Экономическая оценка ESG

Анализ экономических преимуществ платформы кибербразведки Anomali

Авив Кауфман и Алекс Арцилла, старшие аналитики по валидации

Июль 2020 г.

Краткий обзор

Сегодня для организаций критически важно предоставлять сотрудникам, которые все больше работают удаленно, эффективный доступ к приложениям и ресурсам в различных географиях, сетях и устройствах. Организации вынуждены оперативно внедрять решения, уменьшать ограничения и упрощать политики, а также минимизировать преграды, что еще больше увеличивает нагрузку на департаменты информационной безопасности в их работе по эффективной защите организаций и их активов. Департаменты информационной безопасности должны работать более рационально и эффективно, и использовать как можно больше данных кибербразведки для выявления и устранения угроз.

Компания ESG подтвердила, что пакет решений Anomali для работы с кибербразведкой помог оптимизировать работу SOC, автоматизировать рабочие процессы, сократить количество ложных срабатываний, повысить эффективность внутренней и внешней совместной работы, а также сократить время на обнаружение и устранение инцидентов. В рамках серии интервью компания ESG оценила преимущества, которые получили клиенты Anomali, и использовала эту информацию для создания смоделированного сценария, который показывает, как организация может сэкономить 93 тыс. долл. США в месяц за счет повышения производительности, снижения рисков и пользы, полученной от включенных в пакет продуктов. Модель ESG прогнозирует окупаемость инвестиций в размере 233% и период окупаемости всего 11 месяцев для организации с отделом кибербезопасности, состоящим из 10 человек, которая решила внедрить Anomali, в противоположность работе без платформы кибербразведки.

Введение

Данная экономическая оценка ESG ориентирована на количественные и качественные преимущества, которые могут ожидать организации, предоставляя своим специалистам по безопасности пакет продуктов Anomali для работы с киберразведкой за счет более быстрого и эффективного анализа, обнаружения, расследования, а также реагирования на потенциальные киберугрозы. Эти продукты включают Anomali ThreatStream (платформа киберразведки), Anomali Match (обнаружение киберугроз) и Anomali Lens (знания о киберугрозах).

Проблемы и задачи

Кибербезопасность — одна из главных проблем любой организации. Аналитики SOC прошли путь от реактивного реагирования на алерты и «затыкания дыр» до проактивного использования постоянно растущих объемов информации о киберугрозах для обеспечения более высокого уровня защиты. Исследования ESG показали, что 62% организаций планируют увеличить расходы на услуги по кибербезопасности в течение следующих 12–18 месяцев.[1] Доступность такого большого количества источников киберразведки становится проблемой для специалистов по безопасности, пытающихся найти способы эффективного сбора, управления, анализа и принятия соответствующих мер на основе этой аналитической информации. Такие организации никогда не будут иметь достаточного количества человеческих ресурсов для использования всей доступной им аналитической информации. Автоматизация и аналитика необходимы для эффективного определения приоритетов и извлечения иголки с ценными аналитическими данными из постоянно растущего стога киберразведки.

Многие крупные организации с течением времени внедрили широкий набор средств защиты информации, а также увеличили команду специалистов по безопасности для поддержки этих решений. Внедрение центров мониторинга и реагирования на инциденты кибербезопасности (SOC) привело к объединению знания и опыта таких команд под единым началом, что лучше подходит для обнаружения киберугроз и реагирования на них, однако эксперты по безопасности — это ограниченный ресурс, который сложно и дорого находить, обучать и удерживать. Аналогично, внедрение систем управления событиями безопасности (SIEM) позволяет более эффективно обнаруживать киберугрозы, объединяя киберразведку и информацию, сгенерированные множеством серверов и устройств, однако SIEM-системы имеют ограничения на объем данных, по которым можно осуществлять поиск и аналитику, и создают довольно много ложных срабатываний, требующих внимания специалистов, что ограничивает выявление киберугроз в организации. Поэтому неудивительно, что организации стремятся помочь своим перегруженным командам SOC более точно выявлять реальные киберугрозы и ускорять их реагирование на эти киберугрозы. Исследование ESG показывает, что технологии, которые используют искусственный интеллект (ИИ) и машинное обучение для выявления угроз, чаще других упоминаются как область кибербезопасности, в которую организации будут вкладывать наиболее значительные средства в 2020 году (см. рис. 1).

Рис. 1. Топ-5 приоритетных расходов на кибербезопасность в 2020 г.

