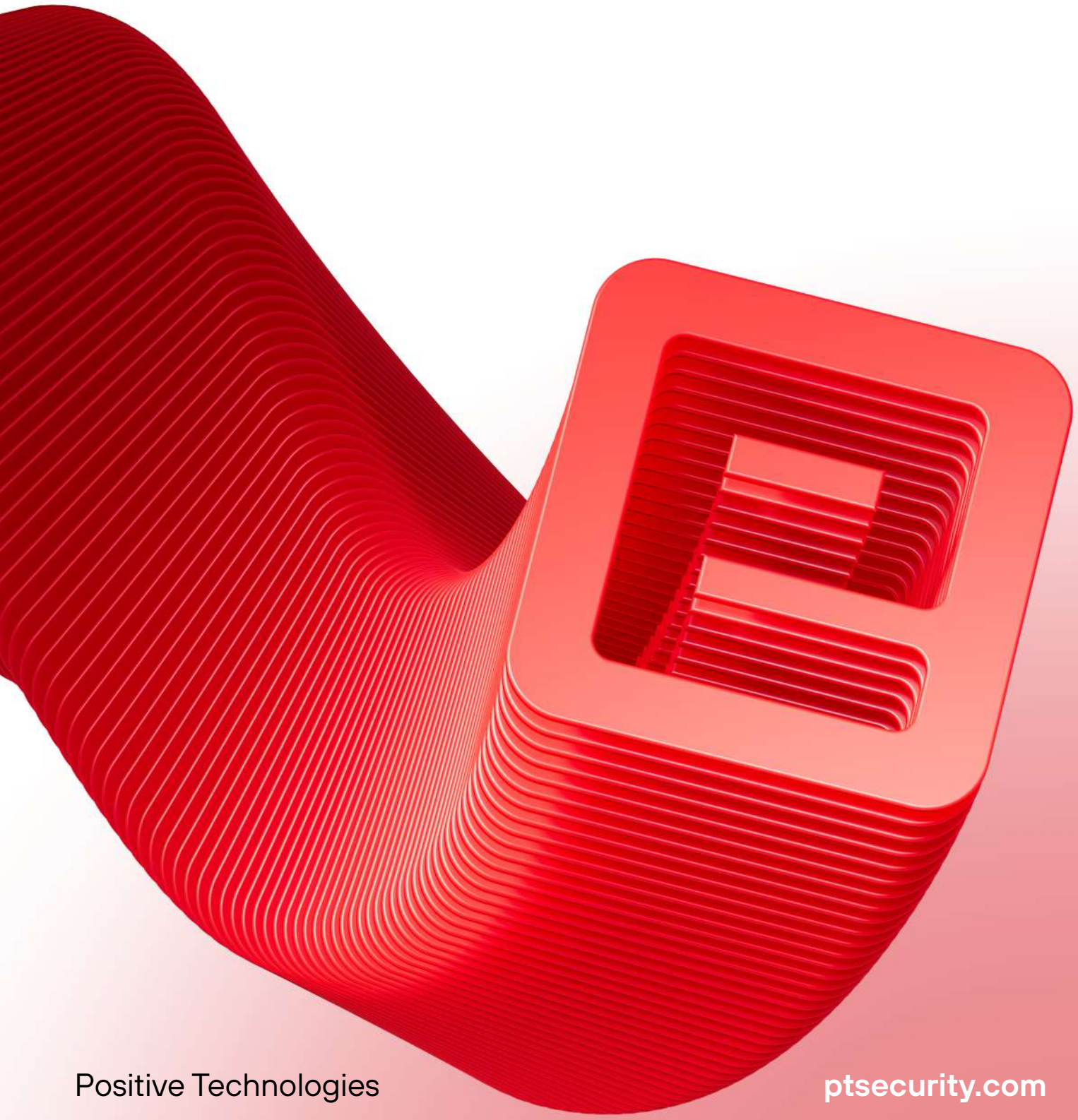
Сценарии использования продукта



Positive Technologies

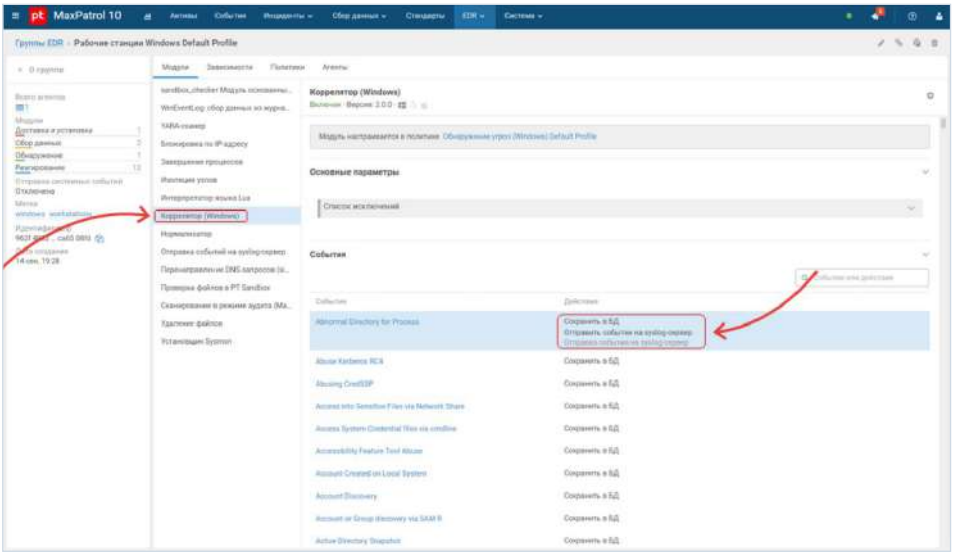
ptsecurity.com

Выявление и расследование сложных атак

Злоумышленники постоянно совершенствуют свои инструменты и техники. Чтобы обойти традиционные средства защиты, вредоносное ПО маскирует свои действия под легитимные. Для обнаружения APT-угроз на конечных устройствах важно уметь выявлять эксплуатацию уязвимостей, повышение привилегий, разведку, закрепление в системе и другие тактики и техники атакующих.

MaxPatrol EDR:

- Выявляет сложные атаки на ранних этапах с помощью динамического и статического анализа.
