Юрий Бережной

Руководитель направления
по развитию защиты конечных
устройств Positive Technologies

Многообразие современных вредоносов

Как они обходят традиционные СЗИ и что этому противопоставить

Современные угрозы

78%

атак в 2023 году были целенаправленными*

Топ-3 ВПО

которое злоумышленники используют прямо сейчас: шифровальщики, инфостилеры, ВПО для получения удаленного доступа*.

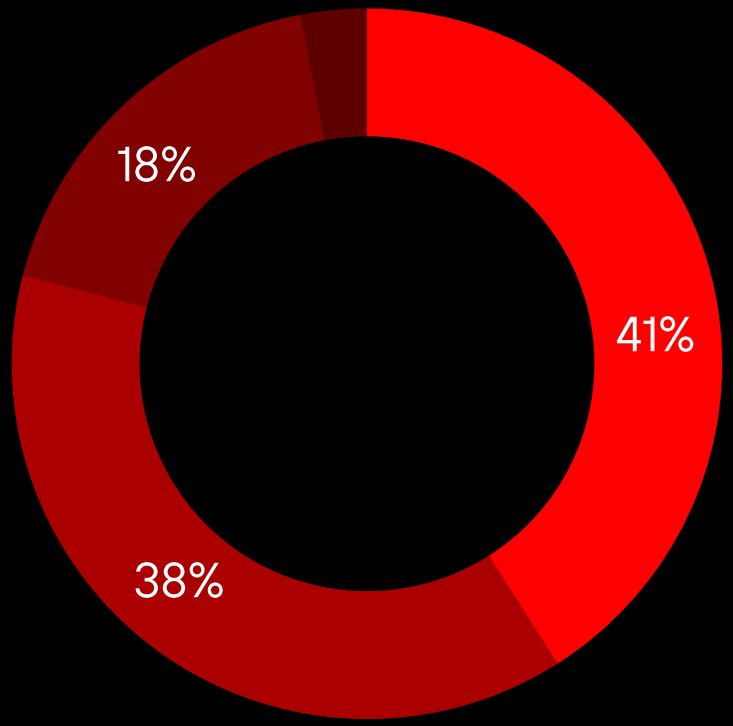
ВПО для разных систем

Злоумышленники осуществляют активный поиск уязвимостей в российских ОС на базе Linux.

Расширяют возможности проникновения в разные ОС за счет портирования ВПО (языки Go, Rust, Nim и другие).

* Актуальные киберугрозы

Современные угрозы



Типы вредоносного ПО (по количеству успешных атак)

Продолжает тренд и набирает еще большую популярность ВПО для получения удаленного доступа — 41%

Шифровальщики тоже остаются в тренде — 38%

Шпионское ПО — 18%

Конечные устройства, серверы и сетевое оборудование — № 1 для злоумышленников

* Актуальные киберугрозы

Источники и векторы угроз

Группировка Hellhounds
Ранее неизвестный бэкдор Decoy Dog, атаки типа supply chain, маскировка под процессы легитимного ПО

Инфраструктура российских компаний под управлением Linux и Windows

Группировка ExCobalt
Используют модуль CobInt, руткит Facefish, новый бэкдор GoRed, фишинговые рассылки вредоносных файлов, вложенных в архив, запуск которых приводит к загрузке модуля CobInt

Кредитно-финансовые организации, интересы — кража денежных средств

Группировка Dark River
Используют высокотехнологичный бэкдор MataDoor, способный незаметно действовать в скомпрометированной инфраструктуре в течение долгого времени

Предприятия российского оборонного комплекса, шпионаж и кража конфиденциальных данных