Источник: Enterprise Strategy Group

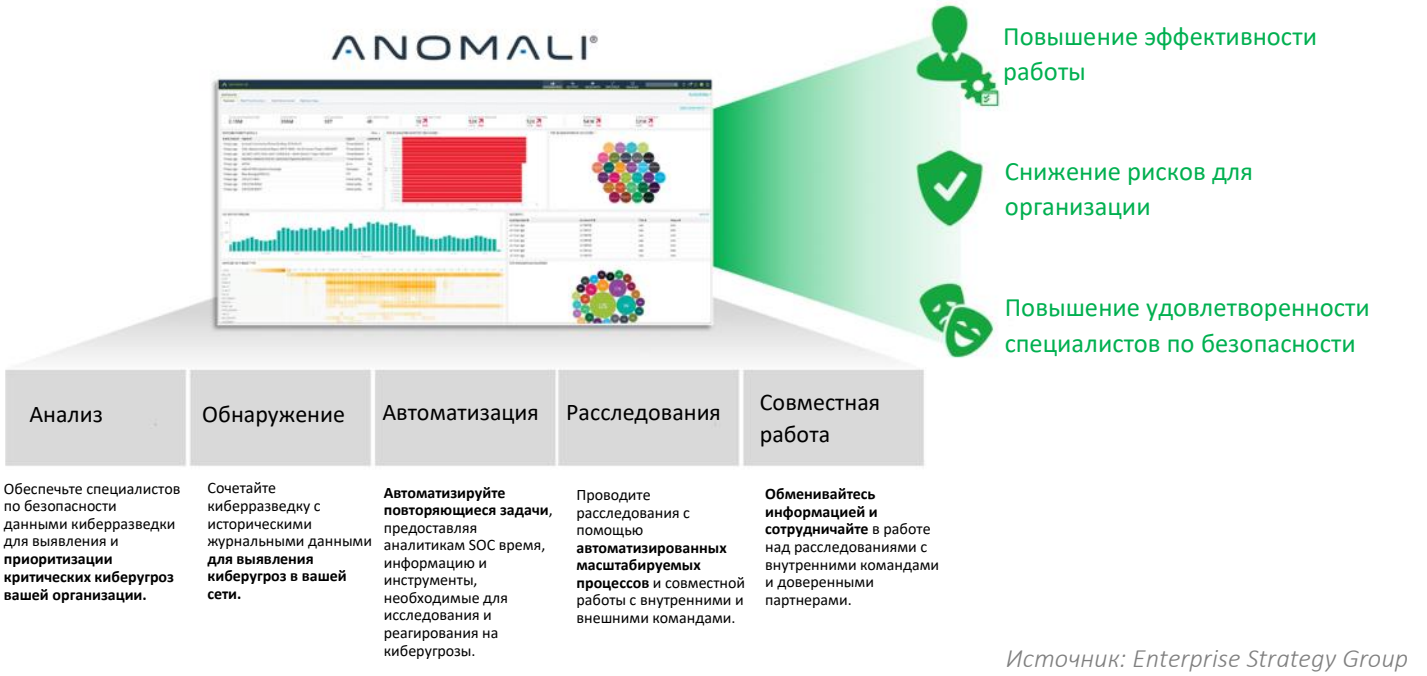
[1] Источник: результаты основного исследования ESG, *Исследование планируемых расходов на технологии 2020 г.*, январь 2020 г. Все ссылки на исследования ESG и графики в данной экономической оценке взяты из этого набора результатов основного исследования.

Несмотря на то что доступность огромных объемов киберразведки и журнальных данных потенциально позволяет обеспечить повышенный уровень безопасности, более эффективная защита может быть достигнута только в том случае, если организации смогут высвободить и оптимизировать коммуникации между наиболее ценными ресурсами — аналитиками SOC и специалистами по киберразведке.

Решение Anomali

Компания Anomali предлагает пакет решений по работе с киберразведкой, который обеспечивает непревзойденную аналитику по киберугрозам, ускоренное обнаружение и реагирование на угрозы, а также более высокую производительность. Продукты Anomali помогают организациям автоматизировать сбор, управление и внедрение множества внутренних и внешних потоков киберразведки, отфильтровывать ложные срабатывания, выявлять киберугрозы в своих средах и повышать эффективность работы, сосредотачиваясь на наиболее важных задачах кибербезопасности.

Рис. 2. Платформа киберразведки Anomali



Источник: Enterprise Strategy Group

Платформу Anomali можно развернуть в облаке, на площадке заказчика или в изолированном сегменте (локально без подключения к сети Интернет). Платформа состоит из трех основных продуктов: Anomali ThreatStream, Anomali Match и Anomali Lens.

