



PT X



Облачное решение
для мониторинга
и реагирования
на кибератаки
от Positive Technologies



Молния не бьет дважды?



Хакеры могут успешно атаковать одну и ту же организацию снова и снова

Атакующим достаточно одной бреши в безопасности



14–16%

всех успешных кибератак в мире пришлось на Россию*

71%

доля успешных атак с ВПО*

33%

атак совершали финансово мотивированные группировки*

Социальная инженерия

Стараемся... Внедряем системы AV, DLP, SIEM как можем

BDU:2022-01141
BDU:2023-05857
...

Атаки через сервисы VPN и RDP

Уязвимость
BDU:2021-01123
(ProxyLogon)

Отсутствует двухфакторная аутентификация

* CODE RED 2026: Актуальные киберугрозы для российских организаций

Как решать



Заплатить хакерам

Если взломали, можно откупиться, заплатив BTC
≈330 тыс. \$

И подвергнуться повторному взлому и выводу данных



Строить свой SOC

Долго и дорого растить компетенции, искать людей и выстраивать процессы

В среднем на это уходит больше года



Выбрать аутсорсинг

Доверяй, но проверяй

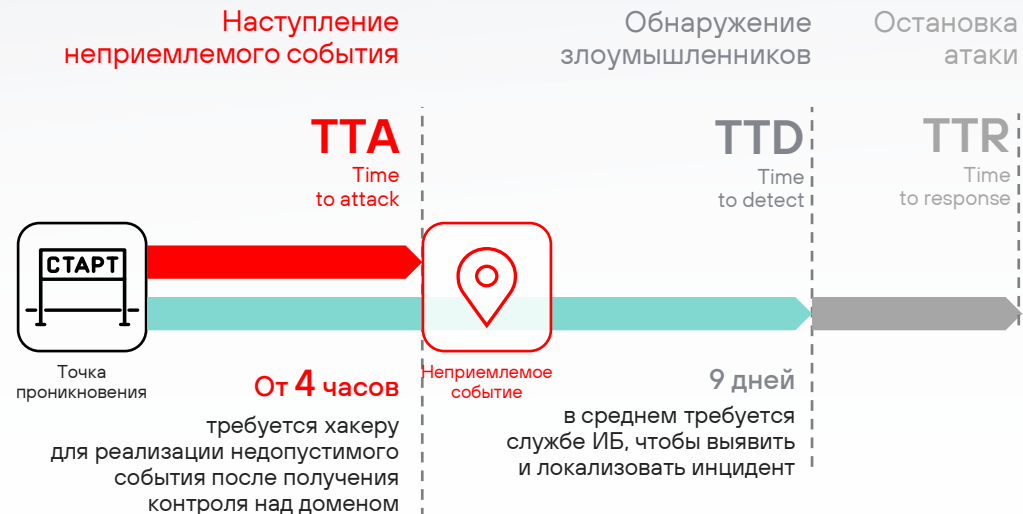
В SLA не заложена привязка к конкретному результату

Хакеры атакуют быстрее, чем служба ИБ реагирует



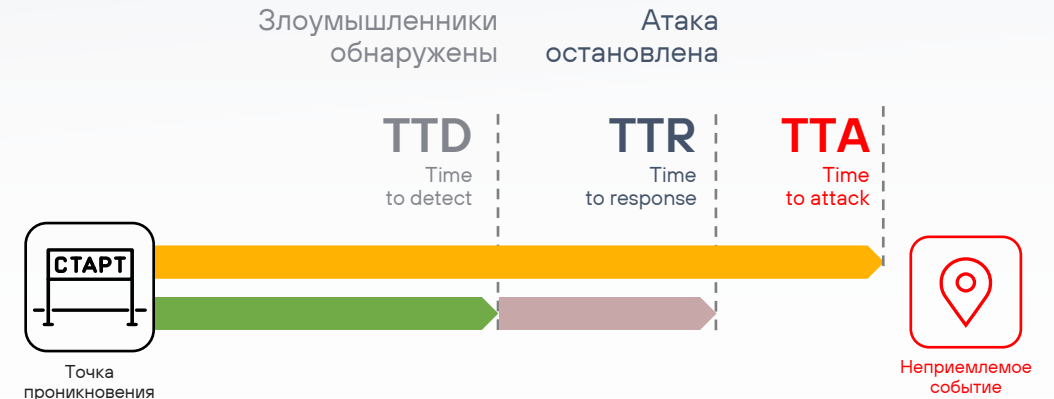
Классическая проблема кибербеза

Время атаки < Время реагирования = Успешная атака



Задача кибербеза

Время атаки > Время реагирования = Киберустойчивость



SLA не гарантирует, что TTR будет меньше TTA
Необходим другой способ подтверждения результата

Где функционирует РТ Х



До атаки

- Анализ поверхности атаки на периметре и киберразведка
- Поиск опасных уязвимостей внутри инфраструктуры
- Поиск опасных мисконфигураций внутри инфраструктуры



Во время атаки

- Непрерывное обнаружение признаков атак на узлах, в трафике и файлах
- Реагирование на атаки 24/7
- Расследование инцидентов (DFIR)
- Проактивный поиск угроз

Ключевые преимущества РТ Х



Фокус на результате

1

Уже через несколько часов после внедрения — подтверждение результативности, уверенная защита от шифровальщиков, вредоносного ПО и использования распространенных уязвимостей в инфраструктуре

Быстрое подключение, минимум затрат

2

Для старта достаточно установить агенты на конечные устройства. Решение не требует выделения ресурсов и длительного внедрения

Команда опытных экспертов

3

Непрерывная защита обеспечивается за счет поддержки от специалистов экспертного центра безопасности РТ ESC, имеющих опыт в области выявления и предотвращения тысяч сложных кибератак

Самое широкое покрытие

4

РТ Х имеет уникальный набор компонентов для глубокого анализа данных, оперативного обнаружения угроз и реагирования. Комбинация MaxPatrol EDR, MaxPatrol SIEM, PT Sandbox, PT NAD, MaxPatrol VM и MaxPatrol HCC обеспечивает автоматизированный сбор телеметрии, быстрое выявление и блокировку действий злоумышленников

Помогаем стать профи в киберзащите

5

Мы гарантируем, что при использовании РТ Х и выполнении рекомендаций защита компании выдержит кибериспытания, и готовы выплатить вознаграждение белым хакерам, если недопустимое событие будет реализовано

Кому и для чего нужен РТ X



1

Нужно **быстро снизить риски** остановки бизнеса, утечки конфиденциальной информации и ноу-хау, кражи денег

2

Бюджет на кибербезопасность ограничен, сложно найти специалистов, а задачи нужно выполнять **уже сейчас**

