

PT Platform 187: Решение по защите компактных объектов КИИ

POSITIVE TECHNOLOGIES

ptsecurity.com

1

В 2013 году вышел Указ
Президента №31с для
создания ГосСОПКА



2

Вступил силу 187-ФЗ
«О безопасности
критической
информационной
инфраструктуры
Российской Федерации»



3

Субъекты КИИ
должны выполнить
требования
законодательства

PT Platform 187

Реализация основных требований 187-ФЗ
и функций центров ГосСОПКА
для небольших обособленных инфраструктур





MaxPatrol SIEM

Система мониторинга событий и выявления инцидентов



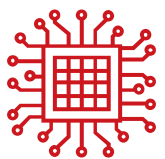
MaxPatrol 8

Система контроля защищенности



PT MultiScanner

Система выявления вредоносного контента



PT Network Attack Discovery

Система комплексного анализа сетевого трафика



ПТ Ведомственный центр

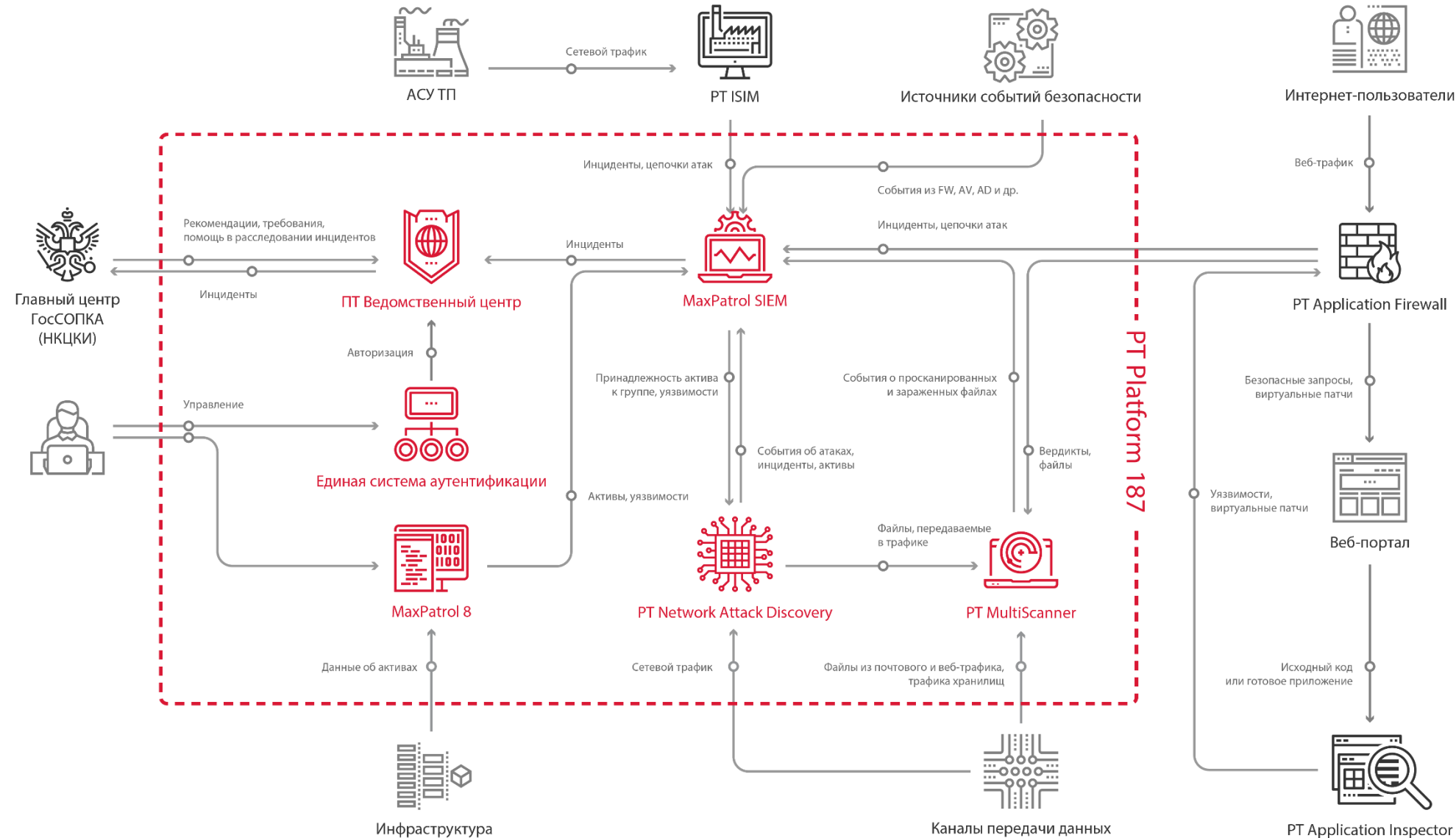
Система управления инцидентами и взаимодействия с НКЦКИ

