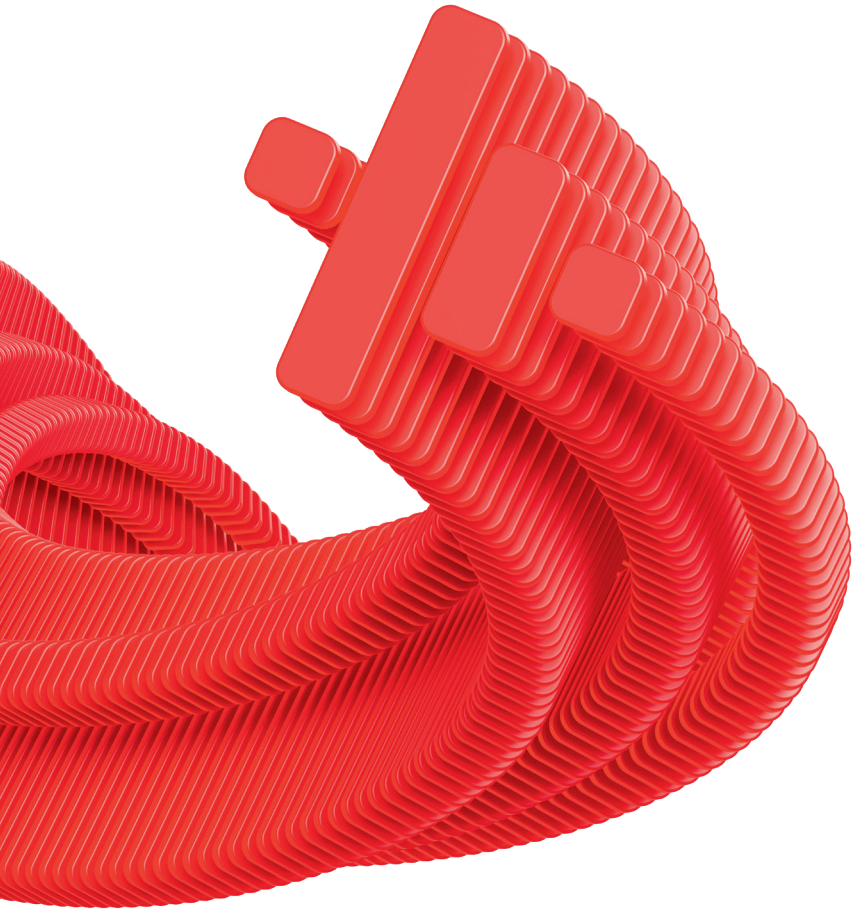
positive technologies

PT Network Attack Discovery



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

PT NAD знает, что искать

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.

Эталон среди NTA-решений

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

За счет объединения восьми методов обнаружения угроз (в том числе уникальных) видит точки проникновения в инфраструктуру и масштаб атаки в режиме, близком к реальному времени

Незаменимый инструмент для ретроспективного анализа и расследований

Технология DPI позволяет детально разбирать 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 выявление атак, распространенных на территории России. Защищает внутренние сети крупных компаний из разных отраслей

Сценарии применения

Выявление атак в инфраструктуре, профилирование сетевых узлов

- PT NAD находит аномалии и отклонения от типичного для конкретной инфраструктуры поведения с помощью ML-модели, самообучающейся на трафике компании
- Встроенные модули глубокой аналитики и собственные правила детектирования угроз позволяют отследить атаки на ранних стадиях и после проникновения в инфраструктуру

