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:

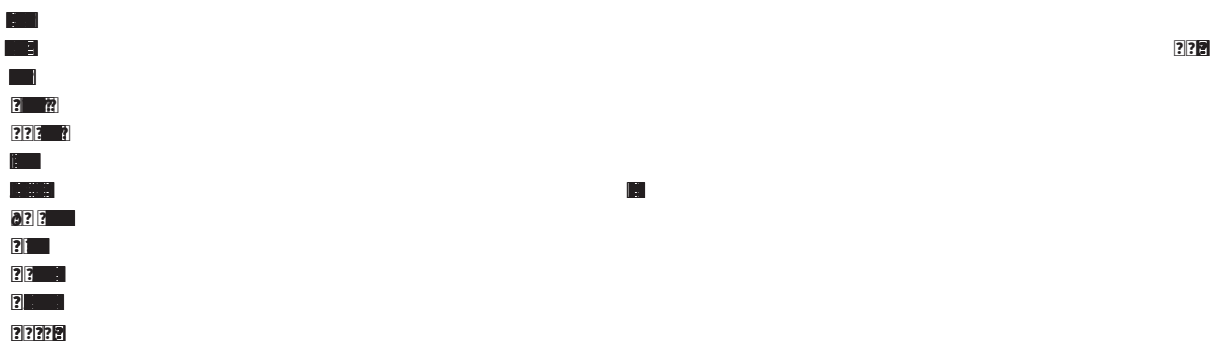
- Избыточное количество сообщений
- Слишком малое количество аналитиков безопасности
- Узконаправленные инструменты
- Отсутствие интеграции
- Нехватка времени

Рис. 2: Команды SOC сталкиваются с пятью основными проблемами

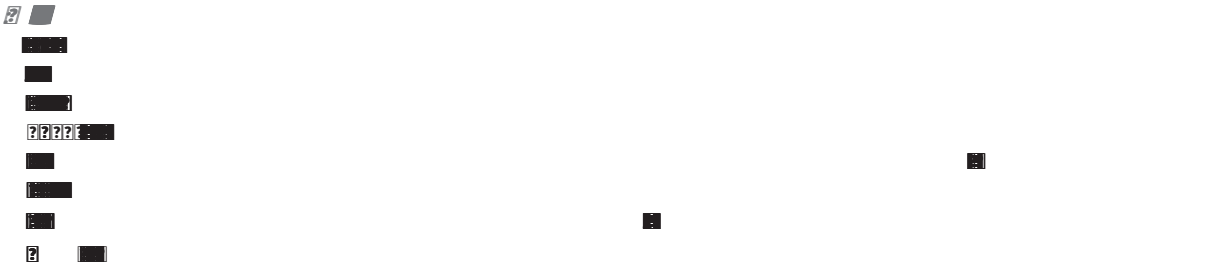
авайте рассмотрим каждую проблему в деталях.

1

2



3



- мо ет сократить время расследования для опытны р пп реа ирования на ин иденты но оно о рани ено данными с коне ны то ек на которы мо но становить а ент Кроме то о мо ет ре ко вели ить об ем пред пре дени то треб ет индивид ально ра работки для обеспе ения ба ово автомати а ии обременяя тим др и астников команды
- треб ет правильно о ра ме ения дат ика тобы и бе ать недостаю е о об ема тра ика редко вклю ает ответ и не вклю ает данные от рабо е стан ии в ка естве актора обнар ения аномали или расследования ро
- анали поведения поль ователя и с носте в основном сосредото ен на данны и рнала и проп скает клю евые детали и л боко о анали а сетево о тра ика не оворя е о рабо е стан ии и обла ны рес рса Кроме то о при исполь овании наблюдается достато но высоки ровень ло ны срабатывани то дополнительно вели ивает на р к на аналитиков

се ти исполь овании наблюдается достато но высоки ровень ло ны срабатывани то дополнительно вели ивает на р к на аналитиков

Кр оворот р тины при расследования

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.

ă. “SÄ³ÆXÉ: ĬŬ ;X³NX«º -Ƶ.A °³-ƵX´´ -«Jß´ ³XNX ÆX ª -³X º|J« ă ª ßß -« ´XNÄ³ ºÉ JßX³º´ TJ ßÉ,” . ª °X³ÆJ, 5 JÉ ĬЛ, ĬĂăЛ,
|À°´://ÇÇÇ. ª °X³ÆJ.N- ª /Mß-z/ĬĂăЛ/Ăð/ĬŮć°X³NX«ºć-Ƶć°º³-ƵX´´ -«Jß´ć³XNX ÆXć ª -³Xćº|J«ćăć ª ßß -«ć´XNÄ³ ºÉćJßX³º´ćTJ ßÉ/.

2. “2017: Security Opera ons Challenges, Priori es, and Strategies,” ES , March 2017, h p://resources.siemplify.co/hubfs/PDF 20Downloads/ES -Research-Insights-Report-Siemplify.pdf?hsCtaTracking=4303efc5- f7b-4a8a- 438-263c0588b8 8 7C6043 a-2881-4 40- a0e-623 a8686b81.

3. “2017 lobal Informa on Security orkforce Study,” Frost & Sullivan, accessed anuary 8, 201 , h ps://iamcybersafe.org/wp-content/uploads/2017/06/Europe- IS S-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:

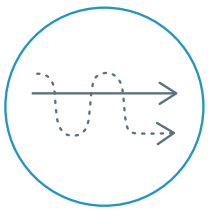
- Отслеживать активности в сети, на рабочих станциях и облаках для обнаружения инцидентов ИБ, сортировки оповещений, расследования и реагирования.
- Интегрироваться с инструментами, которые генерируют оповещения или предоставляют информацию для автоматического представления информации, получения выводов 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.