PT X

Круглосуточный автоматизированный мониторинг инфраструктуры и реагирование на кибератаки

- Вся необходимая защита для бизнеса в одном решении
- Ощутимый эффект уже через несколько часов после подключения
- Самое широкое покрытие по техникам атак на рынке
- Уникальная комбинация экспертизы, машинного обучения и защитных технологи
- Гарантированный результат: отвечаем деньгами за безопасность клиента

5,1 млн руб.
Минимальный бюджет проекта

от 2-х месяцев
Средний цикл продажи

33 млн руб.
Средний чек проекта за три года

Плюсы PT X

Полностью укомплектованная защита

Не нужно нанимать команду в штат, тратить месяцы на обучение сотрудников и докупать продукты для ИБ. PT X позволит оперативно укрепить защиту и обеспечить максимальное покрытие угроз без дополнительных вложений.

Быстрое внедрение

Полное подключение займет всего восемь часов, а первые результаты будут видны уже через несколько часов после внедрения. Агенты PT X устанавливаются на конечные устройства, потребляют мало ресурсов и быстро настраиваются.

Ответственность за результат

Решение предусматривает проверку защиты на кибериспытаниях. Если белым хакерам удастся реализовать недопустимое событие, Positive Technologies выплатит им вознаграждение.

Фокус на отражении атак

Передовые ML-технологии для обнаружения угроз

ИИ-модели выявляют до 80% инцидентов, фокусируя внимание аналитиков на реальных угрозах. Все вердикты проходят верификацию экспертами перед принятием мер реагирования.

Второе мнение для зрелого SOC

Решение поможет разобраться с неочевидными инцидентами — за PT X стоят эксперты Positive Technologies с многолетним опытом выявления и предотвращения сложных кибератак.

Проактивный мониторинг инфраструктуры

Помимо атак PT X выявляет на узлах уязвимости и ошибки конфигураций, с помощью которых злоумышленники могут проникнуть в инфраструктуру. Решение также дает рекомендации по усилению защиты.

	PT X Base Стандартный уровень защиты от хакерских атак	PT X PRO Продвинутый уровень защиты от хакерских атак
Применяемые технологии		
Защита конечных устройств	MaxPatrol EDR, MaxPatrol EPP	MaxPatrol EDR, MaxPatrol EPP
Анализ сетевого трафика		PT NAD
Анализ вложений на наличие ВПО		PT Sandbox
Подключение дополнительных источников	СЗИ Positive Technologies (при наличии)	MaxPatrol SIEM (поддерживаемые источники, детектирующие атаки)
Индикаторы компрометации	+	+
Управление жизненным циклом инцидентов	+	+
AI-технологии (ML, LLM)	+	+
Экспертиза		
Выявление инцидентов (24/7)	+	+
Реагирование на инциденты (24/7)	+	+
Threat hunting	+	+
Рекомендации по устранению уязвимостей и ошибок конфигураций	MaxPatrol VM, MaxPatrol HCC, PT EASM	MaxPatrol VM, MaxPatrol HCC, PT EASM
Цифровая криминалистика и реагирование на инциденты (DFIR)	+ (1 расследование)	+ (4 расследования)
Выделенный сервис-менеджер	+	+
Выделенный аналитик		+
Минимальная стоимость	**5 110 000 руб.**	**9 198 000 руб.**

Какие боли клиента «лечит» PT X

Компания уже подверглась кибератаке
Развертывание решения за несколько часов поможет оперативно отразить атаку

Непонятно, где и как искать следы компрометации
Встроенные агенты PT NAD , PT Sandbox и MP SIEM (в PT X Pro) позволят быстро провести расследование и обнаружить следы компрометации инфраструктуры

Не хватает ресурсов и экспертизы для предотвращения инцидента ИБ
Рекомендации по безопасности и настройке средств защиты – значимая часть эффективной работы решения

Нет времени на раскачку, полноценная защита нужна прямо сейчас
Будут выстроены процессы регулярного мониторинга ИБ и реагирования на инциденты

Регулятор предписал исправить недочеты в сжатые сроки
PT X позволит на 100% выполнить требования регуляторов и отраслевых стандартов

Бюджет позволяет закрыть только часть требований к киберзащите
Решение позволит кратно повысить уровень безопасности без серьёзного увеличения бюджета на ИБ

Фонд оплаты труда не позволяет нанимать больше сотрудников в SOC
Решение позволит автоматизировать большую часть работы с помощью AI/ML обработки инцидентов и тредхантинга.

Нет уверенности в качестве обработки инцидентов
В решении аккумулирован опыт расследования сотен инцидентов самых опасных кибератак.