3

Стали жертвой кибератаки, **срочно нужна защита**

4

Необходимо **эффективно усилить команду ИБ (SOC)**

5

Хочется **иметь второе мнение** от экспертной команды на случай неочевидных ситуаций

6

Нет экспертных ресурсов для решения задач threat hunting, форензики и поддержки других процессов в сфере ИБ

Решение с фокусом на результате



Кибериспытания

Ответственность за результат



Финансовая ответственность Positive Technologies
в случае реализации кибератаки

Кибериспытания

Привлечение
белых хакеров для проверки
эффективности системы
защиты

Страхование киберрисков

Страхование от ущерба,
который может быть
причинен компании
в случае успешной атаки

Кибериспытания



Большое сообщество белых хакеров продемонстрирует возможность реализации комплексных сценариев атак, которые могут привести к недопустимым для компании событиям

Самое большое сообщество белых хакеров в России

Более 30 000 независимых российских и международных исследователей с разной специализацией и опытом проверят максимальное количество векторов атак

Реальная оценка защищенности

Кибериспытания позволяют оценить достаточность, эффективность и необходимость доработки реальной системы защиты компании

Непрерывный процесс улучшения безопасности

Исследователи работают в режиме 24/7, позволяют быстро и безопасно выявлять и устранять киберриски

От кого мы защищаем



PT X	УРОВЕНЬ КВАЛИФИКАЦИИ АТАКУЮЩЕГО	ПРОФИЛЬ И МОТИВАЦИЯ	ПОРТРЕТ	СЕБЕСТОИМОСТЬ АТАК И СУММА ВЫПЛАТ ИССЛЕДОВАТЕЛЯМ	
	БАЗОВЫЙ	Начинающие злоумышленники		до 500 000 ₽	PT X Base
	БАЗОВЫЙ +	- Хактивисты - Квалифицированные хакеры-одиночки		до 3 000 000 ₽	PT X Base
	ПРОДВИНУТЫЙ	- Финансово мотивированные киберпреступники, АРТ-группировки - Хактивисты		до 20 000 000 ₽	PT X Pro
	ЭКСПЕРТНЫЙ	- Высококвалифицированные АРТ-группировки - Финансово мотивированные киберпреступники		от 20 000 000 ₽	
	МАКСИМАЛЬНЫЙ	АРТ-группировки, мотивированные государственными структурами		Не ограничена	

Ответственность за результат



Финансовая ответственность Positive Technologies в случае реализации кибератаки при выполнении киберминимума

Вывод на кибериспытания и страхование киберрисков

	Базовый	Базовый+	Продвинутый	Экспертный / Максимальный	Страхование от ущерба в случае реальной кибератаки
PT X Base без выполнения киберминимума	+*	+*	—	—	—
PT X Base при выполнении киберминимума	+	+	—	—	+
PT X Pro без выполнения киберминимума	+*	+*	+*	—	—
PT X Pro при выполнении киберминимума	+	+	+	—	+
Максимальный размер выплат на кибериспытаниях (млн руб.)	1	3	20	50 / 100	

* Вознаграждение исследователям выплачивается клиентом

Киберминимум



PT X Base

Полное **покрытие мониторингом и средствами антивирусного ПО** ИТ-активов защищаемой компании

Отсутствие или компенсация **критически опасных уязвимостей и мiskonфигураций.**

Вновь выявленные на периметре и на критически важных активах устраняются в течение **96 часов**

Процесс реагирования согласован с командой заказчика и полностью соблюдается

Ограничение доступа для непубличных сервисов, доступных из интернета.
Невозможность доменной аутентификации без **2FA** на ресурсах, опубликованных в открытом доступе

PT X Pro

Все почтовые ящики в части входящего трафика **защищены от вредоносного ПО**

Осуществляется **анализ сетевого трафика** серверного и пользовательского сегментов, DMZ, а также анализ исходящего интернет-трафика

Путь к результату



Шаг 1 ≈2 недели

Выявление следов
компрометации

Шаг 3 ≈3 месяца

Выполнение
киберминимума

Шаг 2 ≈1 неделя

Подключение
PT X

Шаг 4 Постоянно

Выход
на кибериспытания

PT X Base

Стоимость атак —
до 3 млн руб.

PT X Pro

Стоимость атак —
до 20 млн руб.



Примеры недопустимых событий



На кибериспытания выводится одно недопустимое событие (НС)

**Остановка продаж
и платежей на сайте
или в мобильном
приложении**

Намеренная остановка
службы _____ на сервере
с IP-адресом _____

**Остановка доставки
на маркетплейсы**

Возможность запрета
исходящего сетевого трафика
в интернет с сервера
с IP-адресом _____
на уровне хоста

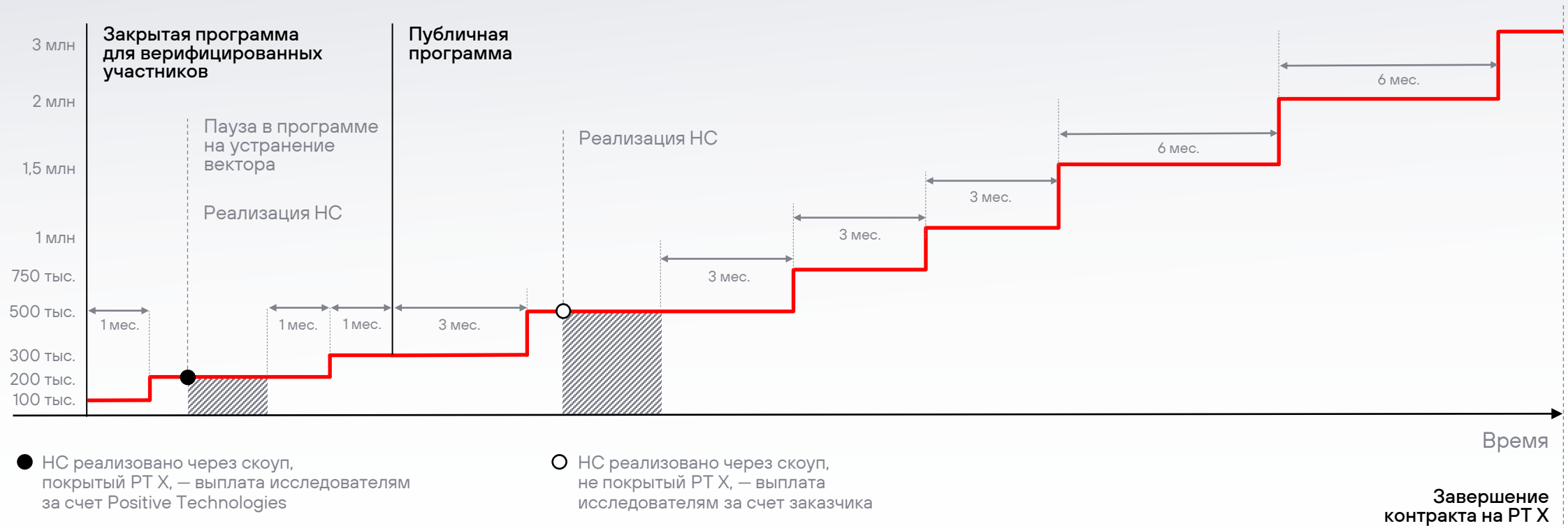
**Остановка доставки
от центрального склада
в региональные
распределительные
центры**

