positive technologies

PT Network Attack Discovery

Раннее выявление угроз и сложных целевых атак
Экспертное расследование по копии сетевого трафика

ПРЕИМУЩЕСТВА

Показывает злоумышленников во всей сети

Выявляет хакерский инструментарий и модифицированное вредоносное ПО

Помогает выполнить требования к защите информации, в том числе к безопасности объектов КИИ и финансовых операций

Интегрируется с решениями класса SIEM и sandbox

Быстрая инсталляция. Меньше 1 часа на внедрение в промышленную эксплуатацию

PT Network Attack Discovery — система анализа сетевого трафика (network traffic analysis, NTA) для контроля вредоносной активности на периметре и внутри сети. Это удобный инструмент для расследований, который обнаруживает активность злоумышленников даже в зашифрованном трафике. PT NAD знает, что искать в сети.

Проверка сетевой активности

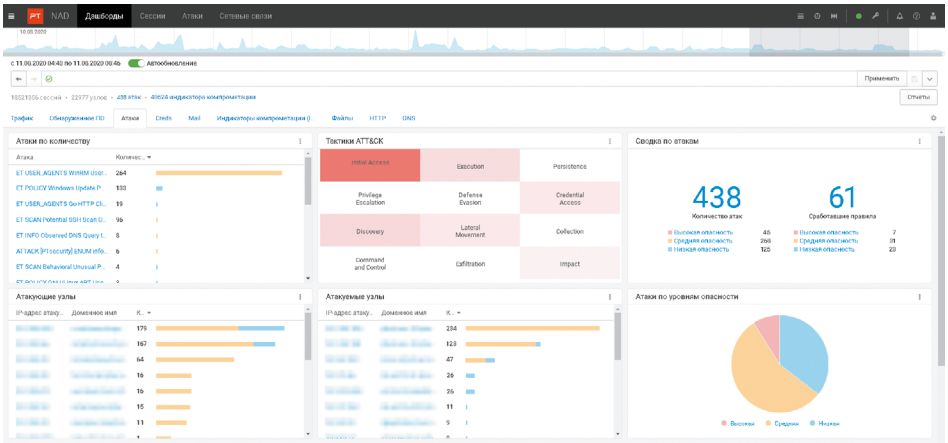
PT NAD определяет более 100 сетевых протоколов и 9 протоколов туннелирования и разбирает 35 наиболее распространенных из них до уровня L7 включительно. На основе разбора и анализа более 1200 параметров протоколов строятся модели сетевых узлов. Это позволяет получить подробную картину активности в инфраструктуре и выявить проблемы ИБ, которые снижают эффективность системы безопасности и способствуют развитию атак. PT NAD знает все о каждом сетевом узле, минимизирует использование неконтролируемых компонентов ИТ-инфраструктуры и снижает риск взлома компании через них.

Обнаружение сложных целевых атак

Система автоматически обнаруживает попытки проникновения в сеть и присутствие злоумышленников в инфраструктуре по множеству признаков, например по примененным инструментам или по данным, переданным на серверы атакующих.

Необходимый инструмент SOC

PT NAD — незаменимый источник данных для SIEM-решений. Система хранит метаданные и сырой трафик, позволяет оперативно находить сессии и отбирать подозрительные, экспортировать и импортировать трафик. Таким образом PT NAD гарантирует полную видимость сети для SOC, упрощает проверку успешности атаки, помогает восстановить хронологию и собрать доказательную базу.



На дашборде оператор получает детальную информацию о подозрительной активности. Это помогает оперативно реагировать на инциденты и проводить расследования