- Маркирует обнаруженные техники атакующих в соответствии с матрицей MITRE ATT&CK.
- Передает файлы для глубокой проверки в PT Sandbox и другие внешние системы.



Остановка вредоносных действий

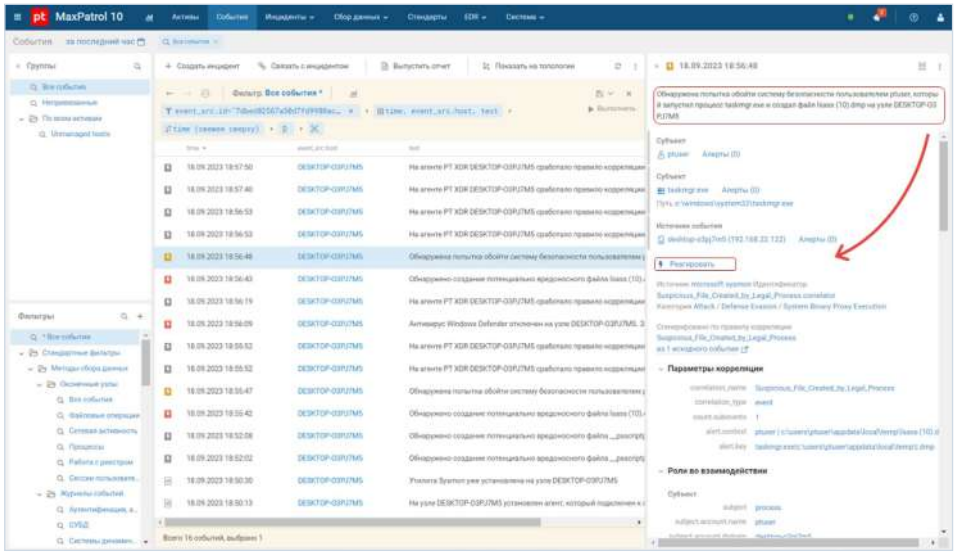
Продвинутые атаки выполняются в несколько этапов, и прежде чем инфраструктуре будет нанесен реальный ущерб, может пройти много времени.

MaxPatrol EDR:

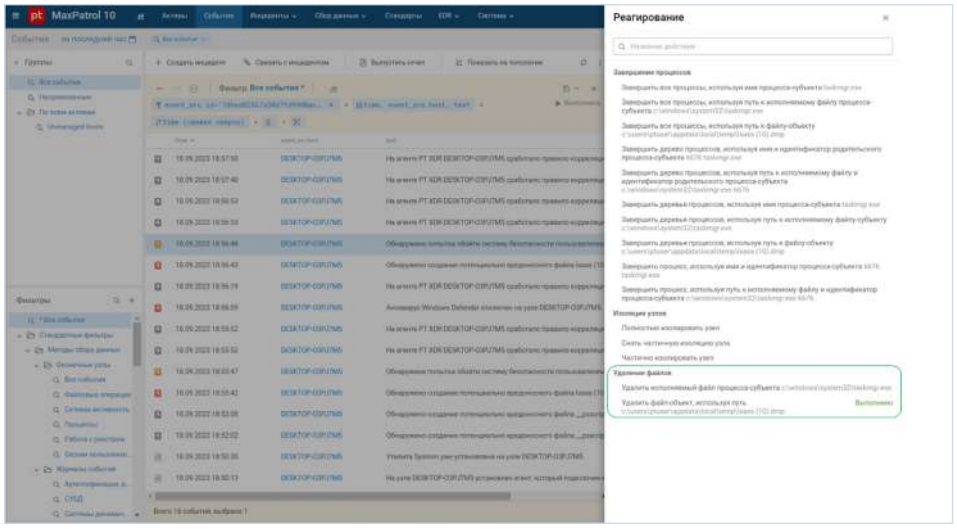
- Обнаруживает угрозы на ранних этапах и может реагировать на них до того, как злоумышленники реализуют недопустимое событие.
- Позволяет реагировать на угрозы в ручном или автоматическом режиме.

