ИЗМЕНИТЕ ПОДХОД К БЕЗОСНОСТИ С ПОМОЩЬЮ XDR

Не останавливайтесь на защите конечных устройств от сложных угроз

Введение

Целью любой команды безопасности является защита инфраструктуры и данных организации от повреждения, несанкционированного доступа и неправильного использования. Архитекторы и инженеры безопасности обычно используют многоуровневый подход к предотвращению вторжений. Поскольку атаки стали более автоматизированными и сложными, подход к защите стал включать уровни визуализации, продукты обнаружения и реагирования, такие как защита конечных точек от сложных угроз — Endpoint Detection and Response (EDR), анализаторы сетевого трафика — Network Traffic Analysis (NTA) и системы управления инцидентами ИБ Security Information and Event Management (SIEM).

Много времени и опыта было потрачено для визуализации по слоям. Разрозненные продукты обнаружения и реагирования атак создают множество сообщений, требующие большего профессионального опыта и навыков для решения проблем. Бесконечный цикл и поток сообщений об инцидентах ИБ, множество инструментов и информации для аналитической работы, всё больше и больше времени требуется для обнаружения вторжений, и в результате, команда безопасности сталкивается с выгоранием, при этом затраченного времени оказывается недостаточно. Чем больше мы реагируем, тем больше отстаем.

Рисунок 1: Сеть, рабочая станция или облако

Многие организации, подобные вашей, борются с одной и той же проблемой: Как мы можем отойти от реагирования на входящие оповещения и перейти к активной оборонительной позиции, которая может улучшить предотвращение угроз?

Пришло время для другого подхода — того, который приносит пользу всей команде безопасности, а не обременяет её, упрощает операции и предоставляет средства для быстрого обнаружения и реагирования на самые сложные угрозы во всей инфраструктуре.

Сегодняшний подход: Решение одной проблемы создает другие

Команды безопасности упорно работают над обеспечением безопасности своих организаций, но сталкиваются с трудностями в своих усилиях по предотвращению нарушений данных. Пять основных проблем включают:

- Избыточное количество сообщений
- Слишком малое количество аналитиков безопасности
- Узконаправленные инструменты
- Отсутствие интеграции
- Нехватка времени

Рис. 2: Команды SOC сталкиваются с пятью основными проблемами

Давайте рассмотрим каждую проблему в деталях.

1. Избыточное количество сообщений

Аналитики безопасности видят слишком много событий, чтобы эффективно справляться с ними. 55% групп безопасности или центров управления информационной безопасности (Security Operations Center — SOC) получают в среднем более 10 000 событий в день[1]. Однако не все события равны — большинству из них необходимо установить правильный приоритет, соотнести или нормализовать и добавить в пул оповещений. Даже с наличием SIEM, команде SOC сложно проверить эту массу данных, аналитик безопасности должен по-прежнему увеличивать время на сбор данных в ручном режиме, выполнять анализ и отсеивать ложные срабатывания очень быстро, чтобы не пропустить самые важные и критические предупреждения. Слишком часто аналитики становятся жертвами рутинной работы, когда они отфильтровывают предупреждения, основанные на предыдущих предположениях или на огромной массе данных. Из-за переизбытка количества оповещений 54% специалистов по безопасности игнорируют оповещения, которые следует расследовать[2].

2. Нехватка квалифицированных кадров

Многие организации пытаются преодолеть растущую нагрузку, нанимая больше людей, но во всем мире существует нехватка квалифицированных специалистов по безопасности, которые, по прогнозам аналитиков, достигнут 1,8 миллиона к 2022 году . Особенно трудно найти специалистов с опытом анализа сети или рабочих станций, а в прочем и тех и других. В результате, группы безопасности перегружены сортировкой уведомлений, а также расследованием и реакцией на события. Они тратят чрезмерное количество времени на утомительные задачи, такие как сбор данных, ручной анализ, умственный труд, пытаются внедрить автоматизацию, но это вызывает лишь дополнительную нагрузку. Это мешает процессу обучения и обмена, поскольку знания и предыдущая деятельность остаются скрытыми и недоступными для других групп.
Сочетание слишком большого количества предупреждений, сложных расследований и слишком малого количества аналитиков приводит к проблеме ошибок из-за человеческого фактора, создает эффект снежного кома в дальнейшем. Из-за недостатка достоверной информации предупреждения делаются с ошибочным приоритетом, что приводит к увеличению объема работы для группы расследования инцидентов, которым требуется помощь группы быстрого реагирования для выполнения рабочей нагрузки.

