PT Security Lakehouse

PT Security Lakehouse

Единая платформа данных ИБ

СОБИРАТЬ | ХРАНИТЬ | ИСПОЛЬЗОВАТЬ БЕЗ ОГРАНИЧЕНИЙ

PT Security Lakehouse — это единая платформа для централизованной работы с данными информационной безопасности.

Любая аналитика и любой ИИ-агент в SOC работают настолько хорошо, насколько полны и доступны данные. PT Security Lakehouse формирует этот фундамент: единый массив событий ИБ, доступный для решения любых задач сегодня и завтра.

Что дает PT Security Lakehouse

Единое хранилище данных ИБ

Консолидация данных продуктов ИБ на одной платформе. Снижает нагрузку на основные хранилища и решает сложности долгосрочного хранения

Открытая масштабируемая архитектура

Петабайты данных, миллионы событий в секунду и открытые форматы хранения – платформа растет вместе с вашими потребностями, оставаясь открытой и гибкой

Полный поток данных

Принимает события и телеметрию без предварительной фильтрации источников. Не требуется отсекать часть потока данных из-за лицензий или ограничений архитектуры и выносить их в отдельные хранилища

Продвинутая аналитика и ML

Интеграция и взаимное обогащение данных из разных источников улучшают качество ML-моделей

Ретроспективный поиск угроз

Расследование и проверка гипотез на полной истории. Данные всегда «теплые» и остаются доступными для поиска, без разморозки архива и выгрузок из отдельных систем

Next-gen ИБ

Агентским системам нужен максимально широкий контекст.
PT Security Lakehouse открывает любой срез данных на всю глубину хранения, повышая точность и скорость LLM-агентов

Место в контуре ИБ

Модель развертывания

Разворачивается на инфраструктуре заказчика или в публичном облаке. Данные остаются под контролем заказчика

Экосистема PT

Нативные интеграции с продуктами Positive Technologies и единый слой хранения без лишних копий данных

Весь ландшафт

Открытая архитектура без привязки к вендору: интегрируйте данные из любых продуктов, которые уже есть в инфраструктуре

Запросить пилот PT Security Lakehouse

ptsecurity.com/pt-security-lakehouse

Когда нужна платформа PT Security Lakehouse

Большие объемы данных, долгий срок хранения и разнородность источников

Потребность в реализации расширенных сценариев работы с данными: агентские системы, поведенческая аналитика, машинное обучение, бизнес-отчетность

Кому полезна платформа

SOC
Единое аналитическое пространство

CISO
Прозрачная стоимость владения и открытая архитектура

ML-инженеры
Данные в одном месте, привычный стек технологий

Как работает PT Security Lakehouse

1 Сбор и обработка

Принимает данные из продуктов Positive Technologies и из любых других источников контура компании:

- На потоке события нормализуются и обогащаются
- Нужный срез может уйти в средства обнаружения
- Основной массив отправляется в хранилище

2 Хранение

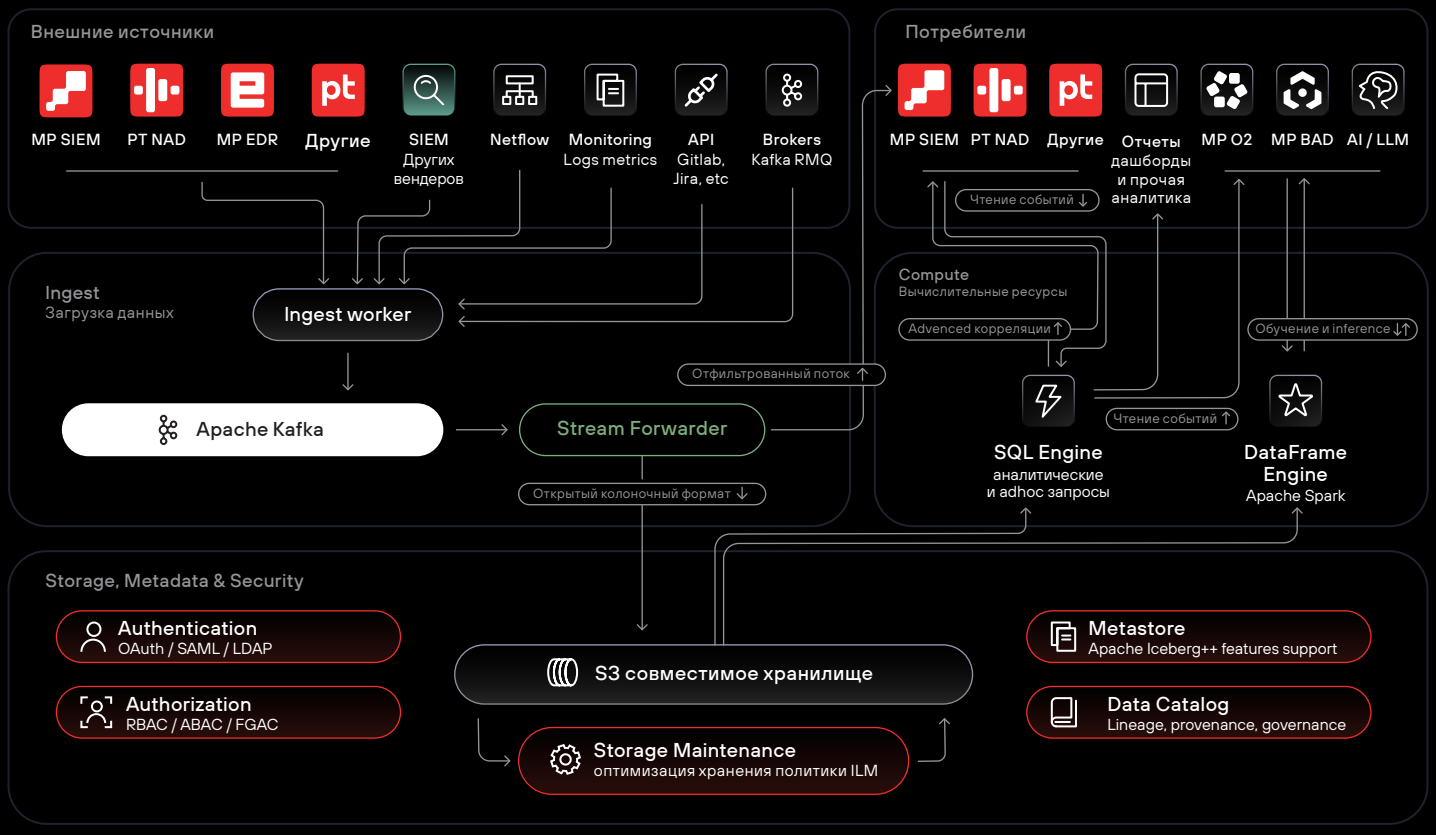
Данные записываются в S3-совместимое хранилище. Слой хранения рассчитан на годы и большие объемы:

- Автоматическая оптимизация хранения и политики жизненного цикла ускоряют доступ данных
- Вся история остается доступной для поиска, без выгрузки массива в холодный архив

3 Вычисления и доступ

Отдельный вычислительный слой независимо масштабируется и предоставляет доступ к данным из единого хранилища:

- Пользователи и внешние системы выполняют поиск, расследования и произвольные запросы
- Датасеты для ML готовятся встроенными средствами платформы либо инструментами экосистемы работы с большими данными



Запросить пилот PT Security Lakehouse

ptsecurity.com/pt-security-lakehouse

Продукт построен на технологии Security Lakehouse

Security Lakehouse — это технологическая архитектура Positive Technologies для работы с большими объемами данных безопасности