Система анализа сетевого трафика для обеспечения безопасности сети

Милановић Евгений Александрович, студент магистратуры;
Селезнёв Игорь Львович, доцент
Белорусский государственный университет информатики и радиоэлектроники (г. Минск)

Одним из эффективных методов обеспечения безопасности сетей, являются методы анализа сетевого трафика. Анализ сетевого трафика (АСТ) — это процесс перехвата, записи и анализа шаблонов передачи сетевого трафика с целью выявления угроз безопасности и реагирования на них. Первоначально предложенный компанией «Gartner», этот подход привел к появлению новой категории продуктов для обеспечения безопасности сетей.

Отличие анализа сетевого трафика от других средств организации сетевой безопасности.

В то время как другие инструменты сетевой безопасности, такие как брандмауэры и системы обнаружения несанкционированного доступа и системы предотвращения несанкционированного доступа [1], ориентированы на мониторинг вертикального трафика, который пересекает периметр сетевой среды, решения для анализа сетевого трафика сосредоточены на всех коммуникациях — независимо от того, являются они традиционными пакетами TCP/IP, «виртуальный сетевой трафик», пересекающий виртуальный коммутатор (или «vSwitch»), трафик из облачных рабочих мест и внутри них и вызовы API для приложений SaaS (software as a service) или экземпляров локальных вычислений. Эти решения также фокусируются на операционных технологиях и интернете вещей (IoT) [2], которые в остальном полностью невидимы для группы безопасности. Современные инструменты АСТ эффективны даже при шифровании сетевого трафика.

Первое поколение этой технологии было направлено на установление критериев того, что является «нормальным» или «хорошим», а затем выявляло аномалии, которые могут быть «нерегулярными» или «плохими». Например, эти решения пытаются выявить аномалии, такие как «Этот IP обычно не видит соединений из Китая. Предупредите, если будет такая связь». Этот подход имеет обратную сторону — появление большого количества предупреждающих сообщений в следствии быстрого развития бизнеса и информационных технологий. Усовершенствованные инструменты АСТ работают более разумным образом, сравнивая работу системы не только с прошлым поведением, но и с другими объектами в окружающей среде. Другие улучшения также описаны в перечне ключевых характеристик ниже.

Важность анализа сетевого трафика.

Злоумышленники постоянно изменяют свою тактику, чтобы избежать обнаружения и часто используют легитимные учетные данные к доверенным инструментам, уже развернутым в сетевой среде, что затрудняет для организаций упреждающее выявление критических угроз безопасности. Продукты для анализа сетевого трафика появились в ответ на постоянные инновации злоумышленников, предлагая организациям реалистичный путь борьбы с новыми видами атак.

Кроме того, благодаря широкому распространению облачных вычислений, процессов DevOps и IoT, поддержание эффективной видимости сети стало очень сложным и громоздким процессом. Продукты АСТ могут служить для организаций единственным «источником правды» [3], определяющим реальное содержимое данных, полученных из сети.

Основные функции анализа сетевого трафика.

Наиболее эффективные и современные решения в области анализа сетевого трафика включают нижеперечисленные ключевые характеристики.