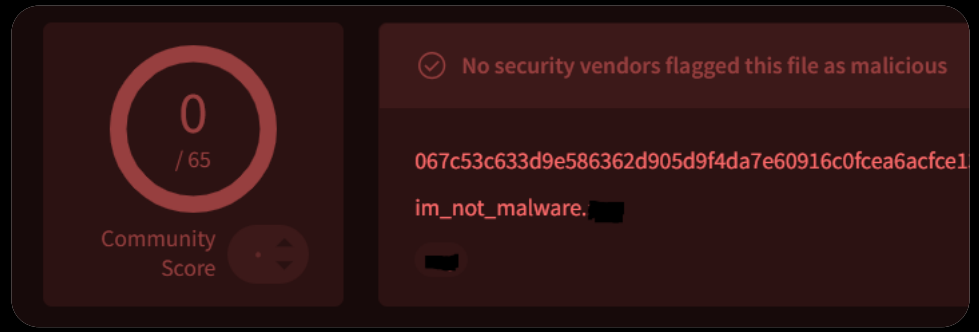
Группировка Space Pirates
Инструменты: ВПО, реализующее нестандартные техники (например, Voidoor), Deed RAT, публично доступные инструменты для продвижения по сети, Acunetix для разведки инфраструктуры и последующей атаки

Государственные и образовательные учреждения, военно-промышленный и топливно-энергетический комплексы, шпионаж и кража конфиденциальных данных

Нелегитимная легитимность

Использование комбинаций целенаправленных техник и инструментария:

- Маскировка атак под системные легитимные процессы
- Использование легитимных процессов (PowerShell)
- Создание ВПО нулевого дня с помощью репликации известного ВПО, смена сигнатур
- Использование эксплойтов в легитимном ПО, ОС и прикладном ПО
- Рассылка фишинговых писем с ВПО
- Использование легитимных учетных записей



Экспертиза на каждом узле

1 **Поставляется с набором экспертизы для обнаружения актуальных угроз**

600+
правил корреляции

5000+
YARA-правил

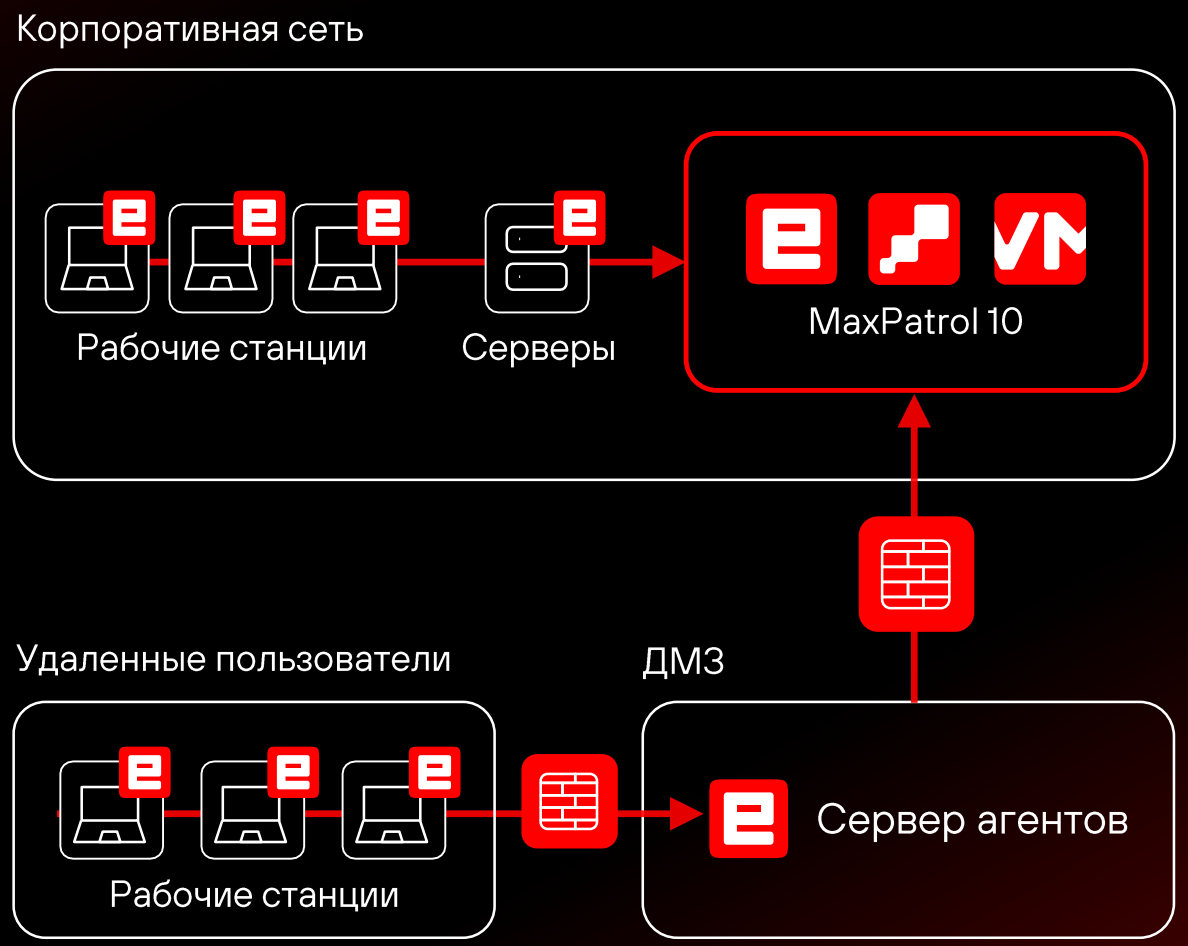
2 **Позволяет создавать и использовать собственные YARA-правила**