Опциональное подключение:

- + PT ISIM
- + PT Application Firewall
- + PT Application Inspector
- + Доп. хранилище до 36 ТБ

Архитектура PT Platform 187

POSITIVE TECHNOLOGIES



Для небольших
инфраструктур –
не более 250 узлов



Продажи в виде
ПАК = сервер + ПО





В реестре российского ПО:

- MaxPatrol 8
- MaxPatrol SIEM
- PT MultiScanner
- PT Network Attack Discovery
- ПТ Ведомственный центр **coming soon**



Сертификаты ФСТЭК России:

- MaxPatrol 8 – сертификат № 2922
- MaxPatrol SIEM – сертификат № 3734
- PT MultiScanner **coming soon**
- PT Network Attack Discovery **coming soon**



до 250 узлов
включаются в мониторинг
MaxPatrol SIEM
и MaxPatrol 8



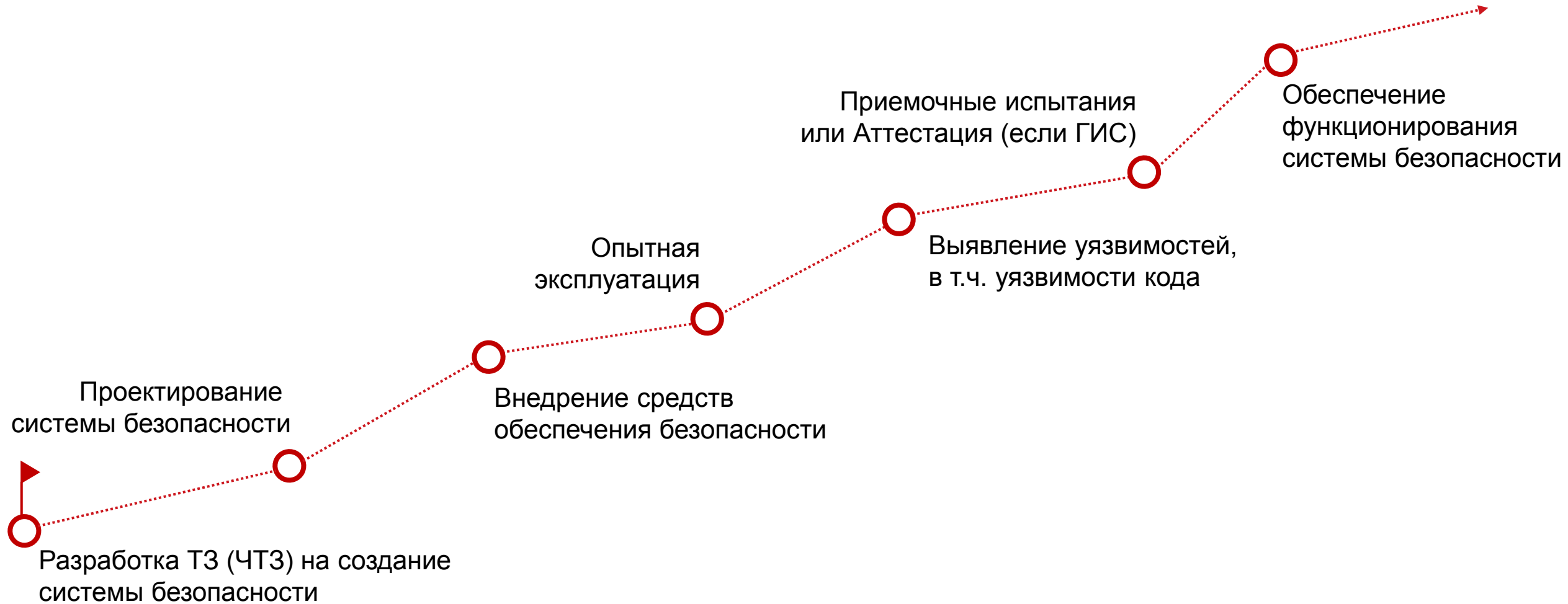
до 100 Мбит/с
пропускная способность
PT Network Attack
Discovery



