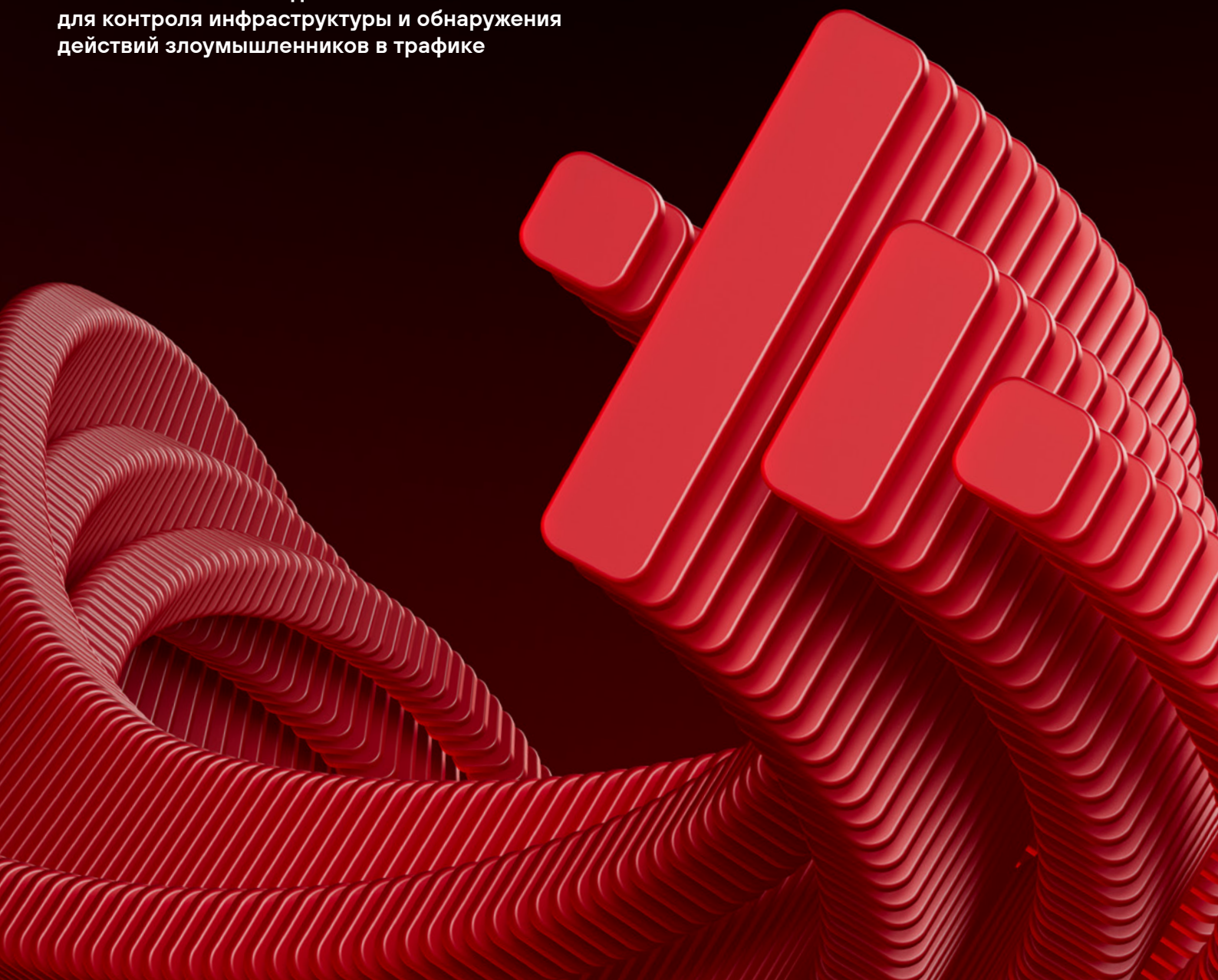
positive technologies

PT Network Attack Discovery

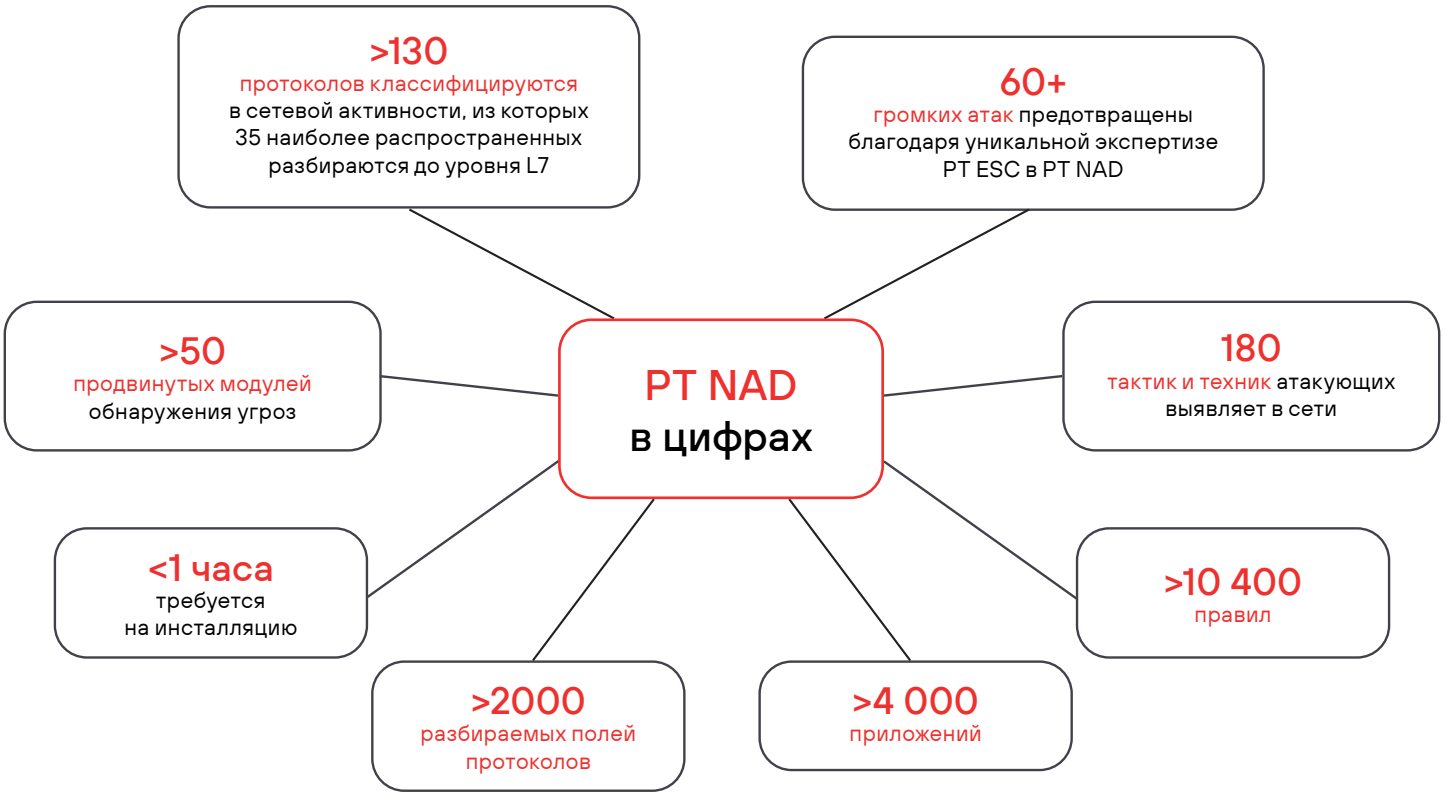
Эталонный источник данных о сети для контроля инфраструктуры и обнаружения действий злоумышленников в трафике



PT Network Attack Discovery — система поведенческого анализа сетевого трафика для выявления скрытых кибератак. Точно обнаруживает действия злоумышленников в сети, упрощает расследование инцидентов и помогает в проактивном поиске угроз.

Зачем анализировать трафик

- Сеть видит все — хакер не может обойти средства анализа трафика и скрыть в нем следы присутствия.
- Минимальные требования — достаточно копии трафика, не нужно устанавливать агенты или вмешиваться в инфраструктуру.
- Независимость от параметров узлов — эффективность анализа не снижается из-за отключенного аудита или некорректной настройки серверов и рабочих станций.
- Выявление угроз на неизвестных узлах — PT NAD обнаруживает атаки на неучтенные устройства (например, на теневые ИТ-ресурсы).