3 **Обрабатывает поступающие события и обогащает их полезной информацией:**

- определяет уровень привилегий учетных записей, от имени которых запускаются процессы;
- фиксирует контрольные суммы процессов и исполняемых файлов;
- отслеживает цепочки подозрительных действий.

Управляемый сбор данных

- Агенты собирают события и инвентаризационные данные, в том числе с устройств вне домена или периметра
- Сбор событий — непрерывно. Сканирование — по расписанию
- Для сканирования не нужны учетные записи с повышенными привилегиями
- Более простая маршрутизация: все данные передаются через соединение агента



Больше чем сенсор

1 Автономная работа

Агенты способны проводить анализ и реагировать самостоятельно, без обращения к серверу управления или без доступа в интернет

2 Поддержка отечественных ОС

Доступен для всех популярных ОС, включая отечественные (Astra Linux, «РЕД ОС», «Альт» и другие)

3 Ручное или автоматическое реагирование

Богатый выбор действий, которые можно полностью автоматизировать: остановка процесса, удаление файлов, изоляция устройства, отправка на анализ, перенаправление сетевых соединений (sinkholing)

4 Своевременное и непрерывное обнаружение

Поставляется с набором экспертных правил PT ESC, благодаря чему способен обнаружить актуальные угрозы, включая тактики и техники из матрицы MITRE ATT&CK (топ-50 для Windows и топ-20 для Linux), даже в полностью автономном режиме. Новые пакеты экспертизы поставляются непрерывно

Обнаружение

Доставка и установка инструментов для расширенного мониторинга на конечные устройства

Комбинирование автономных механизмов обнаружения (статический анализ, поведенческий анализ)

Многоэтапные проверки — последовательный автоматический запуск механизмов обнаружения

Гарантированное хранение артефактов для расследования

Обнаруживает самые популярные техники из матрицы MITRE ATT&CK

Топ-50
для Windows

Топ-20
для Linux

Реагирование

- Полная или частичная сетевая изоляция узлов
- Выполнение команд в удаленной консоли
- Завершение процессов
- Проверка по хеш-суммам файлов
- Отправка в карантин и (или) удаление файлов
- Перенаправление сетевых соединений (sinkholing)