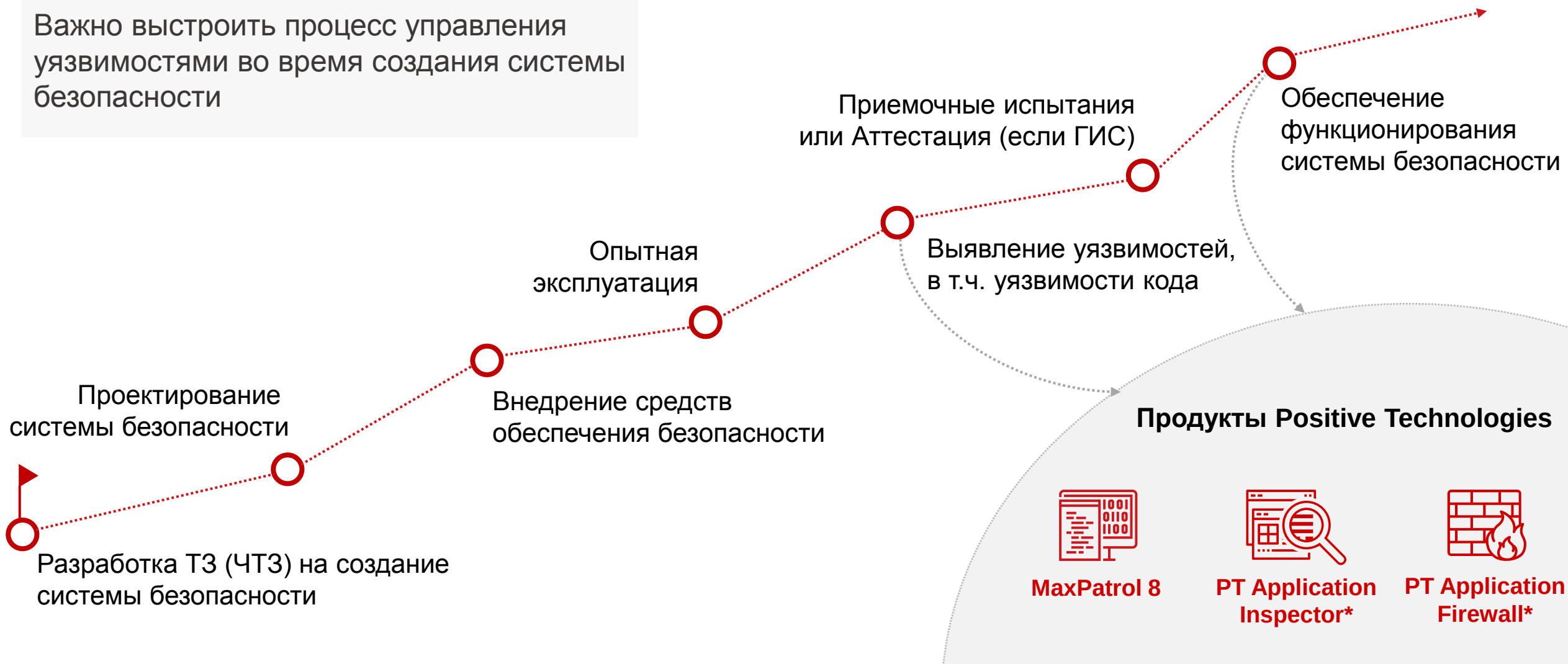
до 3000 файлов
в час - пропускная способность
PT MultiScanner