1. **Широкая видимость** — независимо от того, являются ли рассматриваемые сетевые коммуникации традиционными пакетами в стиле TCP/IP, виртуальный сетевой трафик, пересекающийся с vSwitch, трафик из облачных рабочих нагрузок и внутри него, вызовы API для приложений SaaS или экземпляры локальных вычислений, инструменты АСТ могут контролировать и анализировать широкий спектр сообщений в режиме реального времени.
2. **Анализ зашифрованного трафика** — поскольку зашифрованный веб-трафик составляет более 75 процентов [4], организациям необходим доступный метод для расшифровки сетевого трафика без нарушения конфиденциальности данных. Решения АСТ устраняют эту проблему, позволяя специалистам по безопасности выявлять сетевые угрозы, анализируя всю полезную нагрузку, фактически не заглядывая в нее.
3. **Отслеживание объектов** — продукты АСТ предоставляют возможность отслеживать и определять все объекты в сети, включая устройства, пользователей, приложения, пункты назначения и многое другое. Следующим шагом машинное обучение и аналитика связывают поведение и отношения с именованными объектами, предоставляя организациям гораздо большую ценность, чем статический список IP-адресов.
4. **Обширный базовый уровень —** чтобы идти в ногу с постоянно меняющимися современными ИТ-средами, решения АСТ отслеживают поведение, уникальное для объекта или небольшого числа объектов, по сравнению с большей частью сущностей в окружающей среде. Исходные данные доступны немедленно, и базовые показатели машинного обучения АСТ развиваются в режиме реального времени по мере изменения поведения. Благодаря возможностям отслеживания объектов базовые показатели АСТ являются еще более полными, поскольку они могут понимать устройства источника и получателя назначения в дополнение к шаблонам трафика. Например, то, что может быть нормальным для рабочей станции, не является нормальным для сервера, IP-телефона или камеры.
5. **Обнаружение и реагирование** — поскольку инструменты АСТ приписывают поведение объектам, для рабочих процессов обнаружения и реагирования доступен достаточный контекст. Это означает, что специалистам по безопасности больше не нужно просеивать информацию через несколько источников данных, таких как журналы DHCP и DNS, базы данных управления конфигурациями и инфраструктуру службы каталогов, чтобы увидеть полную картину. Вместо этого они могут быстро обнаруживать аномалии, выслеживать их, определять основную причину и реагировать соответствующим образом.

Последующие перспективы анализа сетевого трафика.

Особенно значимой технологию анализа сетевого трафика делает ее способность объединять свои основные возможности для обнаружения злоумышленных намерений. До появления продуктов АСТ обнаружение злонамеренных действий представляло собой длительный, не поддающийся воспроизведению процесс, требующий высокой квалификации, а специалисты по безопасности вынуждены были вручную искать аномалии, чтобы их можно было использовать в качестве шаблона для автоматизации работы систем безопасности с помощью стека технологий безопасности. Например, в то время как довольно просто реализовать такое правило, как «Оповещать меня, если соединение происходит из страны, с которой мы еще не сталкивались», гораздо труднее автоматизировать такое правило, как, «Оповещать меня, если кто-то подключается к этому сервер базы данных, а затем передает данные в 2 раза или более исторически среднего объема».

Благодаря автоматизации процесса выявления злоумышленных намерений, передовые решения АСТ снижают барьер навыков и усилий, который мешает многим организациям эффективно защитить свои наиболее важные активы. Возможность обнаружения на основе правил инструментов АСТ также позволяет большему количеству организаций искать конкретные тактики, методы и процедуры защиты от сетевых атак. Поскольку сами правила легко определить и они автоматически коррелируют между объектами, временем, протоколами и другими соответствующими параметрами, специалисты по безопасности могут искать последовательности событий в течение недель или месяцев, сопоставляя их с известной цепочкой атакующего преступника, или структурой, такой как матрица MITER ATT & CK [5].

Наиболее многообещающим аспектом решений АСТ является тот факт, что они позволяют организациям адаптировать технологию в соответствии с уникальными нюансами и потребностями любой конкретной сети. Это позволяет специалистам в области безопасности осуществлять индивидуальное обнаружение угроз, характерных для конкретной организации, без необходимости привлечения опытных команд по обработке данных или необходимости изменять обучающие наборы или алгоритмы.

Литература:

1. Миланович, Е. А. Актуальные уязвимости в системах контроля доступа // Молодой ученый. — 2019. — № 44. — с. 88–91.
2. Что такое интернет вещей? // РБК. URL: https://www. rbc. ru/trends/industry/5db96f769a7947561444f118

3. The Network Does Not Lie! Entity data and relationships that you»re missing today // AWAKE. URL: https://awakesecurity.com/blog/network-does-not-lie/
4. Шифрование интернет-соединения по протоколу HTTPS // Отчет о доступности сервисов и данных. URL: https://transparencyreport. google. com/https/overview.
5. MITRE ATT&CK. URL: https://attack. mitre. org