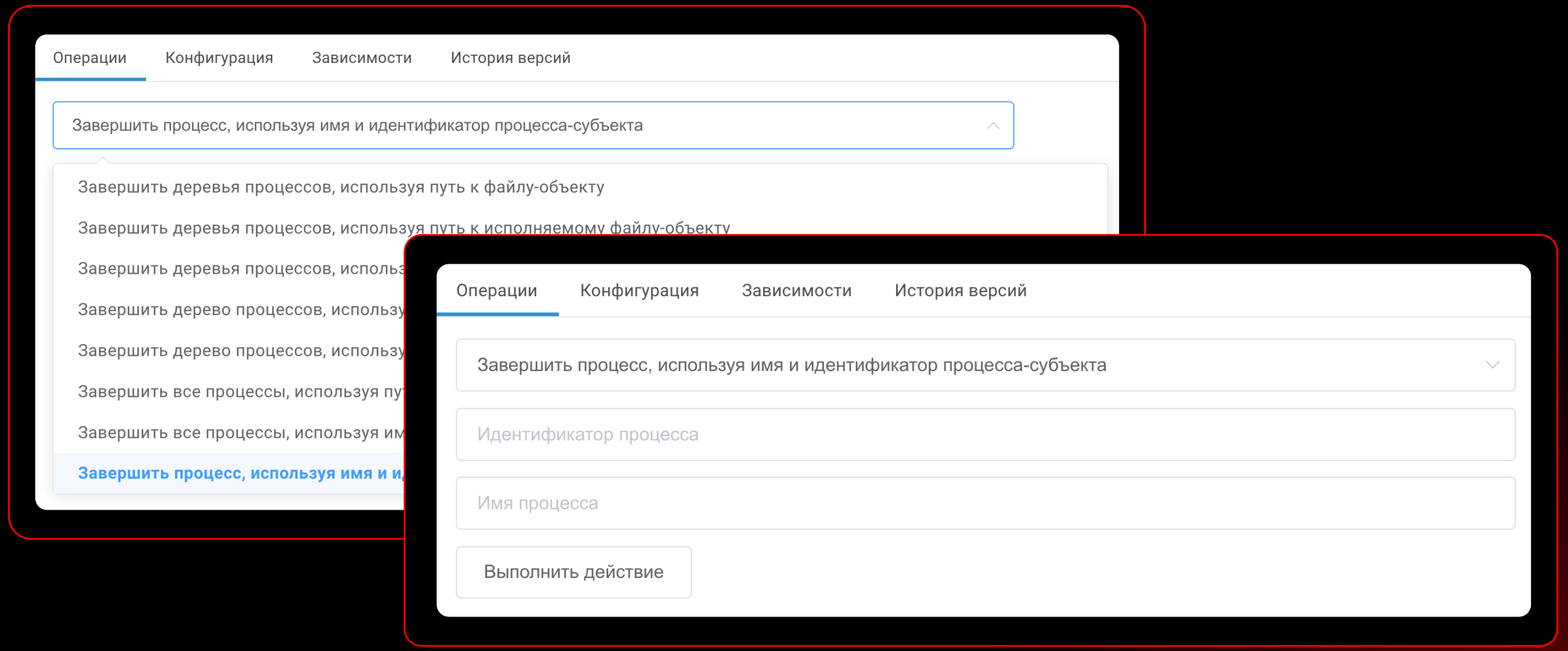
Автоматизация процессов SOC

- Политики реагирования
- Автономные агенты

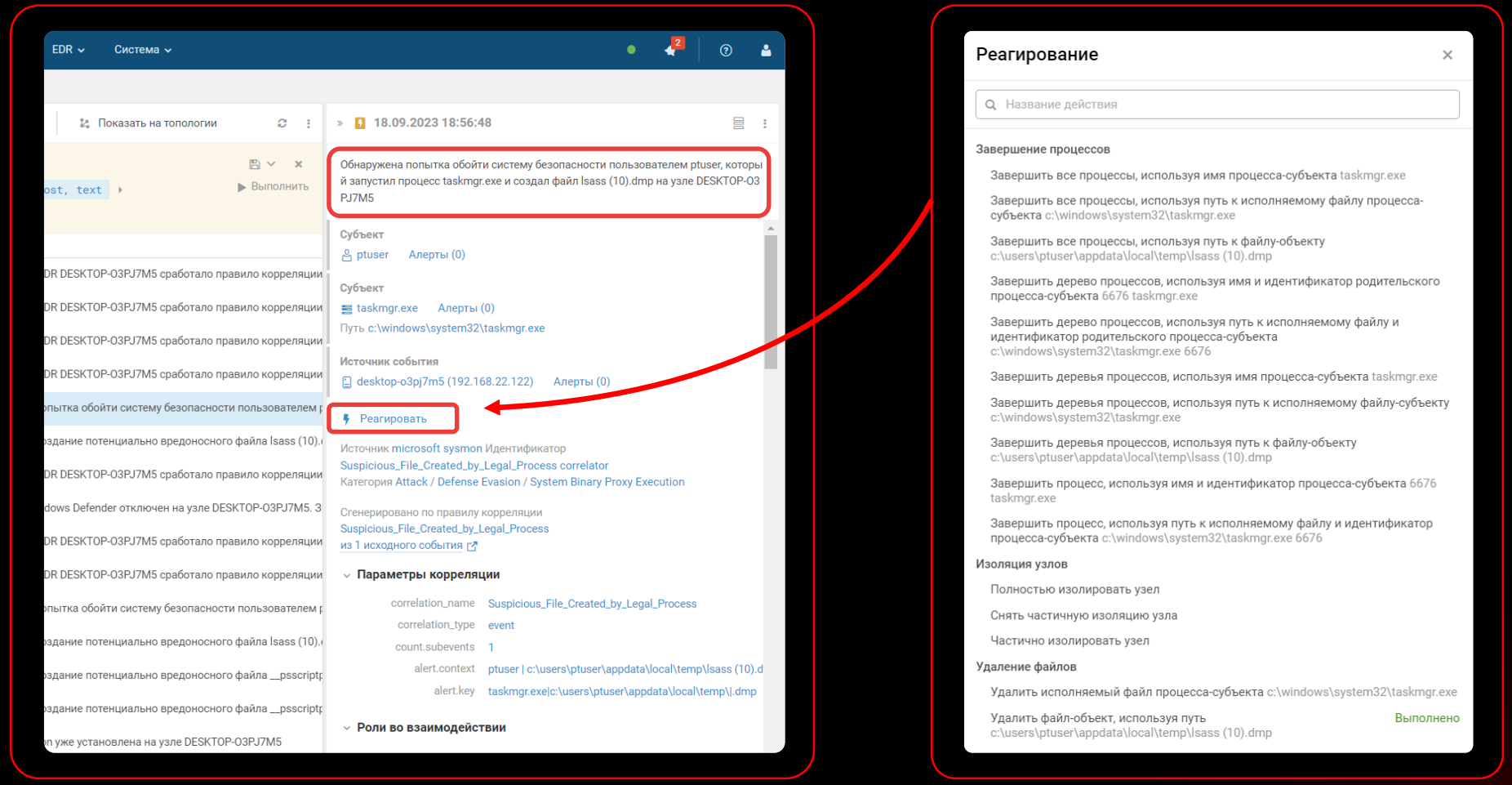
Контроль устройств, находящихся вне КСПД

- Реагирование на устройствах вне корпоративного периметра

Реагирование из интерактива модуля



Реагирование из карточки события в два клика

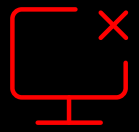


MaxPatrol EDR
Синергия решений

MaxPatrol EDR + MaxPatrol VM

Задачи

Сканировать инфраструктуру полностью. Следить за маршрутами от сканера до каждой цели

