

Автоматизированное сдерживание угроз в PT NAD

От обнаружения до изоляции — все в одной карточке



Автоматизированное сдерживание угроз в PT NAD позволяет операторам SOC сразу изолировать узлы и блокировать атакующего



Аналитик видит атаку и может сразу произвести действия по автоматизированному сдерживанию



Все действия реализуются прямо из карточки атаки, активности или узла — не нужно переходить в сторонние системы

Скорость

Время от обнаружения до сдерживания сокращается до минимума

Единое окно

Действие запускается там же, где аналитик уже работает с трафиком и атаками

Сеть и хост

PT NAD находит то, что видно на уровне сети и сразу изолирует на хосте

Обратимость

Есть возможность журналировать действие по инциденту и отменить его при необходимости

Доступные механизмы для автоматизированного сдерживания в PT NAD

Через MaxPatrol EDR



PT NAD



Responder



MaxPatrol EDR

- Изоляция узла на сетевом уровне
- Изоляция узла на уровне адаптера
- Блокировка учетной записи

EDR

Через External Dynamic Lists (EDL)



PT NAD



EDL

- Блокировка по IP-адресу
- Блокировка по DNS-имени
- Перенаправление DNS-запросов (sinkholing)

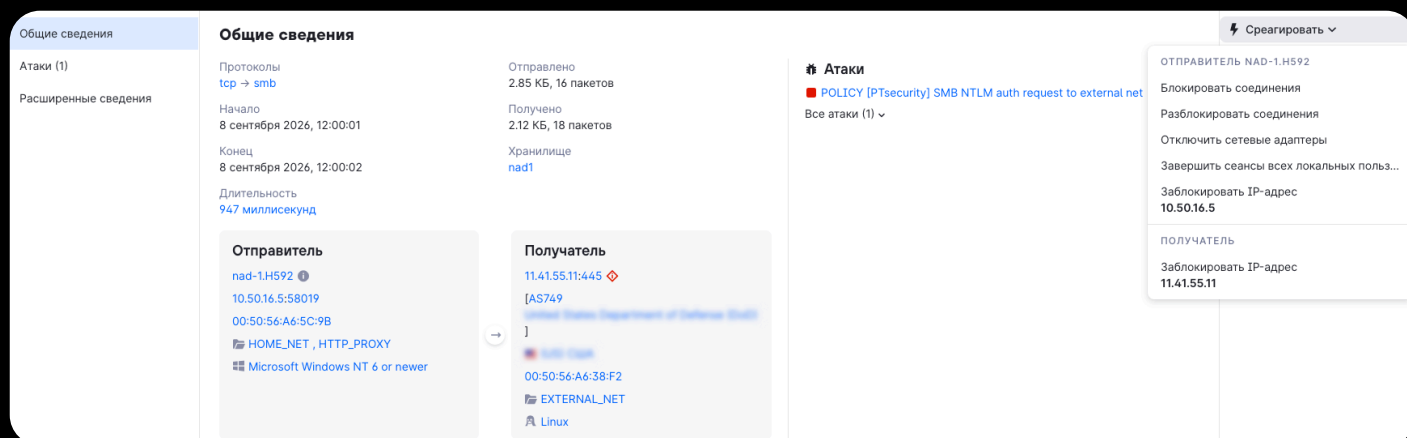
EDL



Хотите увидеть сдерживание в действии?
Покажем сценарий на демонстрации или на вашей инфраструктуре

Оставьте заявку на сайте

Быстрое реагирование на угрозы в два клика: доступно из карточек узла, активности, сессии или атаки с помощью нажатия кнопки «Среагировать»



Как это работает

- 1 Аналитик открывает карточку атаки, активности или узла
- 2 Нажимает «Среагировать»
- 3 Выбирает нужный сценарий
- 4 Действие применяется
- 5 Все фиксируется в журнале
- 6 При необходимости действие можно отменить из того же интерфейса

Сдерживание угроз в сети — важный этап цикла реагирования на инциденты

В PT NAD этот процесс максимально оптимизирован: все необходимые действия выполняются в два клика непосредственно из карточек узла, активности, сессии или атаки, без переключения между консолями

Преимущества для оператора

-  Сокращение времени на сдерживание угрозы
-  Для активных действий достаточно иметь доступ только в PT NAD
-  Возможность предоставления прав для сдерживания только тем, кому они необходимы
-  Приведение инфраструктуры к исходному состоянию после устранения угрозы



Хотите увидеть сдерживание в действии?
Покажем сценарий на демонстрации или на вашей инфраструктуре

Оставьте заявку на сайте