Anomali ThreatStream объединяет разрозненные данные о киберугрозах в высокоточную аналитическую информацию, автоматически распространяет ее на средства защиты информации, а также включает набор инструментов для эффективного расследования киберугроз. ThreatStream автоматизирует сбор киберразведки из сотен внешних и внутренних источников, включая информацию из открытых источников, коммерческих фидов киберугроз, аналитическую информацию партнеров, а также киберразведку из внутренних расследований, анализа в песочнице и т. д. Продукт нормализует и дедублицирует эти фиды в общую таксономию, используя алгоритмы машинного обучения для устранения ложных срабатываний, обогащения данных и оценки данных киберразведки на критичность и достоверность. Затем ThreatStream позволяет использовать киберразведку для практической защиты посредством автоматического распределения машиночитаемых индикаторов на средства защиты информации (например, SIEM, МСЭ, EDR, IPS, SOAR и т. д.). Также продукт предоставляет аналитикам SOC инструменты для проведения расследований на основе моделей Diamond, Kill Chain, STIX и MITRE ATT&CK. Модуль проведения расследований включает в себя обширный набор источников обогащения данных, мощный инструмент Visual Explorer для раскрытия и пивотинга индикаторов, встроенный анализ в песочнице для вредоносного ПО и фишинговых URL-адресов, а также инструментарий для совместной работы по созданию и публикации отчетов по киберугрозам.

Anomali Match автоматизирует обнаружение киберугроз в сети путем постоянного сопоставления всей доступной киберразведки со всеми журнальными данными. Match достигает этого благодаря индексированию всех логов SIEM и других источников событий, храня полученные исторические данные в течение года или более, и постоянно сверяя их с уже существующими и новыми данными киберразведки. Полученные алерты автоматически доставляются в SIEM, SOAR и тикетинг-системы для реагирования и устранения инцидентов. Форензика в реальном времени позволяет аналитикам выявлять первичные источники заражения ранее выявленных атак, осуществлять хантинг киберугроз на основе имен хакерских группировок, уязвимостей или TTP, а также приоритизировать реагирование на основе оценки риска и критичности активов.

Anomali Lens предоставляет оперативную контекстуальную информацию о киберугрозах, автоматически идентифицируя данные киберразведки в любом веб-контенте с помощью обработки текста на естественном языке (NLP). Для этого Lens сканирует веб-страницы, социальные сети, SIEM и другие журналы безопасности, выявляя индикаторы компрометации (IOC), хакерские группировки, семейства вредоносных программ и методы атак. Информация о киберугрозах, идентифицированная Lens, автоматически налагается на матрицу MITRE ATT&CK и может быть импортирована в Anomali ThreatStream для дальнейшего исследования и анализа одним нажатием кнопки. Lens также интегрируется с Anomali Match для выделения тех просканированных индикаторов, которые присутствуют в сети, обеспечивая мгновенное понимание их уровня критичности и влияния на вашу среду.

Экономическая оценка ESG

Компания ESG выполнила количественную экономическую оценку и смоделированный анализ пакета решений Anomali.

Процесс экономической оценки ESG является надежным методом изучения, оценки, количественного анализа и моделирования экономической ценности продукта или решения. Этот процесс использует ключевые компетенции ESG в рыночном и отраслевом анализе, перспективных исследованиях, а также техническую и экономическую экспертизу. Специалисты ESG проанализировали результаты историй успеха и опросов конечных пользователей, а также провели подробные интервью с конечными пользователями, чтобы лучше понять и оценить, как платформа Anomali повлияла на их организации, в частности в сравнении с тем, как они работали до развертывания Anomali, или с предыдущим опытом в других организациях. Качественные и количественные результаты анализа были использованы в качестве основы для простой модели окупаемости инвестиций путем сравнения экономии и преимуществ, которые может ожидать смоделированная организация, с ожидаемыми затратами на развертывание Anomali.

Экономический обзор Anomali

Экономический анализ ESG показал, что клиенты, развернувшие Anomali, были чрезвычайно довольны продуктом и считали, что они значительно усовершенствовали процессы по обеспечению безопасности, стали работать более эффективно и в целом лучше справлялись с защитой организации. Компания ESG обнаружила, что Anomali обеспечила своим клиентам значительную экономию и преимущества в следующих категориях:

- Снижение расходов на текущие процессы ИБ (SecOps) — организации значительно упростили процессы по обеспечению безопасности и сделали более эффективным использование ресурсов безопасности благодаря возможностям автоматизации и оркестрации Anomali, а также хорошо спроектированным и эффективным инструментам и функциям платформы.
- Повышение эффективности и снижение рисков для безопасности организации — клиенты сообщили, что платформа Anomali помогла лучше вооружить команду безопасности и организовать процесс обеспечения безопасности, повысить эффективность работы и сократить время на выявление и устранение проблем безопасности.
- Повышение удовлетворенности и производительности текущих процессов ИБ — Anomali помогает повысить производительность и удовлетворенность специалистов по безопасности за счет автоматизации повторяющихся или трудоемких задач, что позволяет им сосредоточиться на более ценных операциях обеспечения безопасности. Навыки быстро улучшаются, повышается эффективность совместной работы и прозрачность, а также растет синергетическая ценность с другими средствами защиты информации.