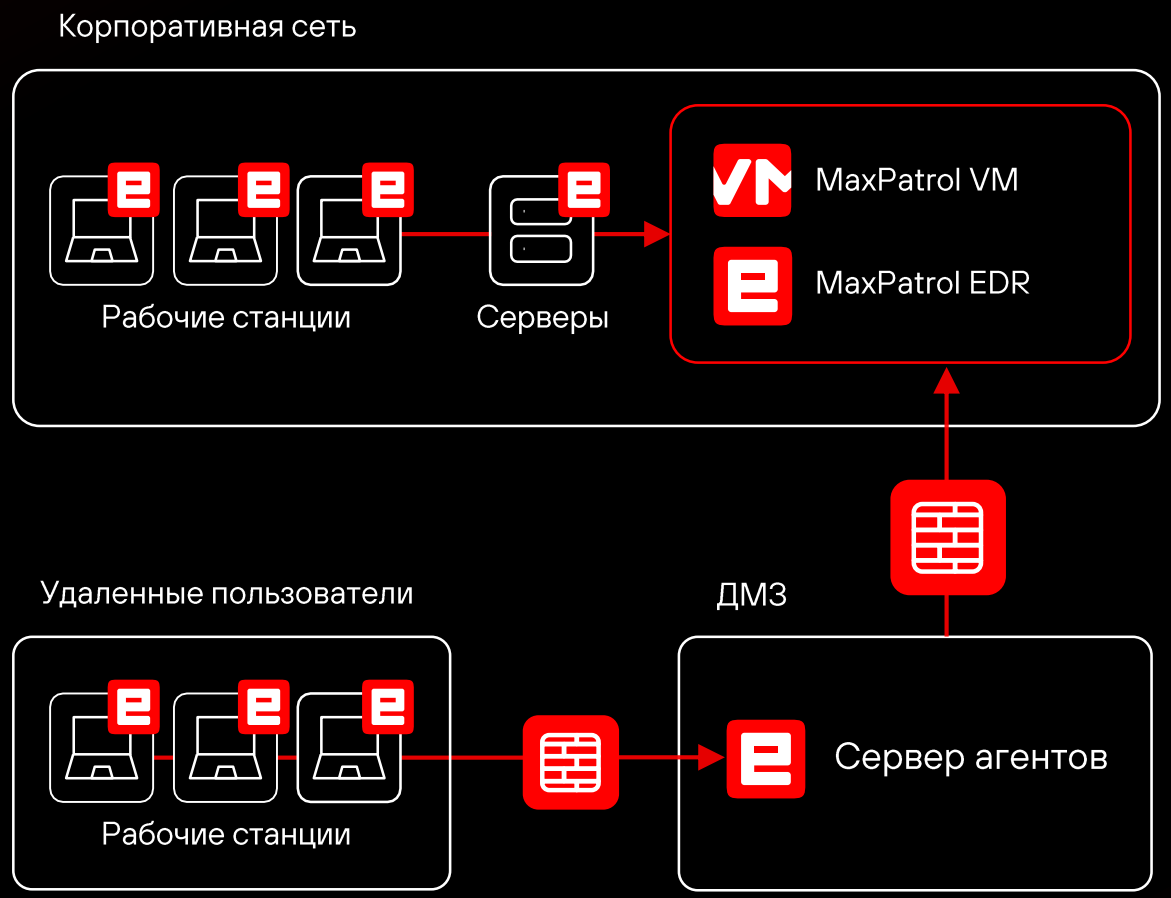


Устройства могут быть выключены или недоступны во время сканирования

Информация об активах обновляется недостаточно часто, данные не соответствуют действительности

Согласовать с ИТ-отделом доступы и учетные записи для сканирования чувствительных сегментов