- Позволяет гибко настраивать правила реагирования, исходя из потребностей организации и задач SOC.
- Дает богатый выбор действий реагирования — для обеспечения необходимого уровня безопасности на серверах и рабочих станциях:
  - изолирование узлов;
  - завершение процессов;
  - удаление вредоносных файлов;
  - блокировка опасных подключений;
  - дополнительный анализ подозрительных процессов.

Реагирование прямо из события



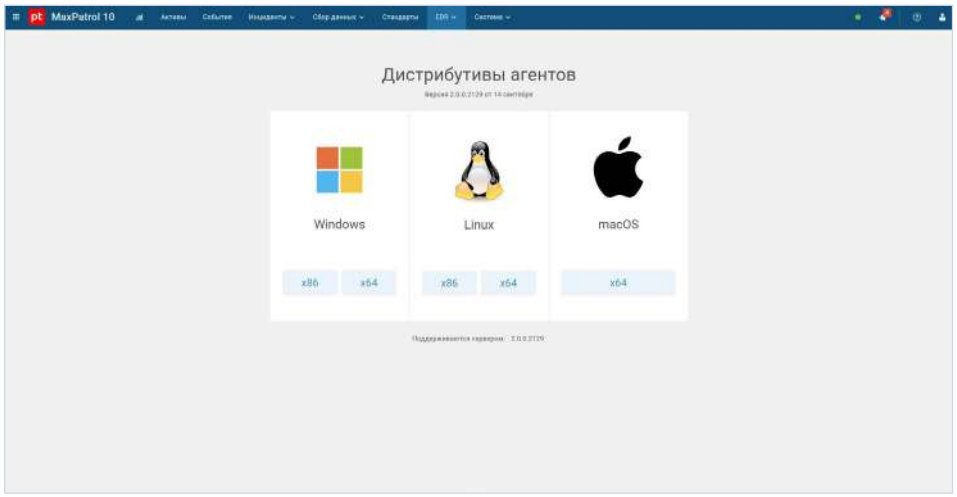
Результат реагирования



Защита узлов на базе отечественных ОС

Большинство организаций используют в инфраструктуре комбинацию операционных систем: Windows, macOS, ОС на базе Linux. Злоумышленники знают, как атаковать каждую из них. Они портируют вредоносное ПО под различные системы и постоянно ищут новые уязвимости.

С помощью MaxPatrol EDR можно защищать все популярные ОС, включая отечественные. При этом развернуть агенты легко: все необходимые дистрибутивы под рукой, в удобной единой веб-консоли, а также есть инструменты группового администрирования.



Аудит рабочих станций для поиска уязвимостей

Управление уязвимостями на конечных устройствах — важный процесс, требующий слаженной работы двух подразделений. Специалисты по ИБ обнаруживают уязвимости на серверах, рабочих станциях и на ноутбуках удаленных сотрудников и определяют, какие следует устранить в первую очередь. IT-специалисты имплементируют результат анализа, внедряют патчи и вносят изменения в конфигурацию систем. На эффективность этого взаимодействия влияют технические и организационные сложности, особенности процессов внутри компании.

Использование MaxPatrol EDR позволяет:

- разгрузить сетевой сканер;
- снизить задержки при повторном сканировании;
- обеспечить быструю обратную связь об устранении уязвимостей;
- отказаться от выделения специальных учетных записей для проведения аудита.

Обнаружение угроз в закрытых IT-сегментах

MaxPatrol EDR содержит всю необходимую экспертизу для самостоятельного устранения угроз. Продукт не полагается на данные из внешних источников или репутационные базы. Это возможно за счет применения поведенческого анализа, коррелятора на узлах и постоянного обновления правил от PT Expert Security Center.

Возможности MaxPatrol EDR:

- Автономная работа агентов: анализ и реагирование без обращения к серверу управления.
- Поставка обновлений экспертизы в закрытые сегменты сети без доступа в интернет (через промежуточный сервер для односторонней передачи данных).