positive technologies

PT Extended Detection and Response

Продукт для оперативного выявления киберугроз и реагирования на них

Возможности PT XDR

Экспертный автономный комплекс XDR. Операторы SOC могут самостоятельно проверять гипотезы о компрометации узлов с помощью телеметрии.

Работа на всех платформах. PT XDR поддерживает работу агентов на Windows, Linux и macOS.

Простая интеграция. Необходимые коннекторы для интеграции компонентов поставляются вместе с продуктом, а для их настройки нужна только сетевая связность.

Автоматизирует реагирование на угрозы и сокращает время на остановку атаки. Автоматически предлагает варианты реагирования на угрозы, проводит «лечение» и позволяет восстановить работоспособность систем в сети.

Снижает требования к ресурсам и компетенциям SOC-команды. PT XDR автоматизирует рутинные процессы, приоритизирует очередь на анализ, дает полный контекст атаки и позволяет найти причину компрометации данных.

PT Extended Detection and Response (PT XDR) — система, предназначенная для защиты конечных устройств от киберугроз. PT XDR собирает и анализирует данные из множества систем, выявляет в IT-инфраструктуре организации сложные целевые атаки и автоматически реагирует на них.

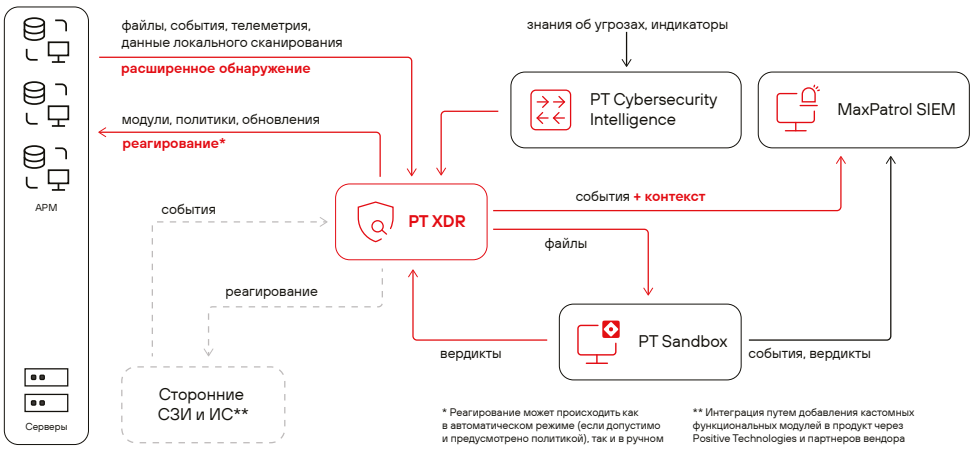
PT XDR встроен в экосистему продуктов Positive Technologies и позволяет:

- отправлять в MaxPatrol SIEM собранные на конечном устройстве системные данные и данные о событиях ИБ;
- отправлять подозрительные файлы на проверку в PT Sandbox и применять полученные вердикты одновременно на всех конечных устройствах;
- использовать данные и экспертизу из других продуктов для выявления и расследования кибератак.

При обнаружении угроз PT XDR может автоматически:

- удалить файл;
- завершить один или несколько процессов;
- заблокировать сетевой трафик;
- отправить файл на проверку в PT Sandbox;
- отправить данные о событиях ИБ на syslog-сервер и в MaxPatrol SIEM;
- выполнять и другие операции.

Кроме того, оператор системы может в любой момент вручную запустить реагирование на угрозу на конечном устройстве.



Закажите бесплатную пилотную версию. Оцените возможности PT XDR в вашей инфраструктуре — заполните заявку на сайте и начните выстраивать процесс реагирования на инциденты ИБ с помощью экспертизы Positive Technologies

Преимущества PT XDR

Автоматизирует реагирование на инциденты ИБ. Это сокращает время на обработку отдельных событий, полученных от средства защиты, и снижает порог входа для работы с XDR системой: не нужно быть экспертом, чтобы проводить расследования и реагировать на инциденты.

Связывает события на узлах в единую цепочку атаки. PT XDR обрабатывает поступающие в него события, объединяет их в понятные цепочки атак и предлагает варианты реагирования, то есть «склеивает» большой поток событий в несколько цепочек и обращает на них внимание SOC-аналитика.

Определяет первоначальную точку атаки. Собрав цепочку атаки, PT XDR определяет причину ее возникновения. Продукт взаимодействует с другими средствами защиты и получает контекст каждого шага атаки.

Объединение средств ИБ в единую систему. В отличие от базовых средств защиты конечных устройств (антивирусы, EPP) и решений класса EDR, которые фокусируются на конечных точках, PT XDR позволяет использовать возможности других используемых систем ИБ и содержащуюся в них экспертизу для реализации комплексных сценариев обнаружения. Точность обнаружения заметно возрастает, а среднее время расследования — снижается.

Упрощает проактивный поиск угроз. PT XDR может получать сведения об угрозах из PT Cybersecurity Intelligence: это различные индикаторы компрометации (например, IP-адреса, URL, домены, хэши файлов). PT Cybersecurity Intelligence работает с потоками данных от Positive Technologies и других поставщиков.

Реагирует на угрозы. Агент PT XDR обеспечивает надежный сбор данных и используется для обнаружения угроз и своевременного реагирования на них.

Какие функции доступны в PT XDR

PT XDR

- **Корреляционный движок на узле**, более 200 готовых правил и возможность писать собственные
- **YARA-модуль** для анализа файлов и процессов, возможность использовать собственные правила
- **Собственный** драйвер для сбора события и реагирования
- **Модуль сбора артефактов для форензики**
- **Модуль исполнения произвольных команд и сценариев**
- **Агенты для Windows, Linux и macOS**
- **Гибкая настройка политик** обнаружения и реагирования с возможностью ветвления логики обработки событий
- **Обнаружение инъекций** вредоносных библиотек, буткитов, криптолокеров и другого ВПО
- **Многопоточность:** модули могут работать параллельно
- **Автономность агента:** основные модули реагирования работают и без подключения к серверу управления, а события кэшируются

PT XDR + MaxPatrol SIEM, MaxPatrol VM, PT Sandbox

- **Обнаружение угроз** во всей инфраструктуре и возможность выстраивать комплексные схемы реагирования на них, в том числе с использованием сторонних продуктов
- **Нативная интеграция с MaxPatrol SIEM:** инвентаризация, межузловая корреляция событий и выявление инцидентов
- **Автоматизация поиска и устранения уязвимостей с использованием MaxPatrol VM.** Расстановка приоритетов на основе экспертизы Positive Technologies и списка трендовых уязвимостей
- **Обнаружение ВПО, используемого в APT-атаках, с помощью PT Sandbox.** Блокировка векторов атак через доставку вредоносного ПО с помощью мессенджеров или через шифрованный пользовательский трафик
- **Расширение экспертизы PT XDR** с использованием платформы threat Intelligence PT Cybersecurity Intelligence
- **Возможность реализации настраиваемых функций** для интеграции со сторонними продуктами и пользовательских сценариев применения

ptsecurity.com
pr@ptsecurity.com

PT-EXD_PB_A4.RUS.0002.03.DEC.22.2022