3. Разрозненные инструменты со слишком узким фокусом

Увеличение арсенала инструментов является одним из способов решения множества проблем, позволяя принимать более быстрые и обоснованные решения, но инструментов слишком много. Большинство инструментов безопасности были разработаны для устранения конкретных технологических пробелов без учета того, как эти инструменты должны работать в операционной среде, и часто не соответствуют целям группы безопасности по обеспечению целостного видения и предотвращения инцидентов ИБ. При недостаточной интеграции с приемом данных только из одного источника, эти инструменты приносят ценность только для тех, кто имеет специализированные навыки в команде безопасности, и не предоставляют никакой ценности, и даже служат источником перегрузки, для других участников.

Некоторые инструменты эффективные, но при этом имеют ограничения:

- EDR может сократить время расследования для опытных групп реагирования на инциденты, но оно ограничено данными с конечных точек, на которых можно установить агент. Кроме того, EDR может резко увеличить объем предупреждений, что требует индивидуальной разработки для обеспечения базовой автоматизации, обременяя этим других участников команды.
- NTA требует правильного размещения датчика, чтобы избежать недостающего объема трафика, редко включает ответ и не включает данные от рабочей станции в качестве фактора обнаружения аномалий или расследования угроз.
- UEBA (User and Entity Behavior Analytics - анализ поведения пользователя и сущностей) в основном сосредоточен на данных из журнала и пропускает ключевые детали из глубокого анализа сетевого трафика, не говоря уже о рабочей станции и облачных ресурсах. Кроме того, при использовании UEBA наблюдается достаточно высокий уровень ложных срабатываний, что дополнительно увеличивает нагрузку на аналитиков.

Все эти использовании UEBA наблюдается достаточно высокий уровень ложных срабатываний, что дополнительно увеличивает нагрузку на аналитиков.

4. Круговорот рутины при расследованиях

Обнаружение сложных атак требует корреляции данных из любой точки цифрового пространства организации. Поскольку большинство инструментов, которые помогают обнаружению и реагированию, основаны только на одном источнике данных, например, рабочей станции, они пропускают важные сообщения из других не менее важных источников, оставляя команде безопасности выполнять тяжелую работу по проверке угроз. При работе в SOC типичной крупной организации, использующей более сорока инструментов, каждый из которых работает независимо, аналитики оказываются в режиме “дикого круговорота рутинных операций”: они переключаются с экрана на экран, пытаясь собрать воедино и сделать верные выводы из потока информации, чтобы они могли смягчить реальные угрозы. Если бы данные коррелировались, это могло бы обеспечить целостное представление об окружающей среде, но это потребовало бы нормализации, сопоставления даты/времени/события и понимания методов расследования во многих областях, таких как сети и рабочие станции. Это не простое дело, и сегодня это приходится делать вручную.

1. “Survey: 27 Percent of IT professionals receive more than 1 million security alerts daily,” Imperva, May 28, 2018, https://www.imperva.com/blog/2018/05/27-percent-of-it-professionals-receive-more-than-1-million-security-alerts-daily/.
2. “2017: Security Operations Challenges, Priorities, and Strategies,” ESG, March 2017, http://resources.siemplify.co/hubfs/PDF%20Downloads/ESG-Research-Insights-Report-Siemplify.pdf?hsCtaTracking=4303efc5-9f7b-4a8a-9438-263c0588b898%7C6043fb9a-2881-4940-9a0e-6239a8686b81.
3. “2017 Global Information Security Workforce Study,” Frost & Sullivan, accessed January 8, 2019, https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf.