Снижение эксплуатационных расходов на текущие процессы ИБ

Компания ESG обнаружила, что специалисты по безопасности, развернувшие продукты Anomali, сообщили, что процессы по обеспечению безопасности были значительно упрощены благодаря удобству использования, автоматизации и оркестрации. Пользователи сообщили о значительной экономии времени или сокращении затрат в ряде областей, включая развертывание новых технологий, исследование киберугроз, обогащение данных, реагирование на ложные срабатывания и сопоставление информации из нескольких источников (а также во многих других областях). Это позволило специалистам получать больше информации от каждого аналитика ИБ, повышать способности младших аналитиков, быстрее приступать к работе и сокращать время, затрачиваемое на менее важные задачи, что дало возможность команде сосредоточиться на более важных задачах, таких как устранение последствий инцидентов.

- Снижение административной нагрузки — клиенты сообщили, что решение ThreatStream снизило административную сложность работы с множеством потоков киберразведки и точечных средств защиты информации. Уменьшилось число интерфейсов управления, новые премиальные фиды можно легко протестировать и внедрить, не покидая продукт, а функционал управления IOC встроен в систему. Это позволило организациям избежать затрат времени и ресурсов на внедрение, управление и интеграцию нескольких продуктов с разными интерфейсами.
- Сокращение сроков окупаемости — решение ThreatStream оказалось быстрым и простым при развертывании, интеграции с IOC, а также добавлении или удалении премиальных фидов. Обширная экосистема партнеров и наборы разработчиков (SDK) позволили организациям быстро внедрить именно те внутренние и внешние инструменты и фиды киберразведки, которые наилучшим образом отвечают их потребностям. Условно-бесплатные опции позволяют клиентам подписаться на коммерческие фиды поставщиков киберразведки для оптимизации программ анализа киберугроз. Процесс продажи не вызвал сложностей, и организации чувствовали, что тратят меньше времени на решение проблем с интеграцией и поддержкой. Это означает, что организации смогли быстрее протестировать и интегрировать стратегии и инструменты обеспечения безопасности. Один клиент прокомментировал: «Anomali экономит нам время и силы при закупке и установке фидов, мы знаем, что они уже настроены и готовы к использованию без интеграции, что позволяет экономить часы и дни в зависимости от сложности».

«Я мог бы потратить несколько часов на расследование и сбор контекста, но с платформой Anomali я могу просто ввести URL-адрес или выбрать опцию в Lens, и точно узнать, какие действия по устранению инцидента я должен предпринять».

- Оптимизированные процессы — платформа Anomali помогла организациям оптимизировать процессы обеспечения безопасности, сократив время, затрачиваемое на расследования аналитиками SOC, киберразведки и реагирования на инциденты, объединив их работу в рамках единой платформы. Упрощение рабочих процессов, тесная интеграция с другими фидами и СЗИ, а также обогащение киберразведки и расследований свели к минимуму время, затрачиваемое аналитиками на все аспекты обнаружения, расследования и реагирования на киберугрозы.
- Автоматизация задач — пользователи сообщили, что после развертывания ThreatStream значительно снижается количество задач, выполняемых вручную. Платформа Anomali автоматизирует многие повторяющиеся и трудоемкие задачи, которые занимают большую часть рабочего времени аналитиков, включая нормализацию источников, расследование и анализ профиля риска, форматирование и обогащение киберразведки, а также создание отчетов. Anomali также выполняет оркестрацию многих задач по конфигурации, интеграции и двунаправленным взаимодействиям между СЗИ, такими как SIEM, МСЭ и сетевые устройства. Решение Anomali Match обработало журнальные данные для одного клиента, причем, по оценкам пользователей Anomali, для ручного исполнения

«Без Anomali для выполнения задачи нам потребовалось бы восстановить журналы SIEM с ленты, что заняло бы более двух недель, в то время как Anomali Match позволила нам выполнить эту задачу менее чем за час».

такой задачи потребовалось бы в 2,5 раза больше людей: «У нас есть четыре человека, которые выполняют работу, на которую в противном случае потребовалось бы, наверное, десять человек».

- Меньше потраченного впустую времени — организации, развернувшие Anomali, сообщили, что теперь им приходится иметь дело с гораздо меньшим количеством ложных срабатываний и «усталости от алертов». Пользователи поняли, что это дало им дополнительное время на то, чтобы сосредоточиться на более важных задачах. Автоматизация расследований и обогащение данных кибербразведки позволили сократить время, затрачиваемое на анализ ситуации, снизить риск дублирования задач и уменьшить количество операций по устранению проблем из-за человеческой ошибки. Один из пользователей заявил: «Мне больше не нужно начинать процесс хантинга с попыток выяснить, что означает индикатор или почему он плохой, что ранее составляло около 90% моей работы».

