# PT Platform 187

## РЕАЛИЗАЦИЯ ОСНОВНЫХ ТРЕБОВАНИЙ 187-ФЗ И ФУНКЦИЙ ЦЕНТРОВ ГОССОПКА ДЛЯ НЕБОЛЬШИХ ИНФРАСТРУКТУР

### КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА

+ **Соответствие требованиям законодательства.**
  PT Platform 187 помогает реализовать меры защиты объектов КИИ в соответствии с требованиями ФСТЭК России и построить центры ГосСОПКА в соответствии с требованиями ФСБ России.
+ **Быстрое развертывание.**
  Единый инсталлятор помогает оперативно внедрить платформу с минимальными трудозатратами и начать взаимодействие с ГосСОПКА.
+ **Собственный мини-SOC из коробки.**
  Платформа включает базовые технические средства, необходимые для SOC, и помогает выстроить процессы информационной безопасности, расширить внутреннюю экспертизу и повысить эффективность ИБ.
+ **Единая система аутентификации.**
  Авторизация в единой системе идентификации дает пользователю автоматический доступ ко всем возможностям платформы.

По требованиям законодательства организации со значимыми объектами критических информационных инфраструктур (КИИ) обязаны построить систему безопасности IT-инфраструктуры и взаимодействовать с ГосСОПКА. Для этого необходимо реализовать следующие основные функции:

+ инвентаризация IT-инфраструктуры,
+ выявление уязвимостей и контроль их устранения,
+ оценка соответствия стандартам,
+ анализ событий безопасности и выявление инцидентов,
+ обнаружение кибератак на сетевом и прикладном уровнях,
+ выявление и блокировка вредоносного ПО,
+ управление инцидентами,
+ подключение к Национальному координационному центру по компьютерным инцидентам (НКЦКИ).

### РЕШЕНИЕ

PT Platform 187 — программно-аппаратный комплекс для реализации основных функций безопасности значимых объектов КИИ и взаимодействия с главным центром ГосСОПКА. Платформа включает в себя набор технических средств, который помогает выполнить основные требования законодательства, автоматизирует процессы ИБ и значительно повышает их эффективность.

#### ДЛЯ НЕБОЛЬШИХ IT-ИНФРАСТРУКТУР

Подходит организациям с инфраструктурой до 250 сетевых узлов* и территориальным подразделениям крупных организаций как часть сегмента ГосСОПКА.

#### ПЯТЬ ПРОДУКТОВ В ОДНОМ

На сервере развернуты MaxPatrol SIEM, MaxPatrol 8, PT Network Attack Discovery, PT MultiScanner, «ПТ Ведомственный центр».

#### МАКСИМАЛЬНАЯ ИНТЕГРАЦИЯ

Все продукты платформы уже интегрированы и обеспечивают максимальную совместимость компонентов.

+ Единая аппаратная платформа на одном сервере
+ Пропускная способность — до 100 Мбит/с
+ Время хранения информации об инцидентах — до 5 лет в режиме архива
+ Проверка объектов на наличие вредоносного ПО — до 3000 FPH (files per hour)
+ Гарантия на оборудование — 5 лет

* Под сетевым узлом подразумевается любой элемент IT-инфраструктуры, подключенный к сети, — сервер, компьютер, принтер и т. п.