Остановка сервиса _____
на сервере с IP-адресом _____

Кибериспытания



Пример плана поэтапного повышения ставки вознаграждения исследователям* для PT X Base

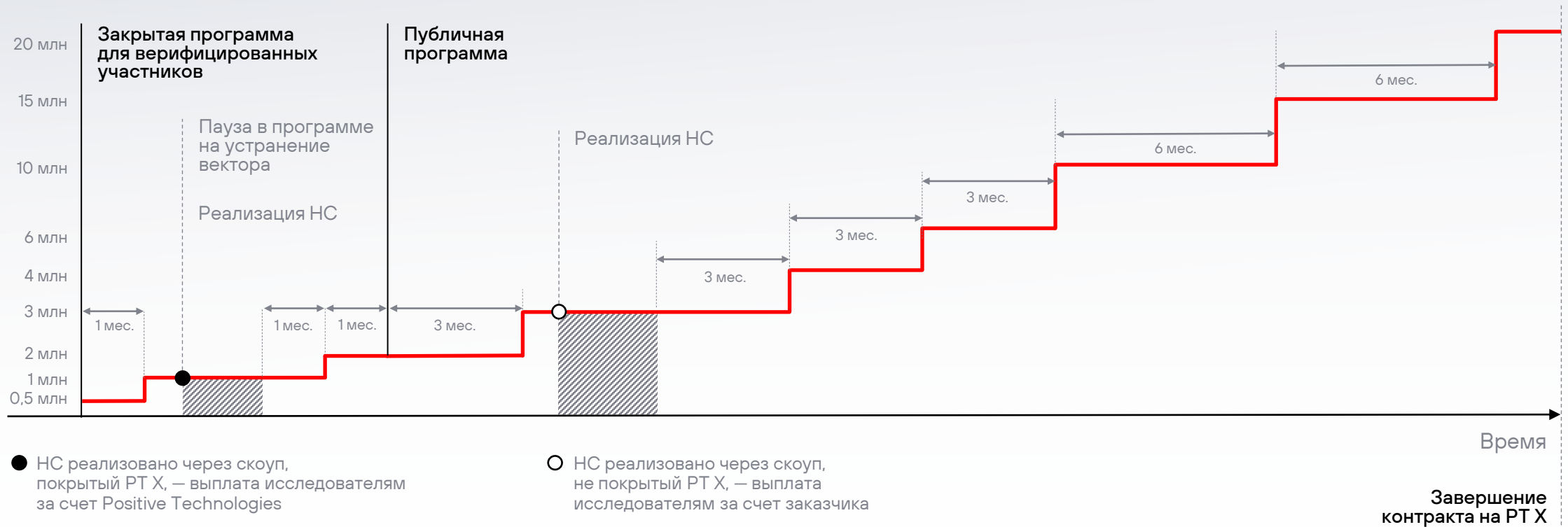


* План является ориентировочным и может быть скорректирован

Кибериспытания



Пример плана поэтапного повышения ставки вознаграждения исследователям* для PT X Pro



* План является ориентировочным и может быть скорректирован



Киберстрахование

Страхование риски



Убытки от простоя

- Остановка бизнес-процессов
- Перерыв в хозяйственной деятельности

Имущественные убытки

- Утрата электронных данных и (или) компьютерных программ
- Неправомерное использование вычислительных ресурсов
- Гибель и повреждение оборудования
- Хищение денежных средств

Расходы на восстановление

- Устранение угроз безопасности
- Консультации и другие услуги внешних специалистов программно-технической экспертизы
- Консультации в области репутации
- Извещение об утечке
- Юридические консультации
- Восстановление электронных данных

Ответственность перед третьими лицами

- Компрометации персональных данных третьих лиц
- Разглашение коммерческой тайны третьих лиц
- Причинение вреда жизни, здоровью, имуществу третьих лиц

Условия страхования*



Базовая
страховая сумма

x3

от стоимости РТ X

Максимальная
страховая сумма

500

млн руб.

Период
страхования

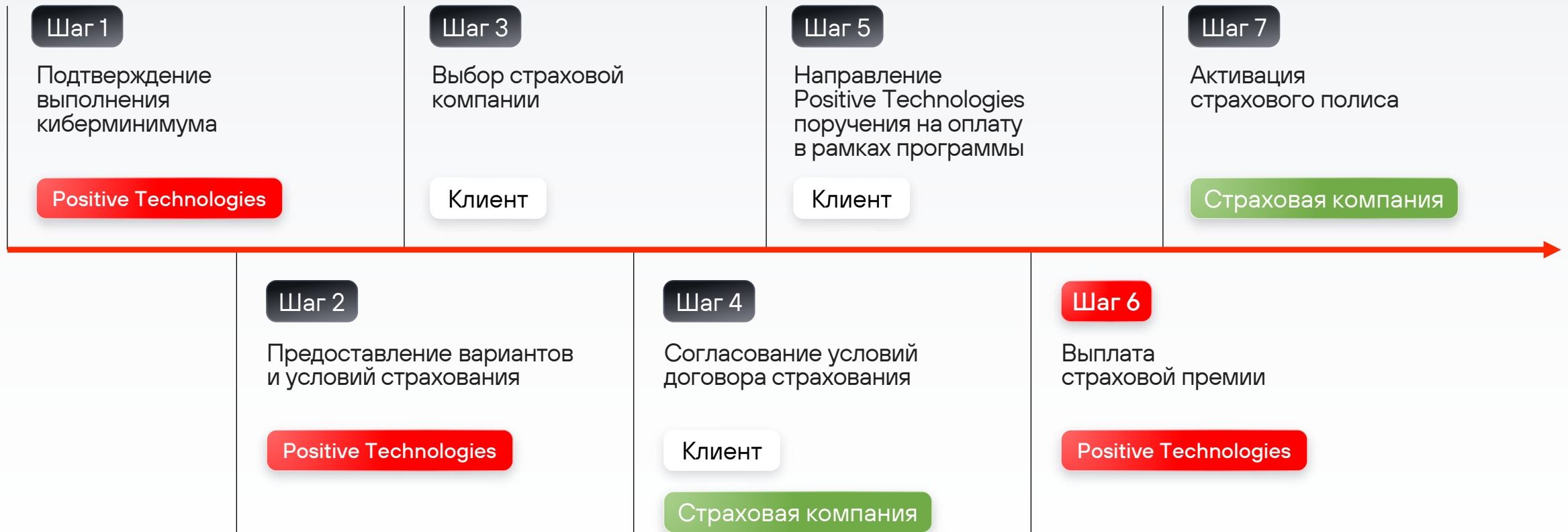
От подтверждения выполнения
киберминимума до окончания
использования РТ X