Повышение эффективности и снижение рисков для безопасности организации

Anomali работает совместно с другими средствами защиты информации и представляет из себя оптимизированное решение, которое более эффективно выявляет индикаторы взлома, уменьшает количество ложных срабатываний, а также предоставляет контекст и аналитические данные для понимания и устранения киберугроз. Клиенты, с которыми мы общались, полагают, что платформа Anomali значительно повысила общую эффективность процессов по обеспечению безопасности, а некоторые из них сообщают, что Anomali также сделала выявление и устранение киберугроз на 90% эффективнее.

- Ускорение результатов — конечные пользователи увидели, что при использовании Anomali совместно с другими инструментами заметно снизилось время на получение практического результата анализа. Клиенты сообщили о большей гибкости фидов, улучшенном мониторинге и данных, обогащенных индикаторами, что помогло сократить время до распознавания и обнаружения киберугроз и, в конечном счете, привело к снижению среднего времени реагирования (MTTR) и устранения угроз. Один пользователь сообщил, что решение Anomali Match помогло снизить MTTR при валидации IOC с более чем девяти дней до десяти минут. Клиенты согласились, что Anomali позволила им обнаруживать, исследовать и устранять более высокие объемы и более широкий набор киберугроз и индикаторов взлома за меньшее время.

«Без Anomali мы бы пропустили множество киберугроз, или затратили бы гораздо больше времени на их выявление и устранение. Платформа стала критически важной частью нашего процесса мониторинга безопасности».

- Аналитика на базе машинного обучения — Anomali использует алгоритмы машинного обучения для обогащения контекста киберугроз, определения приоритетов киберугроз и выполнения хронологической оценки событий. Это предоставляет организациям более целостную, эффективную и своевременную аналитическую информацию, чем можно было бы получить за несколько часов работы вручную. Специалисты сообщили, что это помогло им быстрее идентифицировать, исследовать и реагировать на киберугрозы, также они высказали мнение, что теперь их SOC стал работать эффективнее, чем раньше. Один пользователь прокомментировал: «С Anomali мы впервые можем экспоненциально наращивать и управлять возможностью сбора и использования информации из сети Интернет — теперь человеческий фактор больше не является ограничением».

- Больше обработки кибербразведки — решение ThreatStream позволило специалистам обрабатывать больший объем и более широкое разнообразие кибербразведки, чем раньше. Они могут тестировать и управлять большим количеством внешних фидов, а также объединять их с оперативными отчетами о киберугрозах и внутренней кибербразведкой. Чрезвычайно ценной стала возможность выполнять профилирование источников киберугроз и отслеживать их в течение длительного периода времени. Один из клиентов заявил: «Существуют и другие TIP, которые могут собирать фиды и коррелировать их, однако ключевая польза Anomali заключается в том, что это решение позволяет нам добавлять и наши собственные данные».

- Более эффективное реагирование на киберугрозы — все пользователи, с которыми мы общались, согласились, что платформа Anomali помогла им гораздо эффективнее реагировать на киберугрозы безопасности. Решение ThreatStream не только помогло обрабатывать больший объем кибербразведки и быстрее выявлять угрозы, но и значительно сократило объем работы, которую раньше выполняли аналитики, за счет автоматизации обновления фидов, корреляции индикаторов и анализа кибератак для выявления связей между ними, а также за счет проактивного предоставления отчетов и действий по устранению инцидентов. Один из клиентов поделился: «Вместо того чтобы просто указывать, что IP-адрес плохой, теперь я могу понять, почему IP-адрес плохой, какие действия он осуществлял и какие шаги я должен предпринять».

«Вместо того чтобы проверять каждое из этих электронных писем или каждый из этих IP-адресов один за другим, я могу получить общее понимание происходящего и увидеть, что 90% из них происходят от одной кибератаки, одного типа индикатора или одного тега».

Почему это важно

Целью каждой организации является обеспечение более эффективной безопасности ведения бизнеса.

Клиенты Anomali заявили, что, по их мнению, платформа на 90% эффективнее выявляет и устраняет киберугрозы. Одна организация сообщила, что Anomali стала причиной того, что им удалось избежать похищения пользовательских средств на сумму более 400 тысяч долл. США, за счет упреждающего выявления и принятия кроссфункциональных мер для защиты учетных записей пользователей от попытки взлома.

- Более информированное принятие решений по безопасности — пользователи сообщили, что Anomali предоставляет ряд простых, но эффективных панелей управления, которые помогают специалистам визуализировать киберугрозы, определять приоритеты при принятии решений и обмениваться информацией с другими специалистами удобным способом. Встроенные возможности песочницы, доступность команды экспертов Anomali по кибербразведке и возможность обмена информацией с коллегами помогли предоставить дополнительную информацию, которая оказалась полезной при принятии внутренних решений. Пользователи согласились с тем, что платформа Anomali обеспечила возможность принимать более обоснованные и своевременные решения, помогая снизить риск для организации.

