УДК 004 **Информационные технологии**

Ермаков Глеб Сергеевич, *студент военного учебного центра Российского Технологического Университета МИРЭА, РФ, г. Москва*
Спиридонов Александр Сергеевич, *студент военного учебного центра Российского Технологического Университета МИРЭА, РФ, г. Москва*
Пантелеев Николай Николаевич, *преподаватель военного учебного центра, «Цикл связи» РТУ МИРЭА, РФ, г. Москва*

СИСТЕМЫ АНАЛИЗА СЕТЕВОГО ТРАФИКА КАК КОМПОНЕНТ ЗАЩИТЫ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

Аннотация: В данной работе исследуются системы анализа сетевого трафика (NTA) как ключевой элемент обеспечения информационной безопасности сетевой инфраструктуры. Освещается использование NTA для мониторинга и анализа данных, выявления сложных угроз, обнаружения вредоносных программ и контроля соблюдения политик безопасности. Рассматривается роль NTA в рамках работы центров мониторинга и реагирования на инциденты информационной безопасности (SOC) и их вклад в снижение рисков безопасности и повышение устойчивости организаций к сетевым атакам. Статья подчеркивает значимость NTA для администрирования и выявления нелегитимной активности, что способствует более эффективной защите информационных ресурсов.

Ключевые слова: Сетевой анализ трафика, Информационная безопасность, Обнаружение угроз, SOC, NTA-системы.

Annotation: This work investigates Network Traffic Analysis (NTA) systems as a key component in ensuring the information security of network infrastructure. It highlights the use of NTA for monitoring and data analysis, identifying complex threats, detecting malware, and controlling security policy compliance. The role of

NTA within Security Operation Centers (SOC) is examined, along with their contribution to reducing security risks and enhancing the resilience of organizations to network attacks. The article emphasizes the significance of NTA in administration and the detection of illegitimate activity, which aids in more effective protection of information resources.

Keywords: Network Traffic Analysis, Information Security, Threat Detection, SOC, NTA Systems.

Системы анализа сетевого трафика (NTA – Network Traffic Analysis) – это класс защитных решений, ориентированных на комплексный анализ сетевого трафика как на периметре, так и внутри инфраструктуры [1].

Данные системы обладают возможностью перехватывать потоки данных, выявлять признаки комплексных, часто целенаправленных атак, а также предоставлять обширные данные для глубокого ретроспективного анализа сетевых инцидентов и активностей злоумышленников в рамках сетевой инфраструктуры организации.