Страховые партнеры:



* Условия страхования могут меняться в зависимости от выбранной страховой компании (например, состав страхуемых рисков, ретроактивная дата и период обнаружения, франшиза или ограничения страхователя по виду хозяйственной деятельности)

Порядок страхования



Соблюдение киберминимума*

* При систематическом нарушении условий киберминимума Positive Technologies будет обязана уведомить об этом страховую компанию

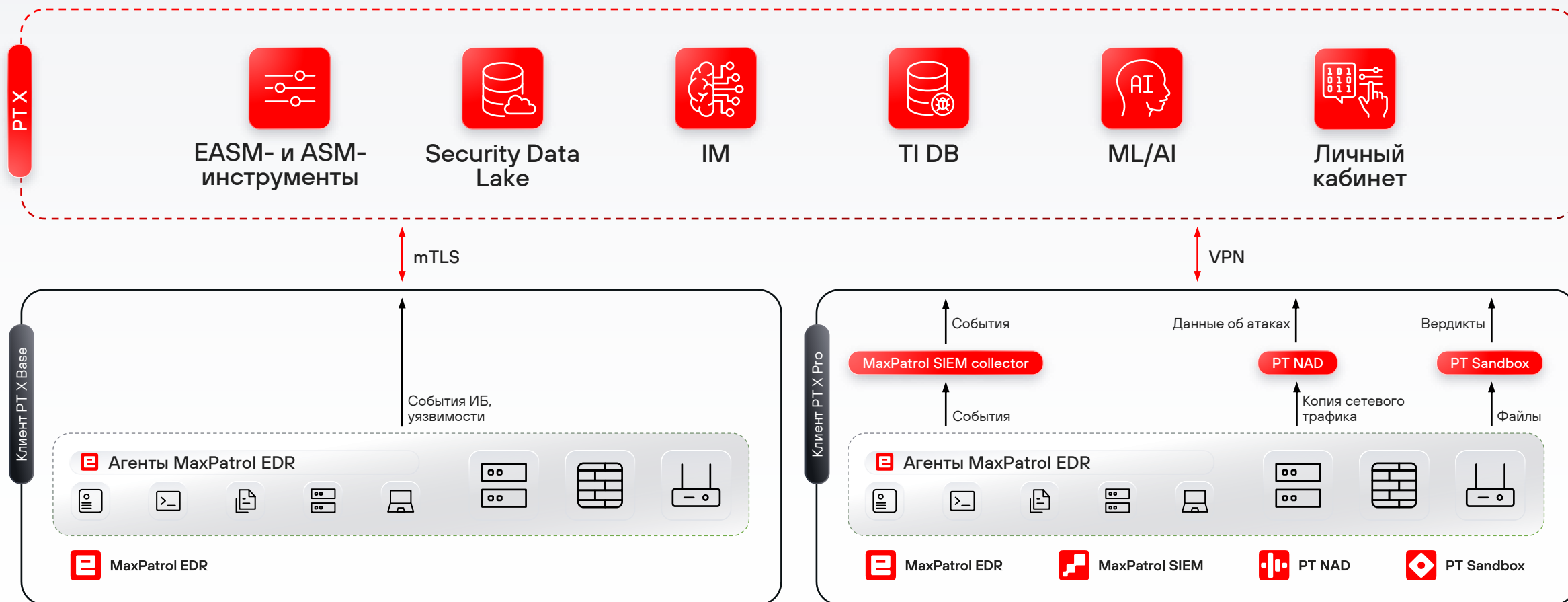
Порядок урегулирования



РТХ в деталях



Функциональная схема



Сравнение версий РТ Х



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 Antivirus**	MaxPatrol EDR Antivirus**
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	+	+
AI-технологии (ML, LLM)	+	+
ЭКСПЕРТИЗА		
Выявление инцидентов (24/7)	+	+
Реагирование на инциденты (24/7)	+	+
Continuous ML threat hunting	+	+
Поиск уязвимостей и ошибок конфигураций и рекомендации по их устранению	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		+

* Подключение дополнительных источников выполняется в случае приобретения лицензии РТ Х на полный объем ИТ-инфраструктуры клиента

** Функциональность будет доступна в Q3 2026 (ориентировочно)

Сравнение версий PT X



	PT X Base	PT X Pro				
	Стандартный уровень защиты от хакерских атак	Продвинутый уровень защиты от хакерских атак				
 MaxPatrol EDR	По количеству защищаемых хостов	≤ 1000	≤ 2000	≤ 3000	≤ 5000	≤ 10 000
 PT Sandbox	Анализ в сетевом трафике и в электронной почте	По количеству защищаемых хостов				
		1 Гбит/с	2 Гбит/с	5 Гбит/с	5 Гбит/с	10 Гбит/с
 PT NAD		1 инсталляция* с объемом анализируемого трафика				
 PT EASM	10% от количества хостов	10% от количества хостов				
 MaxPatrol SIEM		Состав данных, собираемых посредством MaxPatrol SIEM, определяется экспертами PT X Без ограничений по EPS				

* При необходимости количество инсталляций и объем трафика могут быть увеличены

Варианты реагирования



	На стороне пользователя	Нет предварительного согласования с пользователем	Есть предварительное согласование с пользователем
На стороне РТ X	Предоставление рекомендаций по реагированию (активы и действия с ними)	Получение разрешения на реагирование на затронутых активах и действия с ними; выполнение реагирования	Выполнение действий по реагированию на затронутых активах и информирование пользователя
На стороне пользователя	Выполнение рекомендаций	Выдача разрешения на реагирование	Выдача предварительных разрешений на реагирование (активы, на которых можно реагировать без предварительного согласования с пользователем)