Повышение удовлетворенности и производительности процессов ИБ

Каждая организация, с которой мы говорили, сообщила, что платформа Anomali помогла ей трансформироваться для максимального использования имеющихся ресурсов. Они сообщили, что их специалисты стали намного более продуктивными и более удовлетворенными своей работой, и что организация смогла эффективнее взаимодействовать с бизнесом и коллегами.

- Более продуктивные специалисты по ИБ — ThreatStream позволяет каждому сотруднику работать более продуктивно и сосредоточиться там, где он приносит максимальную пользу. Специалисты сообщили, что менее опытные сотрудники, приступая к работе, вносили свой вклад раньше, учились быстрее и стремительно получали больше опыта, выполняя более важные задачи. Это является преимуществом как для организации, так и для карьерного роста сотрудников.

«Благодаря Anomali у нас два человека выполняют работу, на которую [названная организация] выделяет очень большую команду — и мы выполняем ее лучше».

- Более удовлетворенная команда ИБ — конечные пользователи указали, что поскольку Anomali помогает им лучше выполнять свою работу, они лучше спят по ночам, быстрее продвигаются по карьерной лестнице и чувствуют, что достигли большего для защиты компании. В целом они сообщили, что теперь рассматривают свою работу как более положительный опыт. Организации считают, что платформа Anomali помогла им построить более сильную команду и создать среду, в которой проще удерживать сотрудников, в сфере, где люди изо всех сил пытаются найти и удержать талантливых специалистов.

- Улучшение бизнес-процессов — клиенты сообщили, что решение ThreatStream позволило им более эффективно обмениваться информацией между командами и вести гораздо более продуктивные дискуссии между отделами обеспечения безопасности, бизнес-подразделениями и конечными пользователями. Одна организация заявила: «Мы смогли создать несколько действительно интересных процессов на основе Anomali. Мы работали с нашим отделом по борьбе с мошенничеством, нашей Red Team и отделом кибербразведки, даже с отделом комплаенса, и коммуницируем им о том, что мы активно видим». Клиенты сообщили, что они лучше информируют своих пользователей, поскольку могут лучше демонстрировать наблюдаемые киберугрозы в простой для понимания форме. Они ощущали, что без Anomali у них не было возможности взаимодействовать с бизнесом, не затрачивая часы на написание подробных разъяснений.

«Anomali улучшает некоторые уже существующие процессы, а также открывает для нас новые возможности, поскольку мы можем более эффективно взаимодействовать с коллегами».

- Более эффективная совместная работа с коллегами — клиенты считают, что платформа Anomali предоставила им средства для обмена внутренней кибербразведкой и рекомендациями по устранению киберугроз с внешними коллегами в рамках доверенной среды. Это позволяет организации вносить свой вклад или даже стать лидером среди коллег по индустрии, одновременно позволяя сообществу более эффективно выявлять и устранять киберугрозы, а также экономить ценное время за счет отсутствия необходимости повторно выполнять расследования, которые уже были проведены другими членами сообщества. Один из клиентов рассказал: «Возможность обмениваться аналитической информацией с коллегами оказалась чрезвычайно полезной, поэтому нам больше не нужно так глубоко копать или даже пропускать удары благодаря возможности обмениваться кибербразведкой».

Анализ ESG

ESG использовала информацию, собранную с помощью материалов, предоставленных поставщиком, общедоступные и отраслевые знания в области экономики и технологий, а также результаты интервью с клиентами для создания трехлетней модели окупаемости инвестиций, которая сравнивает затраты и преимущества внедрения Anomali ThreatStream, Match и Lens с дальнейшей работой без платформы анализа и обнаружения киберугроз. Интервью ESG с клиентами Anomali в сочетании с опытом и знаниями в области экономического моделирования и технической оценки продуктов Anomali помогли сформировать основу для нашего смоделированного сценария.

Организация, смоделированная ESG, состояла из группы, в которую входили 10 аналитиков кибербразведки с различными степенями опыта предоставления услуг по обеспечению безопасности организации с 1500 сотрудниками. Компания ESG учла ожидаемые затраты на установку, внедрение и обучение сотрудников использованию платформы Anomali, а также ежегодные затраты на подписку, аппаратные узлы, затраты на инфраструктуру, поддержку и обслуживание в течение трех лет.