PT NAD знает, что искать

Быстро и точно определяет действия злоумышленников в сети на ранних этапах атаки

Видит точки проникновения в инфраструктуру и масштаб атаки в режиме, близком к реальному времени

Защищает георапределенные инфраструктуры любого масштаба

Центральная консоль обеспечивает возможность централизации процесса анализа сетевого трафика, гарантируя надежную защиту в условиях нехватки кадров

Является незаменимым инструментом для ретроспективного анализа и расследований

Технология DPI детально разбирает сетевой трафик на любых скоростях — данные используются для автоматического обнаружения аномалий и ручного анализа. Позволяет выявлять угрозы, которых нет в базах данных сигнатур IDS, IPS и NGFW

Оперативно выявляет угрозы, актуальные для российских компаний

Экспертный центр PT ESC поставляет индикаторы компрометации, правила, поведенческие и статистические модули, нацеленные на выявления атак, популярных на территории России

PT NAD на практике

Use case № 1. Предотвращение многоэтапной кибератаки и захвата домена

Проблема

Злоумышленник провел сложную атаку на организацию, состоящую из нескольких этапов, среди которых:

1. Взлом периметра: эксплуатация уязвимостей на веб-сервере Apache для получения первоначального доступа.
2. Создание туннеля: установка туннеля (с помощью Chisel) к C2-серверу злоумышленника для скрытого управления.
3. Разведка сети: активное сканирование внутренней сети инструментом nmap для выявления критически важных активов, включая контроллер домена.
4. Подбора учетных данных: проведение атаки Password Spraying с помощью crackmapexec для получения доступа по WinRM.
5. Расширение доступа: использование Evil-WinRM для входа на внутренний узел с подобранными учетными данными.
6. Захват домена: проведение атаки PetitPotam с целью получения прав администратора домена. Сеть полностью скомпрометирована.

Решение

PT NAD выявил все ключевые этапы атаки в режиме реального времени:

1. Обнаружил аномалии и сигнатуры эксплуатации уязвимостей Apache на периметре.
2. Выявил подозрительную сетевую активность и сигнатуры, характерные для работы туннелирующего инструмента Chisel.
3. Зафиксировал сканирующую активность nmap внутри сети.
4. Обнаружил множественные попытки аутентификации, характерные для Password Spraying (crackmapexec).
5. Идентифицировал использование инструмента Evil-WinRM для удаленного доступа.
6. Выявил сетевые сигнатуры атаки PetitPotam на контроллер домена.

На каждом этапе PT NAD генерировал детализированные алерты для службы безопасности (SOC), предоставив полную картину kill chain.

Результат

- Своевременное реагирование: служба ИБ получила преимущество во времени.
- Предотвращение эскалации: обнаружение Password Spraying и использования Evil-WinRM позволило заблокировать скомпрометированные учетные записи и изолировать зараженный узел до проведения атаки PetitPotam.
- Сохранение контроля: захват домена и полная компрометация сети были предотвращены.
- Форензика: подробные данные от PT NAD стали основой для расследования инцидента, устранения уязвимостей и укрепления защиты.

Use case № 2. Обнаружение и нейтрализация атак нулевого дня

Проблема

Киберзлоумышленники атаковали российскую компанию через две неизвестные (0-day) уязвимости в системе видео-конференц-связи VINTEO:

1. Уязвимость внедрения SQL-кода (9,8 балла по шкале CVSS 3.0).
2. Уязвимость удаленного выполнения кода (8,1 балла по шкале CVSS 3.0), дающая злоумышленнику полный контроль над сервером без авторизации.

Решение

Специалисты Positive Technologies с помощью PT NAD:

1. В режиме реального времени обнаружили аномальную активность в сетевом трафике.
2. Зафиксировали и проанализировали трафик атаки, идентифицировав уязвимости нулевого дня.
3. В течение 10 часов подтвердили инцидент и передали данные для реагирования.

Результат

- Разработчик VINTEO оперативно выпустил патч, закрыв уязвимости.
- Заражение других компаний предотвращено благодаря оперативному реагированию.
- В PT NAD и PT NGFW были обновлены правила для автоматического обнаружения и блокировки подобных атак.

Кейс основан на реальном инциденте 2024 года.

Детали

PT NAD способен выявить злоумышленника с любым уровнем подготовки

Благодаря наличию разнообразных методов анализа трафика PT NAD обеспечивает надежную защиту от злоумышленника независимо от его компетенции и ресурсов на проведение атаки.

Сценарии использования PT NAD

- Контроль соблюдения регламентов ИБ
- Обнаружение теневой инфраструктуры
- Выявление атак и аномалий в сети
- Расследование атак
- Обнаружение некорпоративных ОС и ПО
- Проверка сетевых узлов
- Обнаружение средств удаленного администрирования
- Проактивный поиск угроз
- Инвентаризация информационных потоков

Проверьте свою сеть, оставьте заявку на бесплатный тест-драйв

Подписывайтесь на телеграм-канал PT NAD и получайте ответы на вопросы, а также самые свежие новости о продукте