PT X

positive technologies

БЫСТРЫЙ ПУТЬ К ПОСТОЯННОЙ ЗАЩИТЕ

PT X — решение для регулярного мониторинга и реагирования, которое объединяет опыт лучших экспертов, обеспечивает максимально возможное покрытие угроз и фокусируется на главном — отражении атак.

Знаете ли вы, что...

От 4 часов
нужно хакеру, чтобы проникнуть в локальную сеть и получить максимальные привилегии

50% атак
привели к нарушению деятельности компаний в 2025 году

От 1 года
необходимо, чтобы организовать SOC, найти бюджет, выстроить процессы и нанять экспертов

А еще:

Кибератакам подвержены все — от малого бизнеса до крупных корпораций.

В 2025 году стало на 6% больше атак* по сравнению с предыдущим годом.

Инструменты, тактики и изобретательность атакующих постоянно совершенствуются, атаки не прекращаются, а ущерб — постоянно растет.

Для противодействия злоумышленникам нужен сплав из технологий, экспертизы и опыта. Такое доступно не всем организациям.

Мы, команда Positive Technologies, не согласны с таким положением дел, поэтому разработали PT X — облачное решение, способное эффективно отражать кибератаки в компаниях с любым уровнем зрелости ИБ.

* Подробности в исследовании Positive Technologies

Чем уникален PT X

Защита от широкого спектра кибератак
Уже через несколько часов после внедрения — уверенная защита от шифровальщиков, вредоносного ПО и использования распространенных уязвимостей в инфраструктуре.

Быстрый старт без лишних затрат
Для старта достаточно установить агенты на конечные устройства. Решение не требует выделения ресурсов и длительного внедрения.

Экспертная поддержка
Непрерывная защита обеспечивается за счет поддержки от специалистов экспертного центра безопасности PT ESC, имеющих опыт в области выявления и предотвращения сложных кибератак.

Гарантия результата
Мы гарантируем, что при использовании PT X и выполнении рекомендаций ваша защита выдержит кибериспытания, и готовы выплатить вознаграждение белым хакерам, если недопустимое событие будет реализовано.

Как работает решение

1. Установка легких программных компонентов на ваши конечные устройства — серверы, рабочие станции, виртуальные рабочие места.
2. Автоматизированный сбор телеметрии и ее анализ.
3. Быстрое выявление и блокировка действий злоумышленников — даже если они уже давно находятся в ваших системах.
4. В случае сложных APT-атак наши эксперты свяжутся с вами и помогут остановить атаку.

Узнать о решении

Телеграм-канал экспертного центра PT ESC

Подбирайте решение под ваши бизнес-потребности

Применяемые технологии	**PT X Base** Стандартный уровень защиты от хакерских атак	**PT X Pro** Продвинутый уровень защиты от хакерских атак
Защита конечных устройств	MaxPatrol EDR	MaxPatrol EDR
Анализ сетевого трафика	—	PT NAD
Анализ вложений на наличие ВПО	—	PT Sandbox
Подключение дополнительных источников	СЗИ Positive Technologies (при наличии)	MaxPatrol SIEM (поддерживаемые источники, позволяющие детектировать атаки)
Индикаторы компрометации	+	+
Управление жизненным циклом инцидентов	+	+
ИИ-технологии (машинное обучение, большие языковые модели)	+	+
Экспертиза		
Выявление инцидентов (24/7)	+	+
Реагирование на инциденты (24/7)	+	+
Проактивный поиск угроз	+	+
Рекомендации по устранению уязвимостей и ошибок конфигураций	+	+
Цифровая криминалистика и реагирование на инциденты (DFIR)	1 расследование	4 расследования