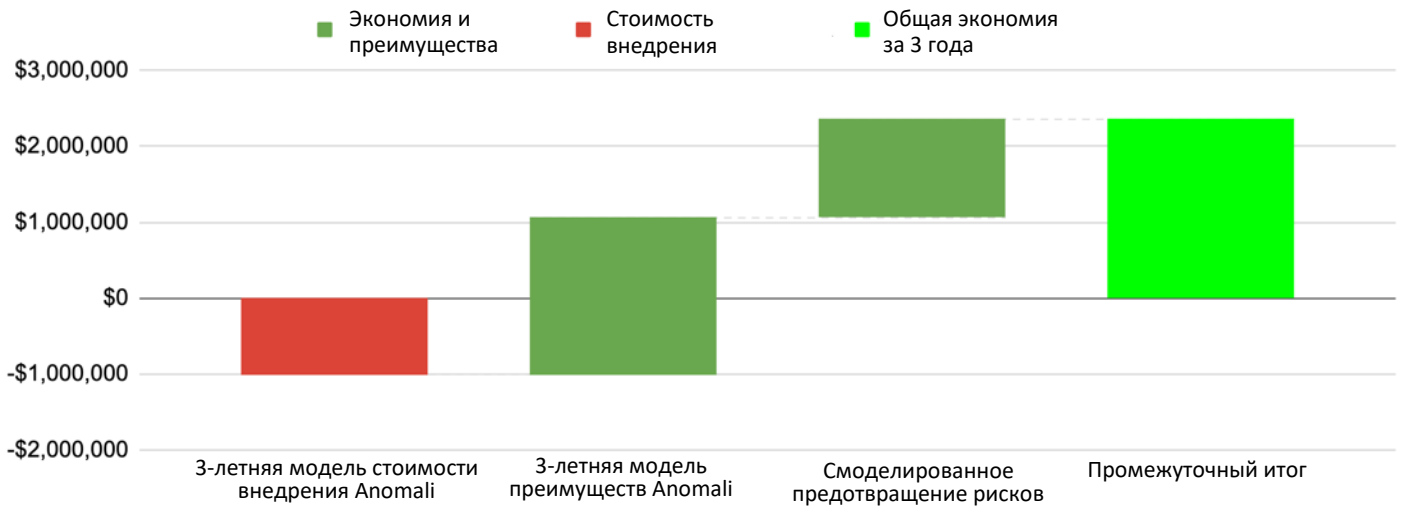
Что касается преимуществ, ESG смоделировала ожидаемые сэкономленные затраты или преимущества от повышения производительности департамента безопасности на основе ожидаемого улучшения от 20% до 70% в отношении задач, связанных с управлением и курированием фидов, выполнением расследований и отчетностью по их результатам, интеграцией с другими системами безопасности, обменом кибербразведкой с сотрудничающими организациями, а также совместным использованием и составлением отчетов по аналитике в рамках организации. ESG консервативно оценила, что только 35% общего количества человеко-часов отдела безопасности были потрачены на выполнение этих задач. Модель ESG показала повышение производительности на 58% при выполнении этих задач и трехлетнюю экономию в размере 969 000 долл. США. Эта экономия проявляется в виде человеко-часов, которые теперь доступны для дополнительных задач, связанных с безопасностью, и которые не были доступны до внедрения Anomali.

В моделях ESG прогнозировалась экономия средств за счет сокращения на 40% количества ложных срабатываний (608 тыс. долл. США), стоимости, связанной с продуктами для обеспечения безопасности, которые предоставляет Anomali (песочница, условно-бесплатные и премиальные фиды кибербразведки, оперативная поддержка Anomali и обучение в Университете Anomali) общей стоимостью 452 тыс. долл. США, а также другая экономия средств за счет отказа от профессиональных услуг, обучения и сертификации, а также упрощения закупки и интеграции (53 тыс. долл. США).

Компания ESG также смоделировала предотвращение рисков, обеспечиваемое за счет более низкой вероятности утечки данных, на основе увеличения вероятности раннего обнаружения, повышенной общей эффективности, а

также ускоренного устранения проблем и снижения ожидаемых затрат при утечке данных благодаря возможности более быстро и эффективно обнаруживать угрозы и реагировать на них. Предположения ESG о вероятности и затратах при утечке данных основаны на общедоступных данных, опубликованных Институтом Понемона. Компания ESG подсчитала, что Anomali может снизить риск для организации, избежав ожидаемых затрат на утечку данных в размере до 1,292 млн долл. США в течение трех лет. Результат данного анализа издержек и преимуществ приведен на рис. 3.

