positive technologies

MaxPatrol Endpoint Detection & Response

Защита устройств компании и сотрудников от сложных и целевых атак

тренды

78% атак

в 2023 году были целенаправленными

Топ-3 ВПО

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

Угрозы для разных систем

Злоумышленники осуществляют активный поиск уязвимостей в российских ОС на базе Linux и расширяют возможности проникновения в разные ОС за счет портирования ВПО (языки Golang, Rust, Nim и др.)

MaxPatrol EDR

MaxPatrol EDR поможет оперативно выявлять сложные угрозы и целевые атаки, обеспечит уверенное реагирование и автоматизацию рутинных операций с учетом особенностей инфраструктуры и процессов построения ИБ в вашей компании.

- **На ранних этапах выявляет развивающиеся на устройствах атаки**, которые могут пропустить другие средства ИБ.
- **Собирает важные данные для проведения расследований.**
- **Останавливает злоумышленника за считанные секунды.**
- **Помогает аналитикам SOC и руководителям служб ИБ расследовать и предотвращать атаки**, блокируя действия злоумышленников на конечных устройствах.

Преимущества

- Возможность автономной работы агента
- Статический и поведенческий анализ на агенте
- Гибкая настройка правил обнаружения и реагирования
- Не конфликтует с другими СЗИ
- Настраиваемая отправка файлов в песочницу
- Поддержка Windows, Linux, macOS и отечественных ОС

Молниеносная реакция на узлах

Предоставляет богатый выбор действий для автоматического и своевременного реагирования: остановка процесса, удаление файлов, изоляция устройства, отправка на анализ, синкхолинг.

Обнаружение угроз в динамике

Обнаруживает атаки с использованием легитимных инструментов (PowerShell, WMI, CMD, BASH), которые могут пропустить традиционные средства защиты, основанные на сигнатурном анализе.

Своевременное и непрерывное обнаружение ВПО

Поставляется с набором экспертных правил PT ESC, благодаря чему способен выявлять угрозы и популярные тактики и техники злоумышленников из матрицы MITRE ATT&CK (топ-50 для Windows и топ-20 для Linux).

Легкое встраивание в инфраструктуры

Выступает в роли единого агента для обнаружения, реагирования, сбора телеметрии и информации об уязвимостях на узлах. Поддерживает работу на всех популярных операционных системах, включая российские, и в VDI-структурах.

Подходит для разных организаций

Экономит ресурсы и время специалистов

Построение эшелонированной защиты на базе комплексных решений или интеграции нескольких продуктов не всегда вписывается в бюджет организации. MaxPatrol EDR позволяет начать решать задачу защиты устройств сотрудников и организации без чрезмерных затрат, постепенно выстраивая процессы ИБ.

Учитывает особенности инфраструктуры

Позволяет гибко настроить политики обнаружения и реагирования с учетом архитектуры. Поддерживает идеальный баланс между нагрузкой на узлы и обеспечением требований SOC.

Работает в закрытых сегментах

Не требует для работы доступа в интернет. Поставка обновлений экспертизы возможна через промежуточный сервер для односторонней передачи.

Не конфликтует с другими СЗИ

Организации могут использовать несколько защитных решений, дополняя экспертизу разных вендоров без влияния на бизнес-процессы.

Автоматизирует функции реагирования

Часто EDR-решения не предлагают автоматических реакций, кроме остановки процессов или удаления файлов.В MaxPatrol EDR вы можете управлять логикой и использовать все доступные опции реагирования как вручную, так и автоматически.

Предоставляет привычную логику и интерфейс

MaxPatrol EDR создан в едином стиле продуктов Positive Technologies и предоставляет знакомые сущности, авторизацию, сервисы и кросс-продуктовые сценарии, обеспечивая пользователю легкий старт.

Как работает MaxPatrol EDR

* Реагирование может происходить как в автоматическом режиме (если допустимо и предусмотрено политикой), так и в ручном

** Интеграция путем добавления кастомных функциональных модулей в продукт через Positive Technologies и партнеров вендора

Телеграм-чат пользователей
t.me/MPSIEMChat

Заказать бесплатный пилот
ptsecurity.com/ru-ru/products/edr/#free-demo

Телеграм-канал Positive Technologies
t.me/positive_technologies