атак. Обширное портфолио «Лаборатории Касперского» включает в себя передовые продукты для защиты рабочих мест, а также ряд специализированных решений и сервисов для борьбы с комплексными и постоянно эволюционирующими киберугрозами, в том числе кибериммунные системы. Наши технологии обеспечивают защиту самых важных аспектов бизнеса более 200 тысяч корпоративных клиентов. Подробнее см. на сайте www.kaspersky.ru.