Рис. 3. Результаты анализа ESG трехлетних издержек и преимуществ работы на платформе кибербразведки Anomali



Источник: Enterprise Strategy Group

Что означают эти цифры

Анализ, смоделированный компанией ESG, предсказал существенную экономию и преимущества для нашей смоделированной организации. Несмотря на то что ни один из смоделированных сценариев не может с точностью представить экономические показатели каждого внедрения, ESG призывает организации провести собственный анализ, чтобы узнать, сколько они могут сэкономить. ESG предлагает организациям учитывать следующие затраты, включенные в наш анализ:

- Стоимость внедрения решения Anomali — включает стоимость подписки Anomali; человеко-часы, необходимые для развертывания, тестирования и обучения специалистов по техническому обслуживанию; оборудование для работы с Anomali, затраты на электроэнергию/охлаждение/рабочее пространство; а также поддержку и техническое обслуживание аппаратного обеспечения.
- Ценность включенных продуктов для кибербразведки — стоимость в долл. США эквивалентных решений для песочницы, фидов, поставляемых с TIP, включая условно-бесплатные и премиальные фиды, обучение в Университете Anomali, экспертную поддержку и т. д.
- Избежание затрат на обработку ложных срабатываний — ESG рассчитала 50 ложных срабатываний в день на одного аналитика, 2 минуты, затрачиваемые на каждое ложное срабатывание, и снижение количества ложных срабатываний на 40% с благодаря Anomali.
- Повышение производительности SOC — подробные консервативные модели ESG учитывали ожидаемое количество человеко-часов, потраченных до внедрения Anomali, в сравнении с ожидаемым улучшением сбора фидов (улучшение на 70%), управления и курирования фидов (улучшение на 70%), исследований и отчетов (улучшение на 60%), интеграции с системами защиты информации (улучшение на 20%), эффективности совместной работы с другими организациями (улучшение на 50%) и внутреннего совместного использования и эксплуатации (улучшение на 60%).
- Количественная оценка снижения риска — компания ESG рассчитала снижение риска утечки данных по сравнению со средним показателем по отрасли, пропорциональное улучшению на 70% обнаружения и реагирования, а также снижению ожидаемых затрат, связанных с утечкой данных, для автоматизированных систем (оба показателя предоставил Институт Понемона).

Вся правда

В опросах респондентов, участвовавших в исследовании ESG, усиление кибербезопасности последовательно возглавляло список бизнес-факторов, определяющих расходы на технологии в течение нескольких лет. По мере того как организации продолжают наращивать и организовывать свои команды и инвестировать в новые решения, очевидно одно: проблема заключается не в недостатке средств защиты информации и кибер разведки, а в отсутствии человеческих возможностей эффективно управлять, интерпретировать и действовать на основе кибер разведки и алертов. Современным подразделениям информационной безопасности требуется платформа кибер разведки, которая может помочь оптимизировать процесс обеспечения безопасности, автоматизировать повторяющиеся задачи, предоставить кибер разведку на основе ИИ и повысить эффективность работы сотрудников.

Компания ESG подтвердила, что решения Anomali ThreatStream, Match и Lens предоставили клиентам платформу, которая помогает извлечь максимальную выгоду из инвестиций в системы безопасности. Отделы информационной безопасности гораздо лучше оснащены, более продуктивны и сосредоточены на наиболее важных задачах; их инвестиции в SIEM и другие средства защиты информации с легкостью интегрируются и улучшаются, обеспечивая еще большую ценность; а фиды кибер разведки готовы к оценке, покупке и интеграции. Клиенты сообщили о значительно улучшенном понимании обстановки и более эффективных возможностях обмена кибер разведкой внутри компании с другими ее подразделениями, а также за пределами компании с коллегами и организациями по обеспечению безопасности.

Смоделированный ESG анализ издержек и преимуществ показывает, что организация, внедряющая Anomali, может рассчитывать на экономию за счет повышения производительности отдела обеспечения безопасности, добавленной стоимости за счет включенных продуктов кибер разведки и избежания рисков. Ключевые предположения в модели ESG проверены с клиентами Anomali. Согласно прогнозам компании ESG, общая экономия составила 93 тыс. долл. США в месяц, а ожидаемая окупаемость инвестиций (ROI) — 233%.

Платформа Anomali не конкурирует с существующими средствами защиты информации организации и не стремится к функциональному изменению способов работы специалистов. Вместо этого Anomali служит для практического применения и улучшения кибер разведки, инструментов и решений, позволяя специалистам по ИБ быть более эффективными и расширять обсуждение вопросов безопасности на другие подразделения компании. Каждая организация, с которой поговорила ESG, чувствовала, что она добилась гораздо большего с командой меньшего размера и увеличила масштабы деятельности, выходящие далеко за рамки того, что было реально достижимо с помощью одних только человеческих ресурсов. Некоторые из них даже стали использовать Anomali на новых должностях: «Я использовал Anomali на предыдущей должности, и когда начал работать здесь, то сказал: без Anomali мы не сможем достичь наших целей». Как аналитик, вы быстро поймете, что такое утверждение является признаком трансформационной технологии. Если вы хотите преобразовать и оптимизировать свой SOC и получить максимальную отдачу от кибер разведки, ESG рекомендует обратиться к Anomali, чтобы узнать, подходит ли платформа кибер разведки для вашей команды.