POSITIVE TECHNOLOGIES

PT Network Attack Discovery

Анализирует трафик. Выявляет атаки.
Незаменим в расследованиях.

ПРЕИМУЩЕСТВА

Видит активность
злоумышленников
во внутреннем трафике

Выявляет даже
модифицированное
вредоносное ПО

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

Интегрируется
с решениями класса SIEM
и антивирусными системами

А КАК АТАКУЮТ ВАШУ КОМПАНИЮ?

Проверьте свою сеть
и периметр — закажите
бесплатный «пилот»
PT NAD на сайте:

PT Network Attack Discovery — система глубокого анализа сетевого трафика (network traffic analysis, NTA) для выявления атак на периметре и внутри сети. PT NAD знает, что происходит в сети, обнаруживает активность злоумышленников даже в зашифрованном трафике и помогает в расследованиях.

Дает понимание, что происходит в сети

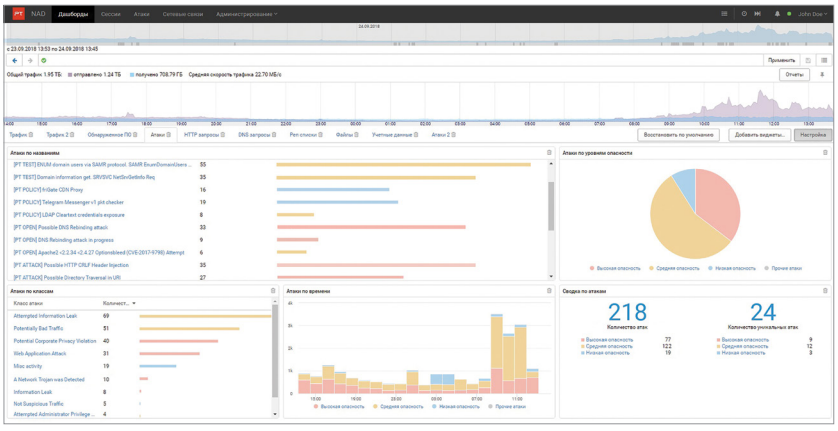
PT NAD определяет более 50 протоколов, разбирает до уровня L7 включительно 30 наиболее распространенных из них. Это позволяет получить подробную картину активности в инфраструктуре и выявить проблемы в ИБ, которые снижают эффективность системы безопасности и способствуют развитию атак.

Обнаруживает скрытые угрозы

Система автоматически обнаруживает попытки злоумышленников проникнуть в сеть и их присутствие в инфраструктуре по множеству признаков, например применение хакерских инструментов или передачу данных на сервер атакующих.

Повышает эффективность работы SOC

PT NAD дает SOC полную видимость сети, упрощает проверку успешности атаки, помогает восстановить хронологию и собрать доказательную базу. Для этого он хранит метаданные и сырой трафик, позволяет оперативно находить сессии и отбирать из них подозрительные, экспортировать и импортировать трафик.



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

PT NAD ВЫЯВЛЯЕТ:

- Угрозы в зашифрованном трафике
- Применение хакерского инструментария
- Горизонтальное перемещение злоумышленника
- Активность вредоносного ПО
- Признаки атак, не обнаруженных ранее
- Эксплуатацию уязвимостей в сети
- Признаки сокрытия активности от средств защиты
- Автоматически сгенерированные домены
- Нарушения регламента ИБ

Сценарии применения

Мониторинг сетевой безопасности

PT NAD помогает обнаружить ошибки конфигурации и нарушения регламентов ИБ, например учетные записи в открытом виде, нешифрованные почтовые сообщения, использование утилит для удаленного доступа или инструментов для сокрытия сетевой активности.

Выявление атак на периметре и в инфраструктуре

Встроенные технологии машинного обучения, глубокая аналитика, собственные правила детектирования угроз, индикаторы компрометации и ретроспективный анализ позволяют детектировать атаки как на ранних стадиях, так и когда злоумышленник уже проник в инфраструктуру.

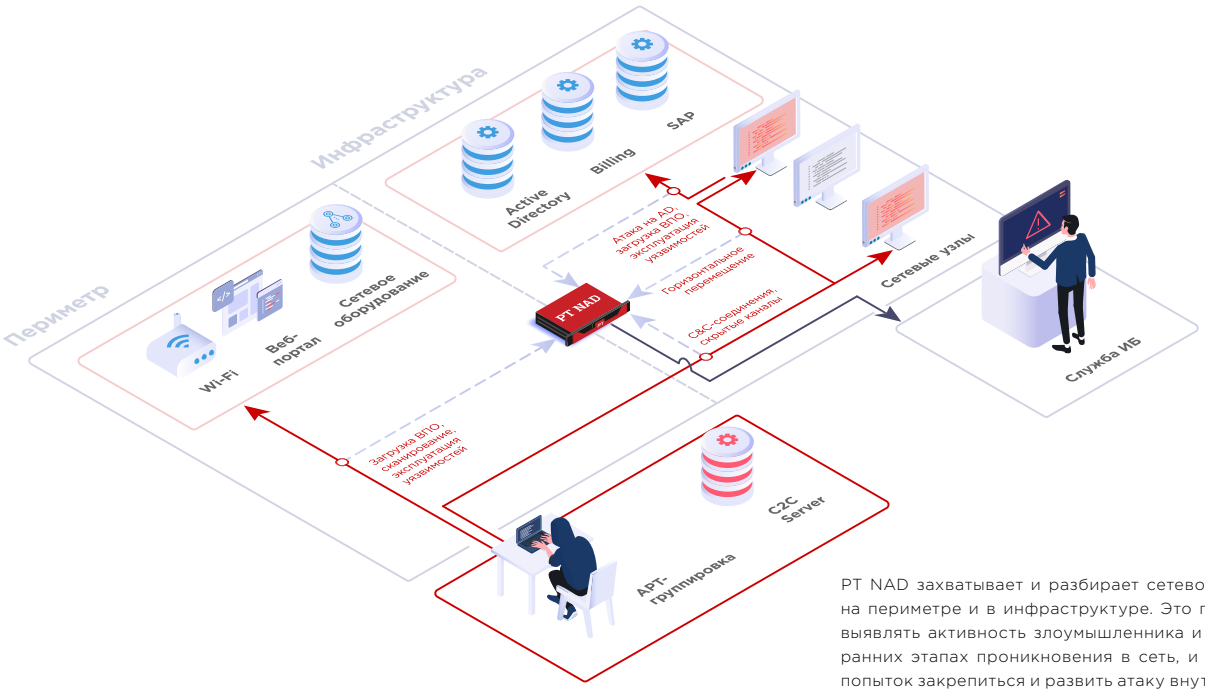
Расследование атак

Оператор ИБ отслеживает атаки и, анализируя метаданные, делает вывод об их успешности. Специалист по расследованию восстанавливает хронологию атаки с помощью данных в PT NAD и вырабатывает компенсирующие меры.

Threat hunting

PT NAD помогает выстроить процесс threat hunting в организации, проверять гипотезы, например о присутствии хакеров в сети, и выявлять даже скрытые угрозы, которые не обнаруживаются стандартными средствами кибербезопасности.

Как работает



PT NAD захватывает и разбирает сетевой трафик на периметре и в инфраструктуре. Это позволяет выявлять активность злоумышленника и на самых ранних этапах проникновения в сеть, и во время попыток закрепиться и развить атаку внутри сети.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.

ptsecurity.com
pt@ptsecurity.com

facebook.com/PositiveTechnologies
facebook.com/PHDays