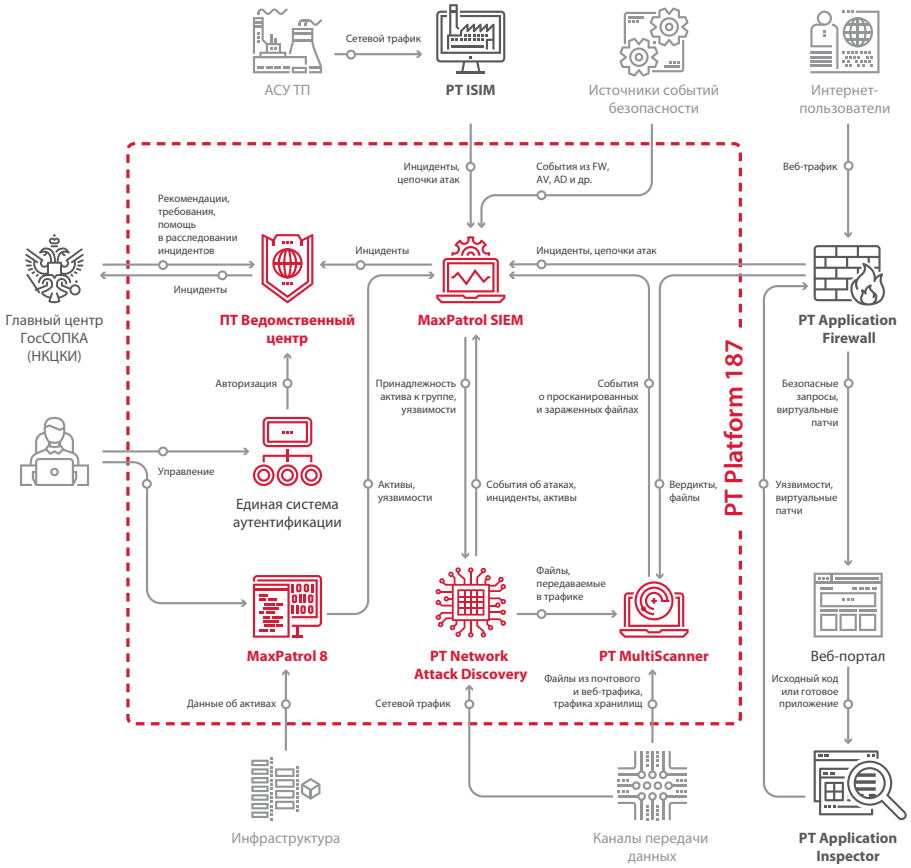
## ПЛАТФОРМА ПОЗВОЛЯЕТ:

- Проводить непрерывную инвентаризацию информационных ресурсов и поддерживать сведения об инфраструктуре в актуальном состоянии
- Проводить анализ защищенности и выявлять уязвимости
- Автоматизировать процесс управления уязвимостями и осуществлять контроль соответствия требованиям
- Анализировать события безопасности из различных источников и выявлять инциденты
- Анализировать сетевой трафик и выявлять атаки, сетевые аномалии, скрытое присутствие, активность вредоносного ПО
- Проводить многопоточную проверку входящих файлов и предотвращать распространение вредоносного ПО
- Управлять процессом реагирования на инциденты и проводить расследования
- Взаимодействовать с НКЦКИ

## ХАРАКТЕРИСТИКИ АППАРАТНОЙ ПЛАТФОРМЫ:

- 64 × Core 2,4 ГГц;
- 256 ГБ ОЗУ;
- 20 ТБ жесткого диска;
- 6 × 1 Гбит/с — сетевой интерфейс;
- дополнительная опция: архивное хранение — СХД емкостью 40 ТБ

## АРХИТЕКТУРА ПЛАТФОРМЫ




Ядро платформы — система MaxPatrol SIEM. Она формирует модель защищаемой IT-инфраструктуры, что позволяет лучше понимать ее уязвимые места, оценивать вероятность успешного осуществления атак и упрощает расследование инцидентов. Модель инфраструктуры обогащается сведениями из MaxPatrol 8 и PT Network Attack Discovery о конфигурации, уязвимостях, программном и аппаратном обеспечении информационных ресурсов.

MaxPatrol SIEM собирает события безопасности из различных источников, в том числе из PT Network Attack Discovery и PT MultiScanner, и по правилам корреляции выявляет инциденты. Информация об инцидентах передается в «ПТ Ведомственный центр» для регистрации, реагирования и отправки в НКЦКИ.

Для выявления вредоносного контента PT Network Attack Discovery передает файлы из сетевого трафика в PT MultiScanner. В случае обнаружения зараженного файла сообщение об инциденте уходит из PT MultiScanner в MaxPatrol SIEM, где автоматически срабатывает уведомление. Это дает возможность специалисту ИБ оперативно выявить и заблокировать распространение вредоносного ПО.

- PT ISIM подключается к платформе для обеспечения непрерывного мониторинга промышленной сети предприятия и выявления кибератак на компоненты АСУ ТП.
- PT Application Firewall используется для выявления и блокирования атак на веб-приложения.
- PT Application Inspector интегрируется с PT Application Firewall для выявления уязвимостей исходного кода и готового приложения и для защиты от атак на время их исправления.

## О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.

POSITIVE TECHNOLOGIES

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays