Cisco Stealthwatch

Масштабируемый мониторинг и аналитика безопасности

Возможно, вас взломали. Но как вы об этом узнаете?

Вы уже вложили значительные средства в ИТ-инфраструктуру и безопасность своей организации. Тем не менее успешные атаки случаются, а враждебно настроенные сотрудники внутри компании действуют безнаказанно. Кроме того, у вас уходят месяцы и даже годы на обнаружение угроз[1]. Мониторинг угроз оказывается неэффективным из-за растущей сложности сети и постоянно эволюционирующих атак. Специалисты по безопасности, обладая лишь ограниченными ресурсами и узкоспециализированными инструментами, мало что могут предпринять. Как убедиться, что имеющиеся средства контроля безопасности работают, управляются и настраиваются должным образом? И как узнать, выполняют ли они свою функцию?

Решение: сеть + безопасность

Метаданные сетевых пакетов могут давать полезную информацию о том, кто подключается к организации и с какой целью. Сеть охватывает все, поэтому аналитику можно распространить на головной офис, филиалы, общедоступное облако, частные центры обработки данных, пользователей в роуминге и даже Интернет вещей (IoT). Такой анализ данных может помочь обнаружить угрозы, способные обойти имеющиеся средства контроля, прежде чем эти угрозы нанесут серьезный ущерб. Кроме того, он позволяет выявлять подозрительное поведение враждебно настроенных сотрудников. И главное, эффективная аналитика снижает нагрузку на специалистов по безопасности, позволяя им сосредоточиться на более вероятных угрозах. Такой подход к обнаружению сложных угроз выглядит следующим образом.

Встроенный
с текущей инфраструктурой

Без использования агентов
и без необходимости развертывать повсюду датчики

Гибкость
развертывания и потребления: локальные и облачные системы, аппаратные и виртуальные устройства или SaaS

Уверенность в том, что существующая безопасность эффективна

С решением Cisco Stealthwatch вы получаете средства мониторинга в масштабе всего предприятия: от частной сети до общедоступного облака. В нем применяется расширенная аналитика безопасности, позволяющая обнаруживать угрозы и реагировать на них в режиме реального времени. Непрерывно анализируя активность в сети, решение получает базовые показатели стандартного поведения, а затем использует эти показатели и передовые алгоритмы машинного обучения для выявления в сети аномалий. Однако *необычное* не обязательно значит вредоносное. Stealthwatch может быстро и с высокой степенью точности проверять корреляцию аномалий с такими угрозами, как атаки с помощью систем управления и контроля, вирусы-вымогатели, DDoS-атаки, скрытый криптомайнинг, неизвестное вредоносное ПО и внутренние угрозы. Единое решение без использования агентов обеспечивает комплексный мониторинг угроз в центрах обработки данных, филиалах, на оконечных устройствах и в облаке, независимо от наличия в сети шифрования.

Преимущества

Контролируйте каждый хост. Узнавайте о каждом разговоре.

Отличайте нормальное от подозрительного. Получайте предупреждения об изменениях.

Реагируйте на угрозы оперативно.

- **Непрерывный мониторинг и обнаружение** сложных угроз, которые обходят имеющиеся средства контроля безопасности или возникают внутри компании.
- **Акцент на критические инциденты, а не шум** благодаря высокоточным уведомлениям с учетом контекста и приоритизации по критичности угроз.
- **Быстрое и эффективное реагирование** за счет полных сведений об активности угроз, журналов событий сети для ретроспективного анализа, а также интеграции с существующими средствами контроля безопасности.
- **Использование уже имеющихся ресурсов** ИТ-инфраструктуры и подробных данных телеметрии сети для более эффективной защиты.
- **Масштабирование защиты под растущие потребности бизнеса** по мере появления новых филиалов или центров обработки данных, переноса рабочих нагрузок в облако или просто добавления других устройств.
- **Обеспечение соответствия требованиям** с помощью уведомлений о нарушении политик, настраиваемых под логику работы компании.

1. Среднее время обнаружения проникновения составляет 197 дней согласно отчету Института Ponemon за 2018 г.

«Решение Cisco Stealthwatch помогло нам получить 100%-й мониторинг внутреннего трафика, позволив идентифицировать угрозы, которые было невероятно трудно обнаружить ранее».

ИТ-архитектор крупной компании в сфере промышленного производства

Следующие шаги

Для того чтобы узнать больше, зайдите на страницу https://www.cisco.com/c/ru_ru/products/collateral/security/stealthwatch/datasheet-c78-739398.html или обратитесь к представителю по работе с заказчиками Cisco в соответствующем регионе.

C45-736510-05 11/18

Контекстный мониторинг всей сети

Stealthwatch обеспечивает **мониторинг без использования агентов в масштабе всего предприятия**: как на территории организации, так и в любых общедоступных облачных средах. Предоставляя сведения о присутствии и активности пользователей в сети, решение также позволяет организациям внедрить **интеллектуальную сегментацию**, настроив ее в соответствии с логикой работы предприятия. Оно также предоставляет **оперативную аналитику**, обогащенную контекстом, то есть сведениями о пользователях, устройствах, местонахождении и приложениях, а также метками времени и другими данными.

Прогнозная аналитика угроз

Stealthwatch использует целый конвейер аналитических методов, позволяющих обнаруживать сложные угрозы до того, как они проникнут в сеть. Сначала решение выявляет аномалии, используя **анализ поведения в сети.** Затем эти аномалии анализируются сочетанием методов **машинного обучения с учителем и без учителя**, что обеспечивает обнаружение угроз с высокой точностью. За счет этого рабочая группа по безопасности может сосредоточиться на угрозах самой критической важности. Ядро аналитики безопасности Stealthwatch также поддерживает ведущую отраслевую **аналитику угроз Cisco Talos**, содержащую самые актуальные данные для корреляционного анализа локальных и глобальных угроз.

Автоматизированное обнаружение и реагирование

Мониторинг с учетом контекста в масштабе всего предприятия в сочетании с продвинутыми аналитическими методами помогает организациям обнаруживать такие угрозы, как **неизвестное или зашифрованное вредоносное ПО, внутренние угрозы, нарушения политики,** то есть все, что вызывает «тревожные сигналы». Специалисты по безопасности могут просматривать **уведомления с приоритизацией по критичности угроз** и получать дополнительную информацию, чтобы легко принимать меры. Stealthwatch также поддерживает хранение телеметрии в масштабе и предоставляет журналы событий сети для **ретроспективного анализа** прошлых событий и **мониторинга соответствия требованиям.** Наконец, решение интегрируется с уже имеющимися у вас средствами контроля безопасности, позволяя реагировать на любые угрозы без прерывания бизнес-процессов.

Улучшение безопасности за счет анализа зашифрованного трафика

Быстрый рост объемов зашифрованного трафика меняет ландшафт угроз. Хотя шифрование помогает в обеспечении безопасности и защите конфиденциальных данных, оно также создало для киберпреступников возможность скрывать вредоносное ПО и избегать обнаружения. Gartner прогнозирует, что к 2019 году 80 % всего веб-трафика будет зашифрованным и 70 % атак будут использовать шифрование. Расшифровка такого трафика для анализа не оправдывает затрат, а в скором времени с внедрением TLS 1.3 она вообще станет невозможна. Компания Cisco представила революционную технологию **Encrypted Traffic Analytics (ETA)**, поддерживаемую Stealthwatch и сетью Cisco нового поколения, которая позволяет анализировать зашифрованный трафик без какой-либо расшифровки. С ее помощью организации могут: 1) обнаруживать угрозы в зашифрованном трафике; 2) проверять соответствие требованиям криптографии, чтобы знать, какой объем цифровых бизнес-данных использует стойкое шифрование, и выявлять нарушения политик. Для получения дополнительной информации зайдите на страницу https://www.cisco.com/go/eta.