Расследование атак

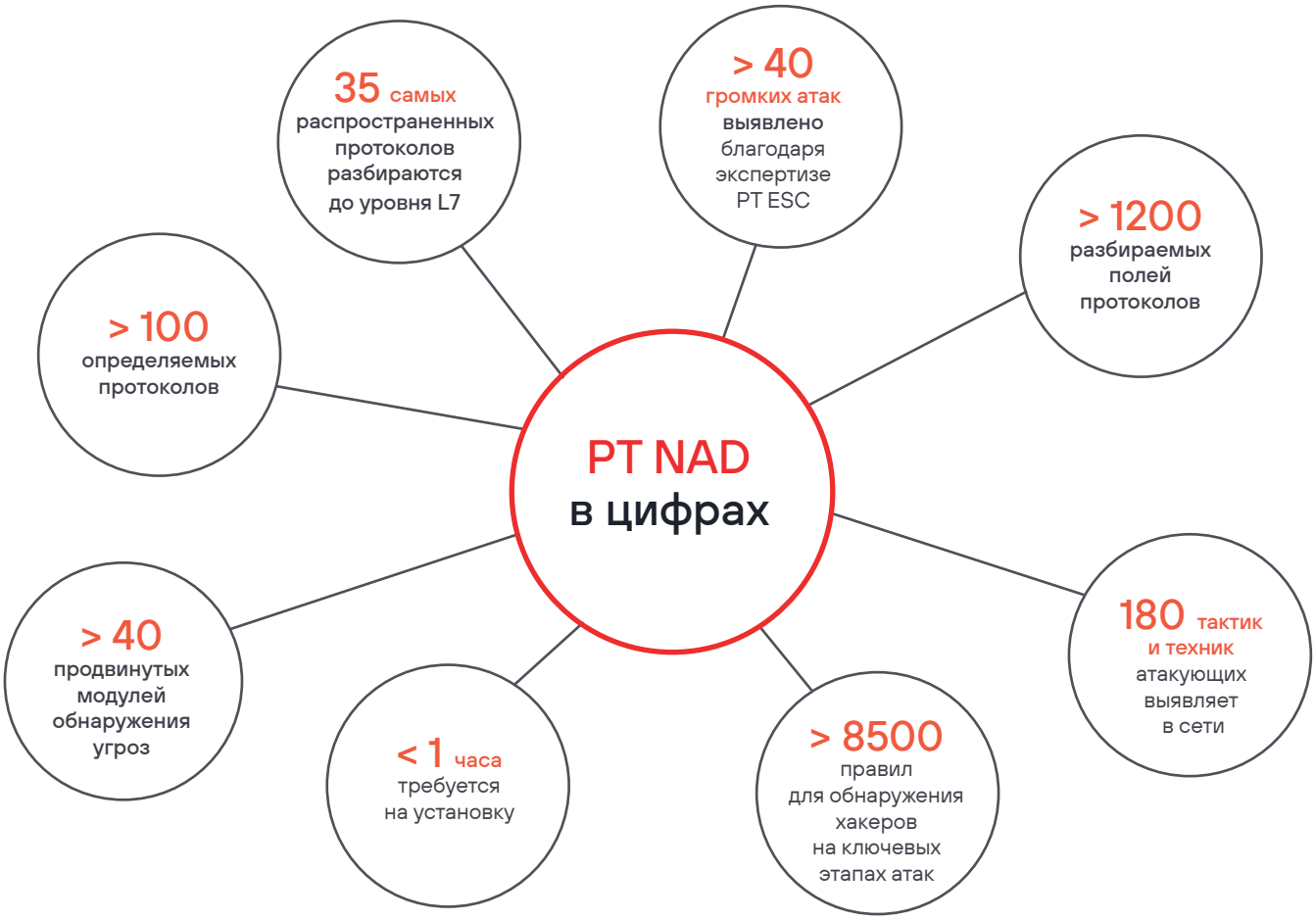
- PT NAD выявляет атаки и аномалии, а оператор определяет их успешность на основе собранных данных
- Специалист по расследованию восстанавливает хронологию атаки с помощью данных из PT NAD и вырабатывает компенсирующие меры

Проактивный поиск угроз

- PT NAD помогает выстроить в компании процесс threat hunting — проверять гипотезы (например, о присутствии хакеров в сети) и выявлять скрытые угрозы, которые не обнаруживают стандартные средства информационной защиты

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)



Чтобы получить более детальную информацию, оставьте заявку.

Подписывайтесь на телеграм-канал PT NAD — получайте ответы на вопросы и самые свежие новости о продукте.