MaxPatrol EDR + MaxPatrol VM



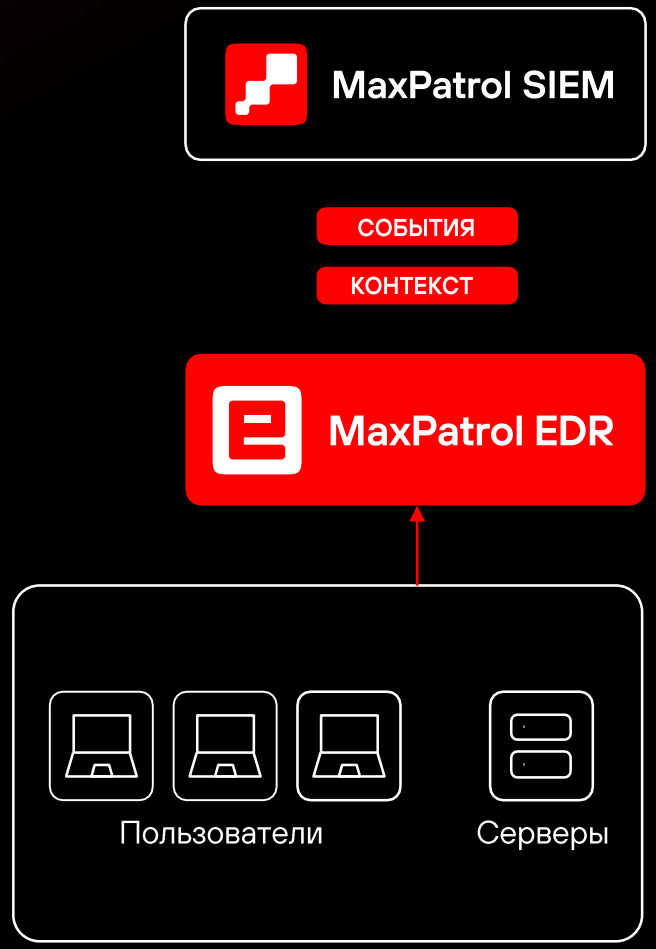
> Задачи

- Сбор данных с устройств, с которых их не получалось собрать средствами только MaxPatrol VM
- Частое обновление данных об активах
- Снижение нагрузки на сканирующий сервер и каналы связи
- Упрощение взаимодействия между отделами ИБ и ИТ

> Каким образом

- Модули сканирования не требуют сервисных УЗ, собирают данные с узлов вне домена и с устройств удаленных сотрудников
- Узловое сканирование происходит параллельно на всех активах в группе
- Отсутствует паразитный трафик, создаваемый сетевым сканером; сканирование производится с помощью мощностей самого узла с агентом
- Не нужны УЗ с повышенными привилегиями, не нужно тратить время на маршрутизацию

MaxPatrol EDR + MaxPatrol SIEM



> Задачи

- Контроль сбора событий с серверов и рабочих станций
- Раннее обнаружение следов атак и подозрительной активности на устройствах
- Возможность оперативного реагирования на устройствах
- Сокращение операционных расходов
- Упрощение взаимодействия между отделами ИТ и ИБ

> Каким образом

- Настройка профиля мониторинга прямо из консоли EDR. Централизованно для всех групп устройств, в том числе вне домена
- Поведенческий и статический анализ прямо на устройствах. Корреляционные и YARA-правила на агентах
- Широкий набор действий для своевременного реагирования
- События, контекст и возможность реагирования прямо из карточки события, в единой консоли
- Договоренности → политики EDR. Автоматизация реагирования в согласованных случаях

MaxPatrol EDR + PT Sandbox

> Задачи

- Защита от ВПО, распространяемого через шифрованные каналы
- Повышение точности обнаружения угроз
- Молниеносное реагирование на угрозы

> Каким образом

- Обнаруживаются файлы, скачиваемые, например, через Telegram, браузеры, P2P и т. п.
- Проводится подробный статический и поведенческий анализ
- Результат анализа становится доступен на всех агентах группы

MaxPatrol EDR

Планы

- Отправка сырых событий и удаленная консоль управления
- API для реагирования
- Обновление UX и UI
- Работа в кластере и HA
- Улучшение интеграций
- Расширение возможностей реагирования

MaxPatrol EDR

Обзор
MaxPatrol EDR

MaxPatrol EDR

Обзор
MaxPatrol VM

MaxPatrol VM

Внимание, опрос!

Спасибо!