Покры́тие требований регуляторов

ФСТЭК России



Важно выстроить процесс управления уязвимостями во время создания системы безопасности



**подключаются к PT Platform 187 в случае необходимости защиты веб-приложений*

АУД.1	Инвентаризация информационных ресурсов
АУД.2	Анализ уязвимостей и их устранение
АУД.10	Проведение внутренних аудитов
АУД.11	Проведение внешних аудитов



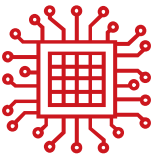
MaxPatrol 8

АУД.1	Инвентаризация информационных ресурсов
АУД.4	Регистрация событий безопасности
АУД.6	Защита информации о событиях безопасности
АУД.7	Мониторинг безопасности
АУД.8	Реагирование на сбои при регистрации событий безопасности
ИНЦ.1	Выявление компьютерных инцидентов
ИНЦ.2	Информирование о компьютерных инцидентах
ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов



MaxPatrol SIEM

АУД.5	Контроль и анализ сетевого трафика
СОВ.1	Обнаружение и предотвращение компьютерных атак
СОВ.2	Обновление базы решающих правил



PT Network Attack
Discovery

АВЗ.2	Антивирусная защита электронной почты и иных сервисов
АВЗ.3	Контроль использования архивных, исполняемых и зашифрованных файлов
АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
АВЗ.5	Использование средств антивирусной защиты различных производителей
ЗИС.7	Использование эмулятора среды функционирования программного обеспечения ("песочница")