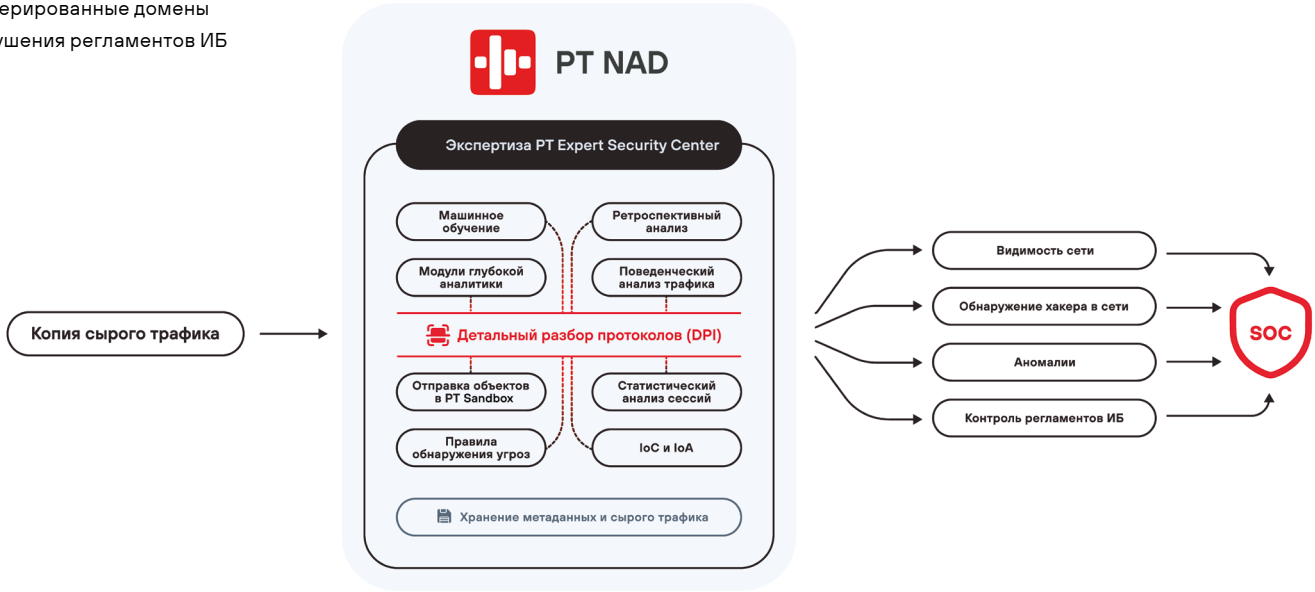
А как атакуют вашу компанию? Проверьте свою сеть и периметр — закажите бесплатную пилотную версию PT NAD на сайте.

PT NAD ВЫЯВЛЯЕТ:

- Угрозы в зашифрованном трафике
- Применение хакерского инструментария
- Перемещение злоумышленника внутри периметра
- Сетевые аномалии
- Зараженные сетевые узлы
- Атаки на контроллер домена
- Признаки не обнаруженных ранее атак
- Эксплуатацию уязвимостей в сети
- Признаки сокрытия активности от средств защиты
- Автоматически сгенерированные домены
- Нарушения регламентов ИБ

Сценарии применения

- **Мониторинг сетевой безопасности.** PT NAD помогает обнаружить ошибки конфигурации и нарушения регламентов ИБ, например незавершенные сеансы, словарные пароли, использование утилит для удаленного доступа или инструментов для сокрытия сетевой активности.
- **Выявление атак на периметре и в инфраструктуре.** Встроенные модули глубокой аналитики, собственные правила детектирования угроз, индикаторы компрометации и ретроспективный анализ позволяют отследить атаки на ранних стадиях и после проникновения злоумышленника в инфраструктуру.
- **Расследование атак.** Оператор ИБ отслеживает атаки и определяет их успешность на основе анализа метаданных. Специалист по расследованию восстанавливает хронологию атаки с помощью данных в PT NAD и вырабатывает компенсирующие меры.
- **Поиск угроз.** PT NAD помогает выстроить процесс threat hunting в организации, проверять гипотезы, например о присутствии хакеров в сети, и выявлять скрытые угрозы, которые не обнаруживаются стандартными средствами кибербезопасности.



Как работает PT NAD

PT NAD захватывает и разбирает сетевой трафик на периметре и в инфраструктуре с помощью собственной технологии DPI. В качестве источника трафика можно использовать устройства TAP, брокеры сетевых пакетов и активное сетевое оборудование. Анализируя копию сетевого трафика статистическими и поведенческими модулями, система определяет активность злоумышленника на самых ранних этапах проникновения в сеть, а также во время попыток закрепиться и развить атаку внутри сети. PT NAD хранит копию сырого трафика и на его основе генерирует метаданные для ретроспективного анализа. После обновления правил обнаружения угроз и репутационных списков от PT Expert Security Center продукт автоматически перепроверяет собранные данные о трафике и сообщает аналитикам SOC о скрытом присутствии злоумышленника в сети. Сочетая в себе несколько механизмов обнаружения сложных угроз, PT NAD обеспечивает видимость сети компании, обнаруживает подозрительные соединения и сетевые аномалии и помогает контролировать регламенты ИБ.

ptsecurity.com
pr@ptsecurity.com

Positive Technologies — ведущий разработчик решений для информационной безопасности. Уже 21 год наша основная задача — предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии и сервисы используют более 2900 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400».

Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI).

Следите за нами в соцсетях (Telegram, ВКонтакте, Twitter, Хабр) и в разделе «Новости» на сайте ptsecurity.com, а также подписывайтесь на телеграм-канал IT's positive investing.

PT-NAD_PB_A4.RUS.0032.23.MAY.10.2023