Высокая вариативность реагирования



Доступно

>40

сценариев



- | | | |
|---|---|--|
| ▪ Удаление файлов | ▪ Получение списка сетевых соединений | ▪ Завершение процесса или дерева процессов |
| ▪ Проверка файлов | ▪ Перенаправление и отмена перенаправления DNS-запросов | ▪ Завершение работы, перезагрузка узла |
| ▪ Завершение сеанса учетной записи | ▪ Блокировка и разблокировка учетной записи | ▪ Выполнение команд в PowerShell или Bash |
| ▪ Сетевая изоляция, снятие изоляции узлов | ▪ Использование YARA-правил и проверки по хеш-сумме | ▪ Сбор дампа памяти для ретроспективного анализа |
| ▪ Выполнение кода на языке Lua | ▪ Блокировка и разблокировка IP-адреса | ▪ Помещение файлов в карантин и восстановление из него |
| ▪ Получение списка автозагрузки | ▪ Получение данных о пользователях | |

> Co-pilot для обработки подозрений на инциденты

Основная задача:
снижение TTD

- Вынесение предварительных вердиктов и автоматическая классификация ложноположительных срабатываний
 - Фокус на обработку действительно важных срабатываний
- Оценка опасности и приоритизация
 - Повышение скорости реакции на реальные угрозы
- Автосбор контекста, агрегация, обогащение, объединение срабатываний
 - Повышение скорости обработки данных
- Подготовка саммари, интерпретация отдельных сущностей (cmdline, процессы)
 - Повышение скорости принятия решений

> ML-based threat hunting по множеству инфраструктур

Основная задача:
недопущение пропуска атаки, снижение TTD

- Проактивный анализ активности процесса
 - Анализ с помощью модели, обученной на данных о множестве атак от разных сенсоров (хосты, сеть, песочницы)
- Широкий анализ вне рамок одной инфраструктуры
 - Выявление кросс-инфраструктурных паттернов атак
- Обогащение данными из Security Data Lake
 - Расширение контекста инцидентов актуальными TI-данными

> ML-верификация и приоритизация в EASM и ASM

Основная задача:
выявление активов, наиболее уязвимых к атакам

- Верификация вновь выявляемых угроз
 - Снижение шума (исключение false positives), группировка обнаруженных уязвимостей
- Формирование PoC
 - Повышение скорости верификации обнаруженных слабостей
- Ранжирование выявленных уязвимостей и мисконфигураций
 - Приоритизация и фокус на критически опасных уязвимостях

ML-технологии



> Генерация новой экспертизы средствами ML

Основная задача:
обеспечение полноты покрытия инфраструктуры

- Разработка новой экспертизы
 - Повышение скорости поддержки новых источников и покрытия новых угроз

> Co-pilot по применению экспертизы

Основная задача:
снижение TTD

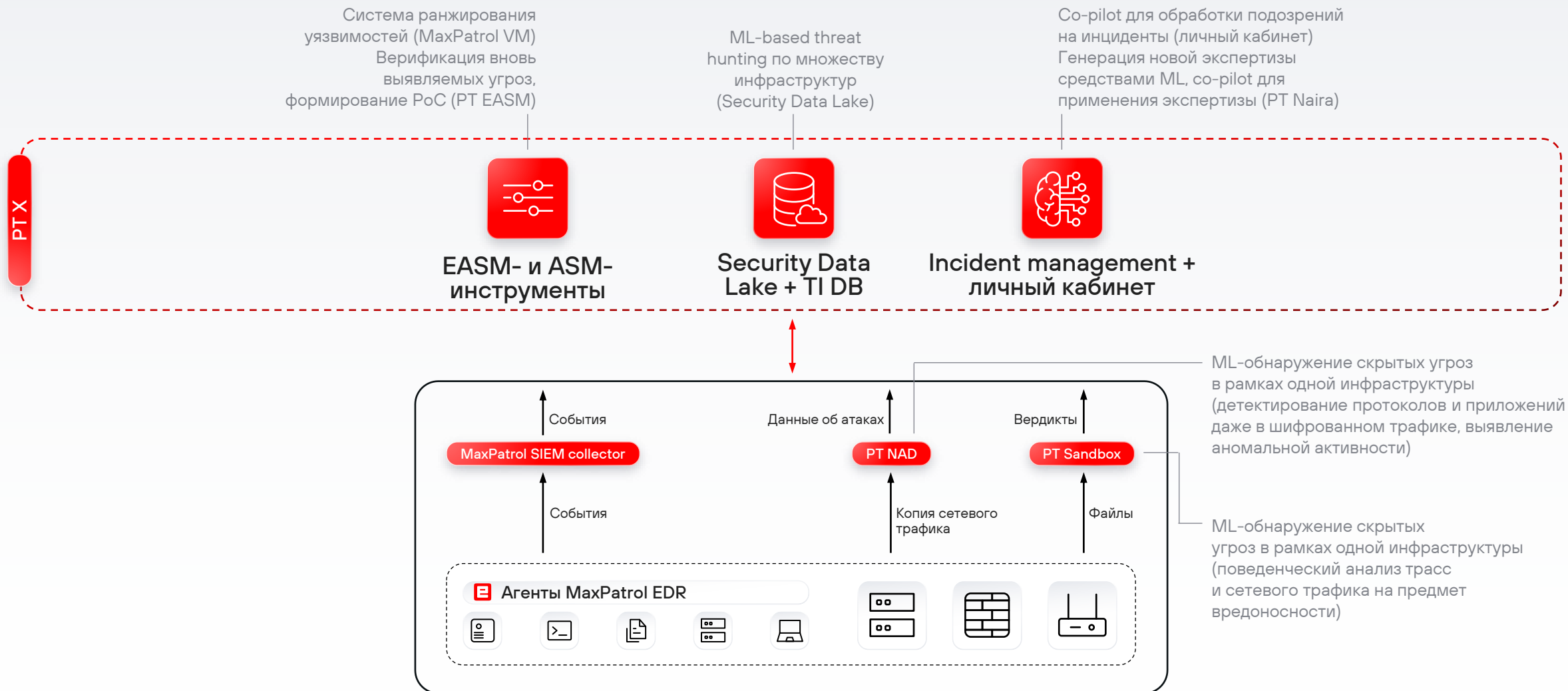
- Подсказки по срабатываниям и контекстные рекомендации
 - Повышение скорости принятия решений