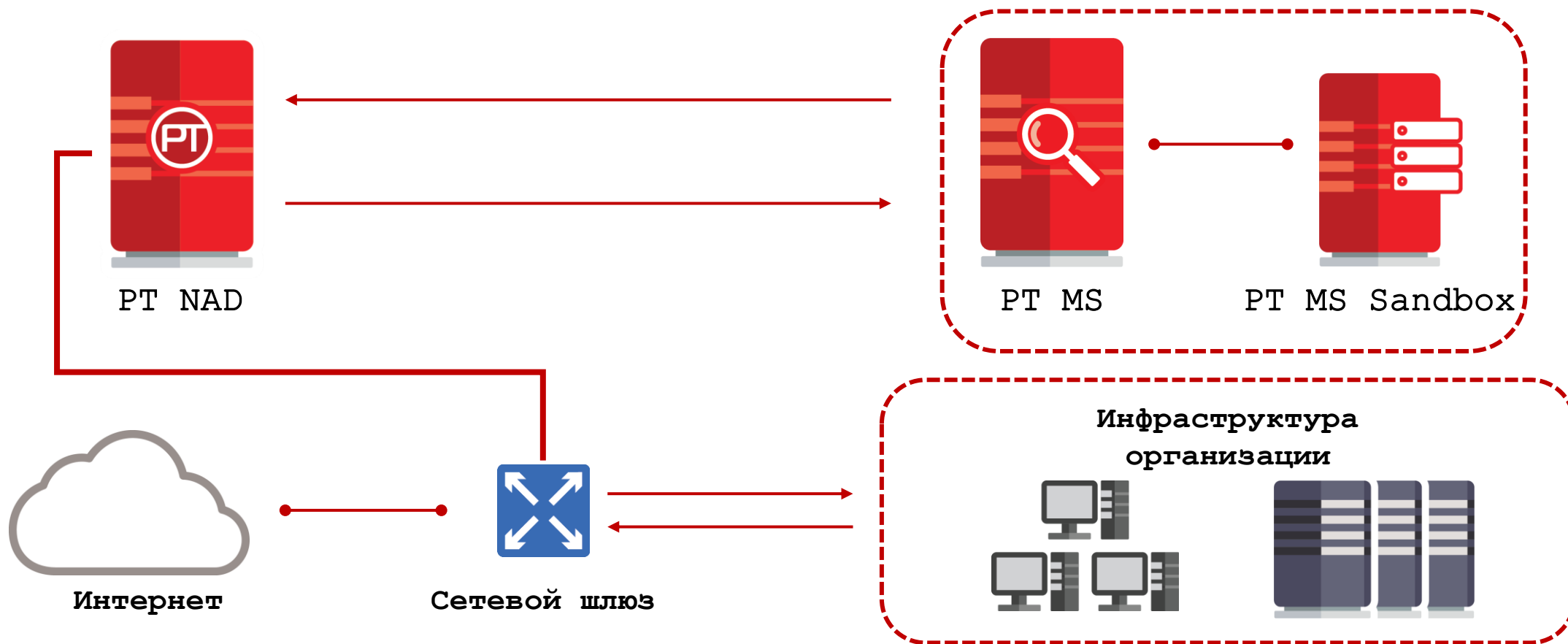


PT MultiScanner

- Детектирование угроз
- Поиск следов компрометации
- Хранение контекста атаки

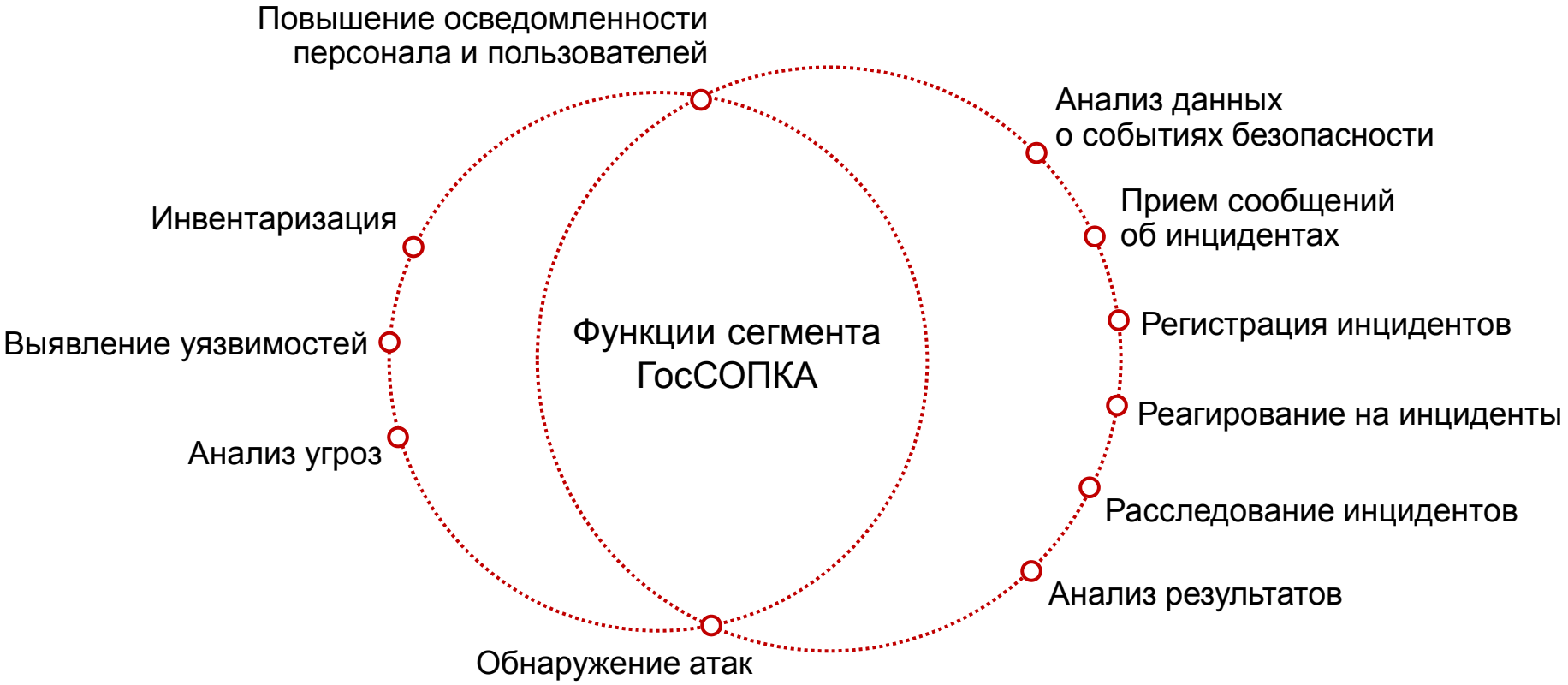
- Выявление ВПО
- Локализация угроз
- Защита актуальных каналов