5. Время — работает против вас

Величайшая ценность из всех — время. Чем быстрее будет выявлена угроза, тем больше шансов на её сдерживание. Пока команды борются с завалами из уведомлений, проблемами с ресурсами и отсутствием корреляции, они рискуют пропустить трудноопределимые важные предупреждения, которые становятся крупными инцидентами, им просто не хватает времени для поиска неизвестных угроз. В среднем, проходит более шести месяцев между тем, когда происходит утечка данных и тем, когда она впервые была идентифицирована,[4] и это "время задержки" увеличивается. Среднее время идентификации (MTTI) выросло со 190 дней в 2017 году до 197 дней в 2018 году, а время реагирования, измеряемое, как среднее время сдерживания (MTTC) — выросло с 66 дней в 2017 году до 69 дней в 2018 году.[5]

Все это происходит в то время, когда организации используют EDR, NTA и UEBA и всецело полагаются на SIEM, тратя почти 60% бюджета на безопасность.[6] Даже с помощью этих инструментов аналитики тратят значительное количество времени на задачи в ручном режиме, такие как написание запросов, сопоставление уведомлений с данными журнала и сбор информации из разных источников. Неудивительно, что при таком постоянном массиве работ лишь у немногих команд безопасности есть время сосредоточиться на критических задачах, таких как выявление сложных угроз, глубокое мышление и решение неявных проблем безопасности, которые даже умные программы и автоматизация не могут разгадать.

В SOC тоже нужны улучшения

Команде SOC нужен подход, который эффективно решает все вышеупомянутые проблемы. Это требует нового подхода, который может помочь SOC на всех стадиях операций — сортировка оповещений, расследование инцидентов, поиск угроз — чтобы помочь быстро завершить расследование, независимо от типа угрозы. С практической точки зрения идеальный подход должен:

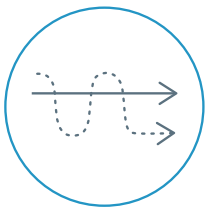
- Отслеживать активности в сети, на рабочих станциях и облаках для обнаружения инцидентов ИБ, сортировки оповещений, расследования и реагирования.
- Интегрироваться с инструментами, которые генерируют оповещения или предоставляют информацию для автоматического представления информации, получения выводов и даже принятия мер, где это возможно.
- Использовать аналитику в больших объемах для корреляции данных из всех источников, позволяя автоматически или вручную обнаруживать труднодоступные угрозы, охватывающие несколько источников данных, с небольшим количеством ложных срабатываний.
- Упростить исследования, чтобы помочь менее опытным аналитикам и уменьшить нагрузку на опытный персонал, резко улучшив время принятия решений на всех этапах операций SOC.
- Убедиться, что данные из каждого исследования могут быть быстро преобразованы материалы для улучшения защиты, например, путем добавления контекста к будущим расследованиям, уменьшения количества предупреждений и закрытия новых или известных уязвимостей.

Это значительно сократит среднее время обнаружения и реагирования на угрозы (время ожидания), а также поможет перевести команды безопасности от реагирования на предупреждения безопасности к проактивной защите сети.

XDR поднимает обнаружение и ответную реакцию на новый уровень

Palo Alto Networks внедряет прорывной подход к операциям безопасности путем повышения визуализации, а также скорости обнаружения угроз, расследования и принятия решений. Это называется XDR, эволюция обнаружения и реагирования. "X" означает любой источник данных, будь то сеть, рабочая станция или облако, с акцентом на увеличение производительности SOC с помощью автоматизации. Полная визуализация обеспечивает целостную картину деятельности организации, связывая данные из нескольких источников, так что более нет ручной корреляции данных и угрозам негде скрыться. Источники из внешних данных, таких как

Поиск скрытых угроз становится быстрее с помощью анализа сети, облачных технологий и конечных устройств



Упрощает расследования и реакцию на известные и неизвестные угрозы

Существенно улучшает процессы безопасности и ускоряет возврат инвестиций

Рисунок 3: Три ключевых преимущества XDR

4. "2018 Cost of a Data Breach Study," Ponemon Ins tute, May 2018, h ps://www-01.ibm.com/common/ssi/cgi-bin/ssialias?html d=55017055USEN&.
5. Ibid.
6. "Infographic: 2018 IT budgets are up slightly; spending focus is on security, hardware, and cloud," ZDNet, October 2, 2017, h ps://www.zdnet.com/ar cle/infographic-2018-it-budgets-are-up-slightly-spending-focus-is-on-security-hardware-and-cloud.