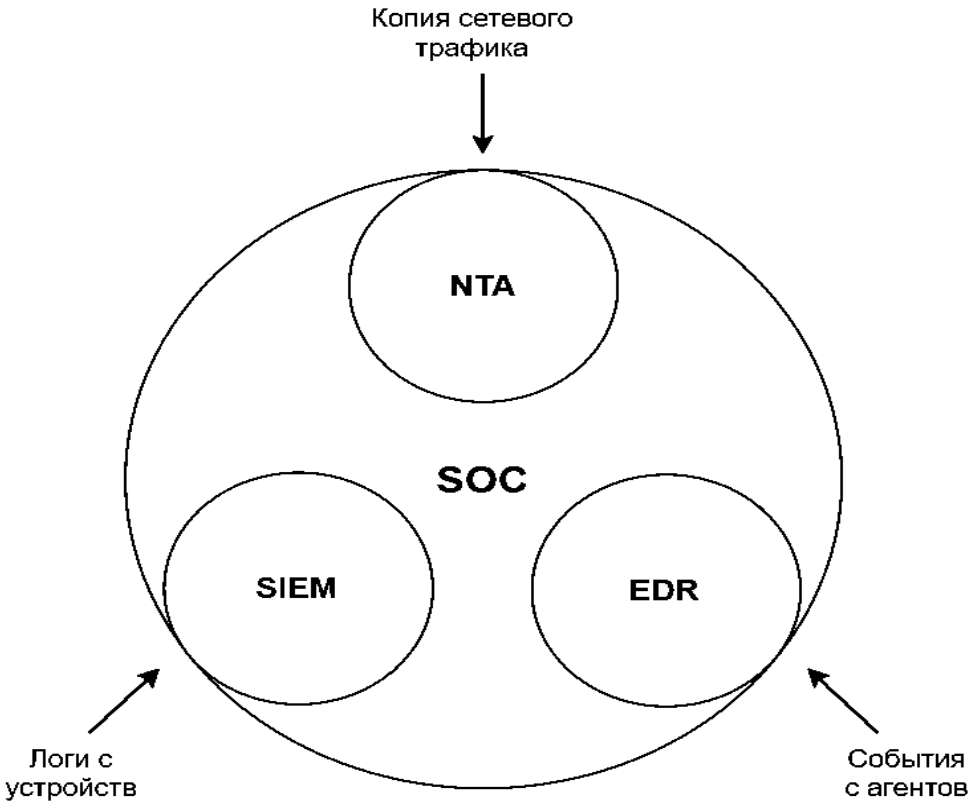

Рис. 1 – Три столпа центра мониторинга и реагирования

NTA системы являются неотъемлемой частью работы центра мониторинга и реагирования на инциденты информационной безопасности (SOC – Security Operations Center), выполняя критически важную роль в обеспечении защиты, обнаружении угроз и снижении рисков безопасности. Использование таких систем позволяет не только своевременно реагировать на текущие угрозы, но и анализировать прошлые инциденты для улучшения стратегий безопасности и повышения устойчивости организации к будущим атакам.

Отличным решением для подобной системы будет ее установка в режиме зеркалирования сетевого трафика с использованием пакетного брокера, как показано на рисунке ниже. Мало того, что такой вариант невероятно удобен в администрировании, но также позволит централизованно обрабатывать весь собираемый сетевой трафик и снизит нагрузку на инфраструктуру.

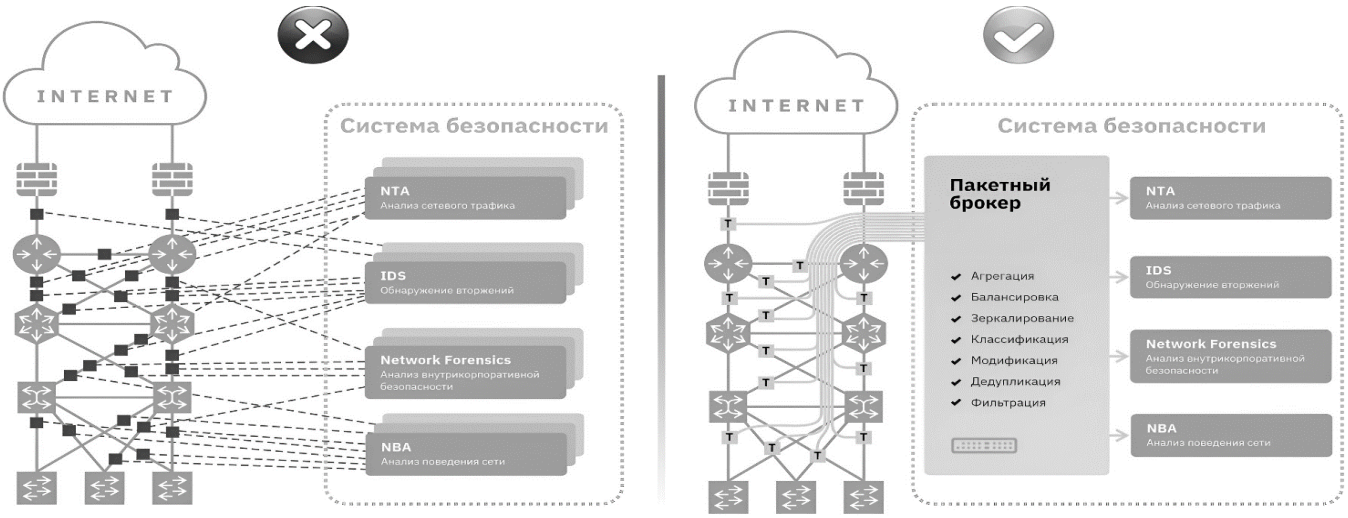

Рис. 2 – Варианты размещения NTA системы

Основными функциями системы анализа сетевого трафика являются:

1. Мониторинг трафика:

- *Сбор данных* – сбор сырых данных трафика для анализа;
- *Визуализация* – предоставление графических представлений трафика для лучшего понимания и анализа.

2. Анализ трафика:

- *Детекция аномалий* – выявление необычных паттернов трафика, которые могут указывать на атаки или другие проблемы с безопасностью;
- *Классификация трафика* – разделение трафика на категории по различным критериям (например, по типу приложения или протоколу).

3. Обнаружение и предотвращение угроз

- *IDS/IPS* – интеграция с системами обнаружения и предотвращения вторжений для реагирования на угрозы в реальном времени.
- *Анализ содержимого/DPI* – проверка содержимого пакетов на наличие вредоносного кода или других угроз.

4. Отчетность и аудит

- *Логирование* – сохранение данных о трафике для последующего анализа и аудита.
- *Отчеты по безопасности* – создание отчетов о состоянии

безопасности сети [1].

Стоит отметить, что системы анализа сетевого трафика также позволяют получать дополнительную информацию, необходимую для эффективного распределения нагрузки по сетевым каналам, что способствует оптимизации производительности всей сети. Помимо этого, данный инструмент позволяет обеспечить соответствие указанным политикам безопасности и требованиям законодательства. Администраторы могут настраивать правила доступа и следить за их соблюдением, предотвращая несанкционированный доступ к ресурсам сети и обеспечивая защиту от внешних и внутренних угроз.

Ключевые компоненты системы анализа сетевого трафика:

1. Сборщик трафика (сенсор) – это устройство или программа, которая непосредственно захватывает пакеты данных, проходящие через сеть. Без сборщика трафика система NTA не сможет получить доступ к данным трафика для анализа.

2. Анализатор трафика – является ядром системы, которое обрабатывает захваченные данные, проводит их анализ, выявляет аномалии, классифицирует трафик и выполняет другие задачи аналитики. Без анализатора трафика собранные данные останутся необработанными и не будут иметь практической пользы.

3. Хранилище данных – место, где сохраняются захваченные и обработанные данные. Хранилище данных необходимо для долгосрочного хранения информации, что позволяет проводить анализ трафика за длительные периоды времени и вести аудит сетевой активности.

4. Пользовательский интерфейс – этот компонент предоставляет администраторам и аналитикам инструменты для взаимодействия с системой, просмотра результатов анализа, настройки параметров системы и получения уведомлений о событиях в сети. Без интерфейса пользователя работа с системой NTA была бы крайне затруднена или даже невозможна. Часто представлен в виде веб-решения [2].

Что способна обнаружить система анализа сетевого трафика:

1. Детектирование аномалий – системы анализа сетевого трафика (NTA) интегрированно отслеживают аномалии в поведении сетевого трафика, латеральные перемещения и несанкционированный доступ. Путём мониторинга необычных соединений и доступов, которые отличаются от установленного профиля поведения, NTA системы помогают выявлять и реагировать на продвинутые угрозы и потенциальные нарушения безопасности в реальном времени.

2. Выявление подозрительного шифрованного трафика – поскольку большой объем вредоносного трафика теперь использует шифрование для маскировки, NTA системы применяют методы, такие как анализ метаданных и исследование характеристик трафика, чтобы выявлять подозрительную активность, даже если само содержимое не может быть просмотрено.

3. Распознавание распределенных атак – системы NTA эффективно идентифицируют аномалии в объемах и паттернах трафика, что может указывать на широкий спектр распределенных сетевых атак. Мониторинг синхронизированных действий между множеством источников трафика помогает своевременно выявлять и противостоять таким угрозам.

4. Обнаружение ВПО – NTA системы могут идентифицировать поведение, обычно связанное с вредоносными программами, такими как частое обращение к известным командным серверам, необычные паттерны передачи данных или подозрительная активность в периоды минимального использования сети.

5. Контроль соблюдения политик – NTA системы могут отслеживать соблюдение политик безопасности, обнаруживая действия, такие как использование неразрешенных приложений, передача данных на внешние устройства или доступ к запрещенным веб-сайтам.

6. Применение интеллектуального анализа данных – используя сложные алгоритмы и базы данных угроз, NTA системы могут анализировать сетевые события для обнаружения шаблонов, характерных для хакерских кампаний, фишинговых атак и других угроз безопасности [2; 3].

Заключение: Как можно понять из перечисленных выше возможностей, NTA системы – это крайне мощный инструмент для администрирования и выявления нелегитимной активности в сетевой инфраструктуре, источник которой могли пропустить средства защиты периметра сети. Функционал таких систем значительно улучшает условия работы специалистов центра мониторинга информационной безопасности, предоставляя им значительное количество информации о происходящем в защищаемой ими сетевой зоне.

Библиографический список:

1. Системы анализа сетевого трафика (NTA) — обзор мирового и российского рынка (электронный ресурс) // URL: https://www.anti-malware.ru/analytics/Market_Analysis/Global-and-Russian-market-Network-Traffic-Analysis-systems-review (дата обращения 25.10.2023).

2. Внедрение. Электронный курс "PT NAD: базовая архитектура, особенности установки" (PT-NAD-CS) (электронный ресурс) // URL: https://edu.ptsecurity.com/mira/#&id0=10&type0=usergmlist&name0=Курсы+и+тесты&step0=1&id1=14&type1=usergmlist&name1=PT+NAD&step1=2&id2=89&type2=usergmlist&name2=Электронные+курсы+PT+NAD&step2=3&doaction=Go&step=5&id=2513&type=studentcourse&pathlength=3 (дата обращения 25.10.2023).

3. PT Network Attack Discovery (электронный ресурс) // URL: https://www.ptsecurity.com/ru-ru/products/network-attack-discovery/#resources (дата обращения 25.10.2023).