> ML-обнаружение скрытых угроз в рамках одной инфраструктуры

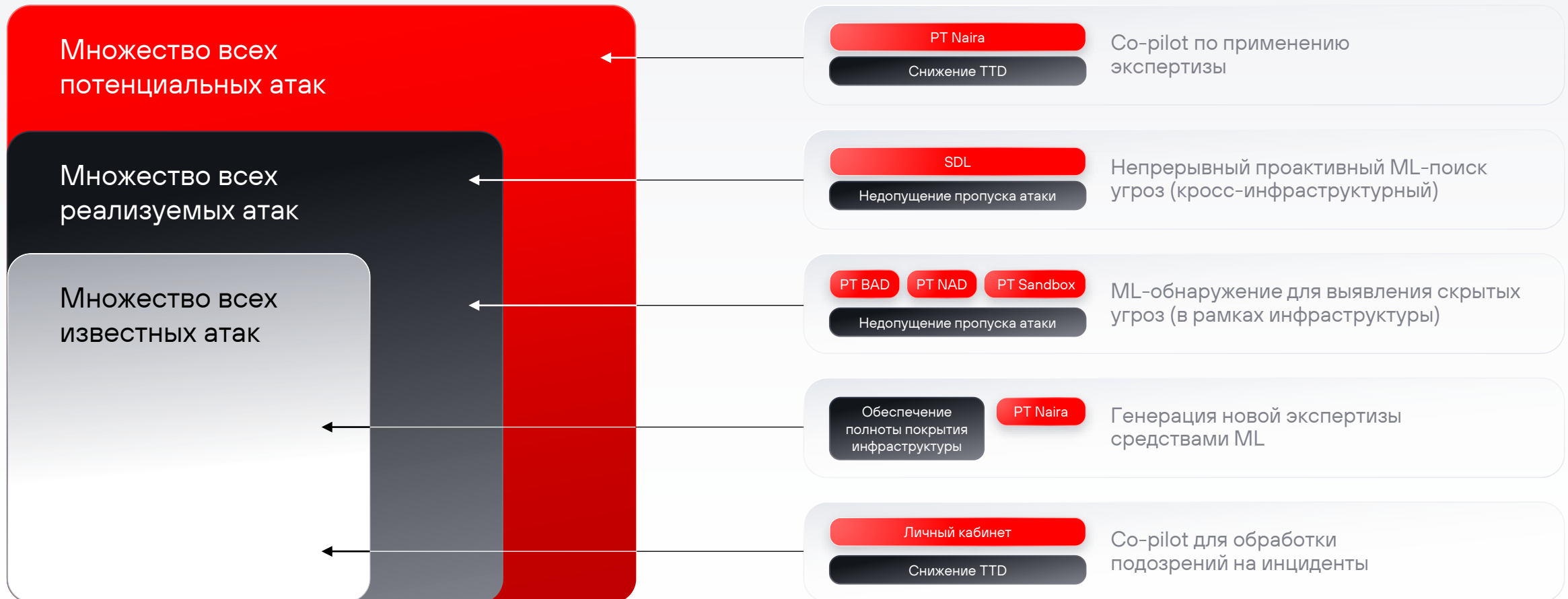
Основная задача:
недопущение пропуска атаки

- Выявление инцидентов вне корреляционной логики, анализ аномалий и скрытых паттернов
 - Обнаружение того, что не видят детерминированные правила, снижение риска пропуска атак

ML-технологии



ML-технологии в детектировании инцидентов



Датасет для ML



Продуктовая
обезличенная
телеметрия

Телеметрия
Standoff

Телеметрия
инфраструктуры
Positive
Technologies

Standoff



Standoff — кибербитва, в которой специалисты по информационной безопасности противостоят атакам белых хакеров, защищая компании из разных отраслей экономики на примере виртуальных государств

Красные команды

Белые хакеры — атакуют системы виртуальных государств. Например, пытаются украсть данные клиентов банка, взломать светофорную систему или остановить работу нефтеперерабатывающего завода

Синие команды

Специалисты по информационной безопасности — выявляют, расследуют атаки и реагируют на них