уведомления безопасности и глобальная аналитика угроз, объединяются чтобы было реальное понимание ситуации. Автоматизация объединяет критические данные на одном экране, делая выводы для аналитиков безопасности, и, делая за секунды то, что обычно занимает часы даже у сотрудников с многолетним опытом. В результате упрощаются расследования в рамках операций по обеспечению безопасности, сокращается время, необходимое для обнаружения, поиска, расследования и реагирования на любую форму угрозы.

XDR – решение новой эры эвристики, аналитики и моделирования, применения искусственного интеллекта и машинного обучения для быстрого обнаружения и предотвращения наиболее изощренных угроз. Отслеживая угрозы из любого источника или расположения в рамках инфраструктуры организации, XDR может автоматизировать защиту, отслеживание каждого шага атаки для восстановления четкой последовательности событий; применить аналитику угроз и закрыть пробелы в системе безопасности в будущем. Это ускоряет время принятия решений и освобождает аналитиков от чрезмерной нагрузки. Важно отметить, что XDR может поставляться в виде облачного приложения для простоты развертывания.

Преимущества XDR

XDR разработан для работы в SOC, что предопределяет три существенных преимущества: безграничный обзор, упрощение процессов безопасности и быстрый возврат инвестиций.

Безграничный обзор для быстрого обнаружения скрытых угроз

XDR выявляет аномальную активность путем сопоставления поведения пользователей, объектов и действий во всех источниках данных. Это снижает сложность поиска угроз за счет мощного поискового движка, точного определения источника угрозы и корреляции данных. XDR автоматизирует обнаружение текущие или прошлых угроз с помощью объединения и аналитики большого массива данных из конечных точек, сетевой активности, облачных данных и аналитических данных из прочих источников в SOC.

Упрощение процессов безопасности при расстановке приоритетов, расследовании и реагировании

XDR ускоряет и упрощает расследования, визуализируя цепочку действий любого события, чтобы автоматически выявить первопричины и предоставить улики для судебной экспертизы и всех аналитиков безопасности. Это устраняет ложные тревоги за счет сопоставления результатов расследования со всеми предупреждениями безопасности от всех технологий, что ускоряет работу менее опытных аналитиков. XDR реагирует на текущие угрозы и предотвращает будущие атаки пути согласованных действий внутри вашей сети, облаках и на рабочих станциях, освобождая аналитиков от рутинной работы и освобождая больше времени для обнаружения реальных угроз.

Быстрый возврат инвестиций

XDR усиливает команду безопасности, оптимизируя рабочие процессы, а также сокращая время на расстановку приоритетов уведомлений, расследования инцидентов, реагирования и принятия мер ИБ. Это позволяет разрозненным инструментам безопасности согласовано работать для автоматического решения проблем, используя полные данные и аналитику угроз. XDR усиливает защиту за счет применения знаний, получаемых в ходе каждого расследования, и предотвращая избыточные уведомления об аналогичных угрозах в будущем.

Преимущества XDR для SOC

XDR преобразует ваш подход по обеспечению безопасности из реактивного в проактивный, не только предотвращая, но и принимая превентивные меры. Полный обзор всех источников данных и правильная фокусировка на процессе, от расстановки приоритетов уведомлений до реагирования на угрозы, помогут существенно улучшить процессы безопасности.

Вы сможете оставить ложные уведомления в прошлом и не тратить время аналитиков на подобные события, дать возможность вашим аналитикам оперативно принимать верные решения, освободить ваших квалифицированных аналитиков от рутинной работы, дать команде быстрого реагирования возможность заниматься их профильной деятельностью и быть готовыми к угрозам любой сложности.

Используя возможности автоматизации XDR, Вы полностью раскрываете потенциал вашего SOC.
Если вы в поисках решения по обнаружению и реагированию на угрозы информационной безопасности, спросите вашего поставщика об XDR.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

redefine-security-operations-with-xdr-wp-012219