16 битв

Проходит
с 2016 года

400+ векторов атак,
900+ уязвимостей в одной битве

1500+ виртуальных машин, включая АСУ
ТП, для максимальной реалистичности

7500+ экспертов со всего мира
приняли участие в Standoff



Positive Technologies на кибериспытаниях



3 года

проверяем
защищенность компании
на кибериспытаниях

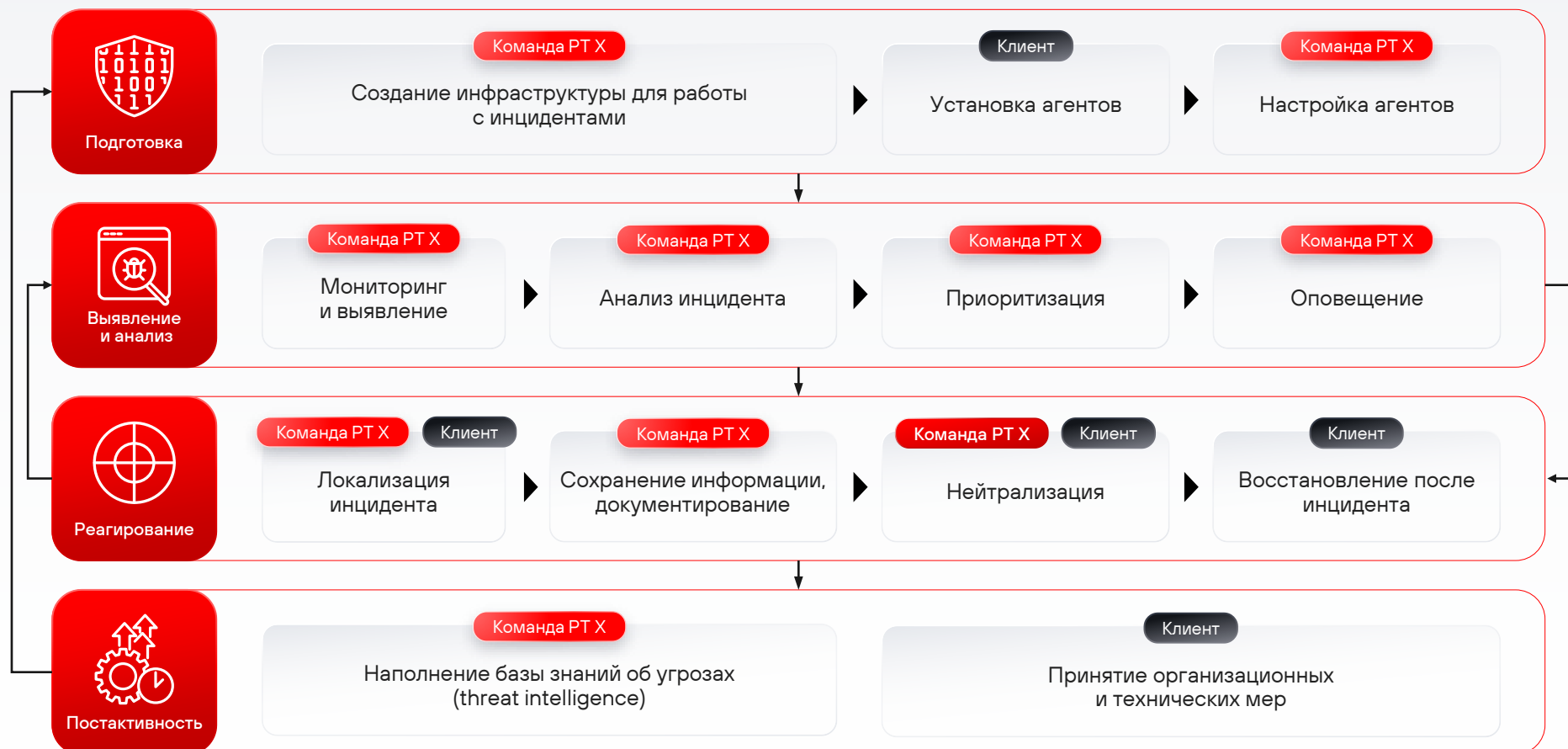
60 млн ₽

платим за реализацию
недопустимого события
Positive Technologies

0

недопустимых
событий реализовано

Зоны ответственности сторон



Зоны ответственности при предоставлении решения



	Клиент	Positive Technologies
Согласование сценариев реагирования	+	
Установка агентов MaxPatrol EDR, PT X*	+	
Поддержка работоспособности агентов	+	
Обеспечение сетевой связности между агентами и облачной платформой	+	
Обеспечение работоспособности облачной платформы		+
Обеспечение работоспособности дополнительных сенсоров и серверов агентов в ИТ-инфраструктуре клиента (опционально)	+	+
Управление конфигурацией политик регистрации событий безопасности на защищаемом узле с помощью агента MaxPatrol EDR, PT X		+
Выявление инцидентов ИБ		+
Реагирование на инциденты ИБ	+	+
Выявление уязвимостей и ошибок конфигураций		+
Устранение выявленных уязвимостей и ошибок конфигурации	+	
Подготовка отчетности		+

* Специализированное ПО для обнаружения угроз безопасности и реагирования на них устанавливается на конечные устройства

Поддерживаемые ОС



Windows 7	Windows 8/8.1	Windows 10	Windows 11	Windows Server 2016	Windows Server 2019
Windows Server 2022	Windows Server 2025	Astra Linux SE 1.7 (Орел, Воронеж)	Astra Linux SE 1.8 (Орел, Воронеж)	Astra Linux SE 1.3 (Орел)	Astra Linux CE 2.12 (Орел)
Debian 10	Debian 11	Debian 12	Debian 13	Oracle Linux 9	«ОСнова» 2.0 Оникс
RHEL 7	RHEL 8	RHEL 9	«РЕД ОС» 7.3	«РЕД ОС» 8	«Альт Сервер» 9
«Альт Сервер» 10.1	«Альт Сервер» 10.2	«Альт Сервер» 10.4	«Альт Рабочая станция» 10.1	«Альт Рабочая станция» 10.2	«Альт Рабочая станция» 10.4
Ubuntu 20.04	Ubuntu 22.04	Ubuntu 24.04	Ubuntu 25.04	CentOS 9	CentOS 10
AlterOS Desktop 7.5	«Мос.ОС» 12				

Подключение дополнительных источников*



Межсетевые
экраны, NGFW



WAF



IDS, IPS



NTA



VPN



Средства
антивирусной
защиты



MFA



Прочие
поддерживаемые
источники,
позволяющие
детектировать атаки



Лицензирование



Основная метрика лицензирования

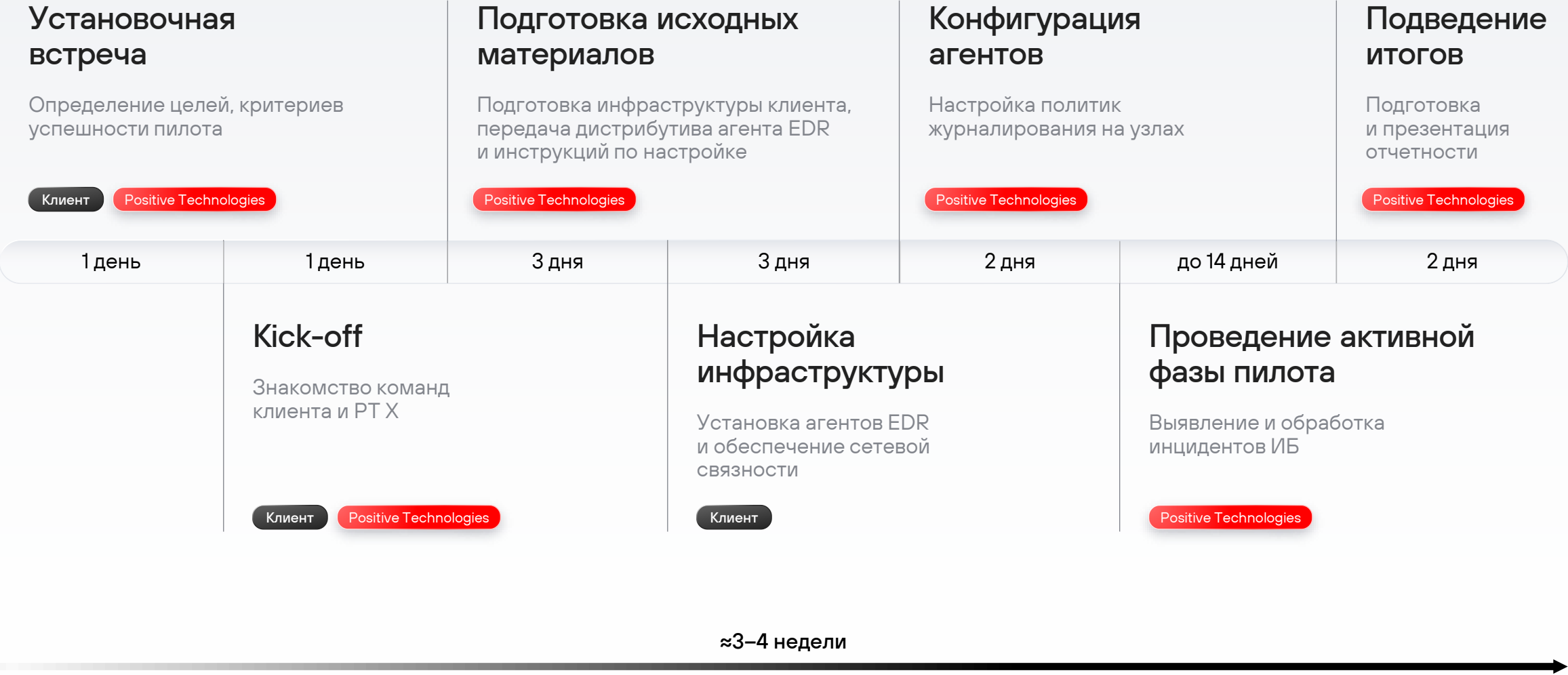
Количество
конечных устройств



Уровень решения (PT X Base или Pro)

Влияет на цену решения
за одно конечное устройство

Пилотный проект



Почему РТ Х



Все передовые технологии Positive Technologies, зарекомендовавшие себя на рынке, в одном решении



MaxPatrol EDR

- Единый агент для широкого круга задач: настройка журналирования, сбор событий, инвентаризация, автоматическое реагирование, сбор форензики и пр.
- Большой выбор действия для реагирования на угрозы
- Быстрая установка и гранулярная настройка
- Антивирус и собственная антивирусная лаборатория



PT NAD

- Более 130 определяемых протоколов на основе поведения, а не привязки к портам
- Глубина разбора протоколов: более 2000 заголовков в общей сложности
- Поведенческий анализ сессий, профилирование узлов и поиск отклонений, машинное обучение
- Стабильность работы на большом потоке



PT Sandbox

- Широкий список источников, поддерживаемых «из коробки»
- Сочетание методов статического, поведенческого и репутационного анализа
- Глубокая кастомизация образов и приманок
- Анализ снимков памяти, выявление ВПО, работающего на уровне загрузчика операционной системы
- Обновление экспертизы за 2,5 часа



PT EASM

- Полная видимость внешнего периметра, включая shadow IT и ресурсы подрядчиков
- AI-триаж в сочетании с экспертной верификацией
- Приоритизация уязвимостей на основе вероятности их реальной эксплуатации
- Мониторинг скомпрометированных учетных записей и индикаторов компрометации

Почему РТ Х



Признанные рынком топовые команды DFIR,
defensive и offensive security



PT ESC IR

Более 100 проектов
в год по расследованию
и ретроспективному анализу
в организациях по всему миру

DFIR



PT ESC SOC

Защищаем мероприятия
международного
и федерального уровня:

- государственные выборы
- международные
спортивные мероприятия
- фиджитал-турнир
«Игры будущего»

Defensive security



PT SWARM

Более 100 белых хакеров различных
профилей: инфраструктура,
имитация АPT-атак,
веб-приложения, системы
дистанционного банковского
обслуживания, смарт-контракты
и другие

Offensive security

Почему РТ Х



Возможность перейти
с РТ Х на собственный
SOC, сохранив продукты
и экспертизу



Большой Security
Data Lake с данными
о тысячах реальных атак
для обучения ML



Ответственность
за результат,
а не только за SLA

Планы развития РТ X на 2026 год



1

Личный кабинет клиента

Инциденты, активы, запросы,
уведомления, дашборды

2

Антивирус

В составе MaxPatrol EDR

3

Cloud PT Sandbox

Отсутствие потребности
«железного» оборудования
на стороне заказчика

4

PT Email Security

Почтовый шлюз безопасности,
антиспам, антифишинг

Реестр отечественного ПО



Программный комплекс РТ Х внесен в реестр отечественного ПО (№31827 от 26.01.2026)

Классы программного обеспечения

Основной класс:

- 03.17 Средства автоматизации процессов информационной безопасности

Другие классы:

- 03.02 Средства управления событиями информационной безопасности
- 03.07 Средства выявления и предотвращения целевых атак
- 03.14 Средства обнаружения и (или) предотвращения вторжений (атак)

РЕЕСТР
ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Российский

Евразийский

Введите запрос

Меню

Главная > Реестр ПО > Программный комплекс РТ Х

Программный комплекс РТ Х

Сведения обновлены 21.03.2026 | Реестр российского ПО

Реестровая запись №31827 от 26.01.2026

Произведена на основании поручения Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 26.01.2026 по протоколу заседания экспертного совета от 14.01.2026 №10пр

Правообладатели программного обеспечения

Полное наименование (коммерческая организация без преобладающего иностранного участия)	Сокращенное наименование организации	Организационно-правовая форма
Акционерное общество "Позитив Текнолоджиз"	АО "Позитив Текнолоджиз"	Непубличные акционерные общества
Государство регистрации в качестве юридического лица:	Основной государственный регистрационный номер	Идентификационный номер (ИНН)
Россия	1077761087117	7718668887



**PT X остановил
APT-группировку**

Хронология событий



12.01

Успешная эксплуатация цепочки известных уязвимостей на сервере корпоративного мессенджера

13.01

Горизонтальное перемещение с использованием привилегированных учетных записей и захват части доменной инфраструктуры

14–25.01

Захват ключевых узлов инфраструктуры и сокрытие собственного присутствия

22.01



Старт внедрения PT X.
Установка первых агентов EDR

26.01

Расследование инцидента (1 час 55 мин):

- выявлены четыре скомпрометированные учетные записи
- обнаружены следы утилиты LaZagne — инструмента для хищения сохраненных паролей
- выявлены следы компрометации служб сертификатов Active Directory (AD CS)
- выявлены другие скомпрометированные узлы, не оснащенные PT X

Локализация инцидента:

- Скомпрометированные узлы и учетные записи заблокированы
- C2-сервер злоумышленников заблокирован
- Пароли сброшены
- Сервер корпоративного мессенджера изолирован от интернета

Выполнена атрибуция злоумышленников:

ими оказались неизвестные PhantomCore

26–28.01

Восстановление:

- Переустановка служб сертификатов Active Directory
- Переустановка корпоративного мессенджера
- Продолжение внедрения агентов EDR для обеспечения видимости

Инцидент в цифрах



14

ДНЕЙ

атакующие находились
в инфраструктуре до обнаружения

7

УЗЛОВ

были скомпрометированы

500

конечных узлов
просканированы на наличие
следов компрометации

2

УЧЕТНЫЕ ЗАПИСИ

доменного администратора
скомпрометированы

3

УЯЗВИМОСТИ

успешно проэксплуатированы
атакующими

Рекомендации после инцидента



1

Выполнить поиск уязвимостей на периметре с помощью PT X

2

Провести аудит учетных записей и усилить парольную политику в домене

3

Провести аудит групп безопасности, чтобы проверить, не закрепились ли злоумышленники в домене при помощи техники T1098 («Манипуляции с учетной записью»)

4

Настроить логирование системы доменных имен (DNS), чтобы выявить попытки обращения к новым C2-серверам

5

Провести зануление доменных зон .online и .space, которые зачастую используют PhantomCore



Спасибо!