- Выявление скрытых и новых угроз



Покрытие требований регуляторов

ФСБ России



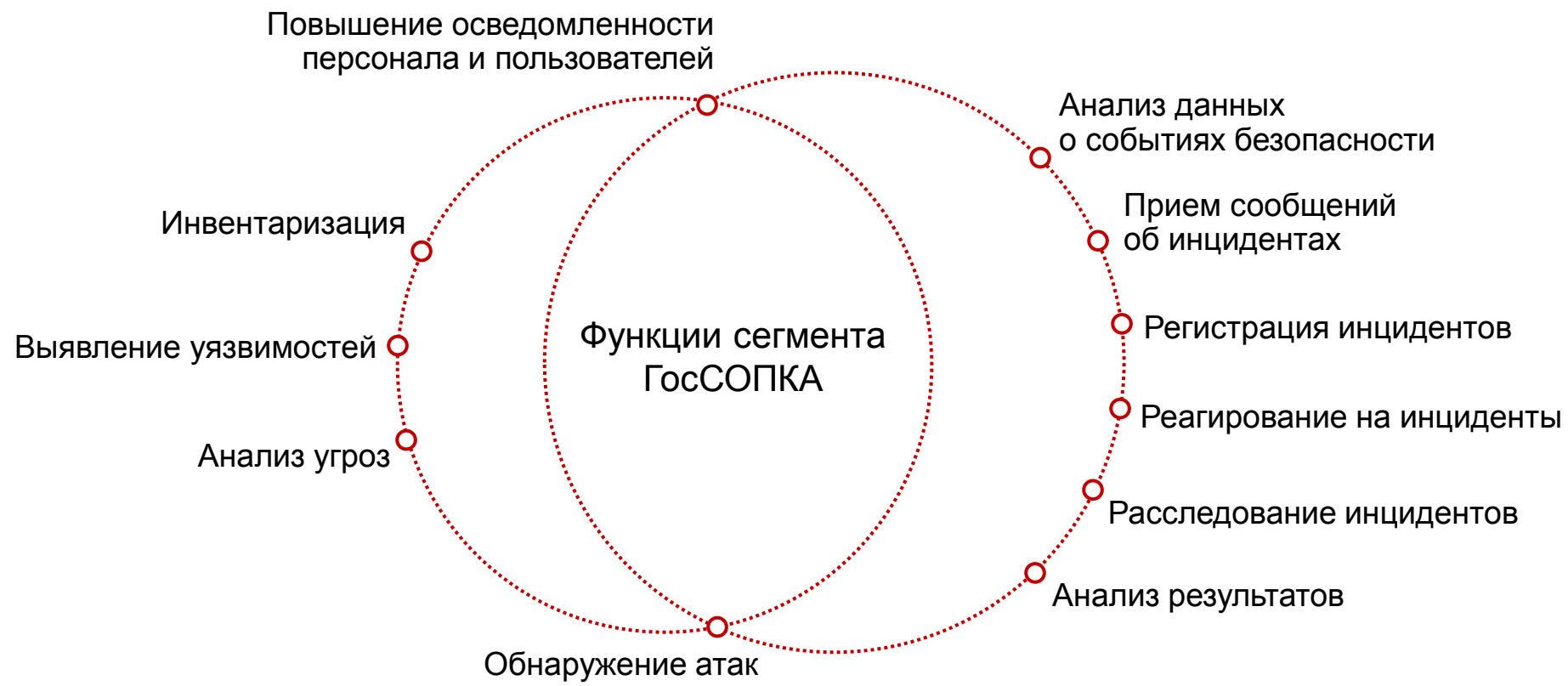
Методические рекомендации ФСБ России по построению центров ГосСОПКА



MaxPatrol 8



MaxPatrol SIEM



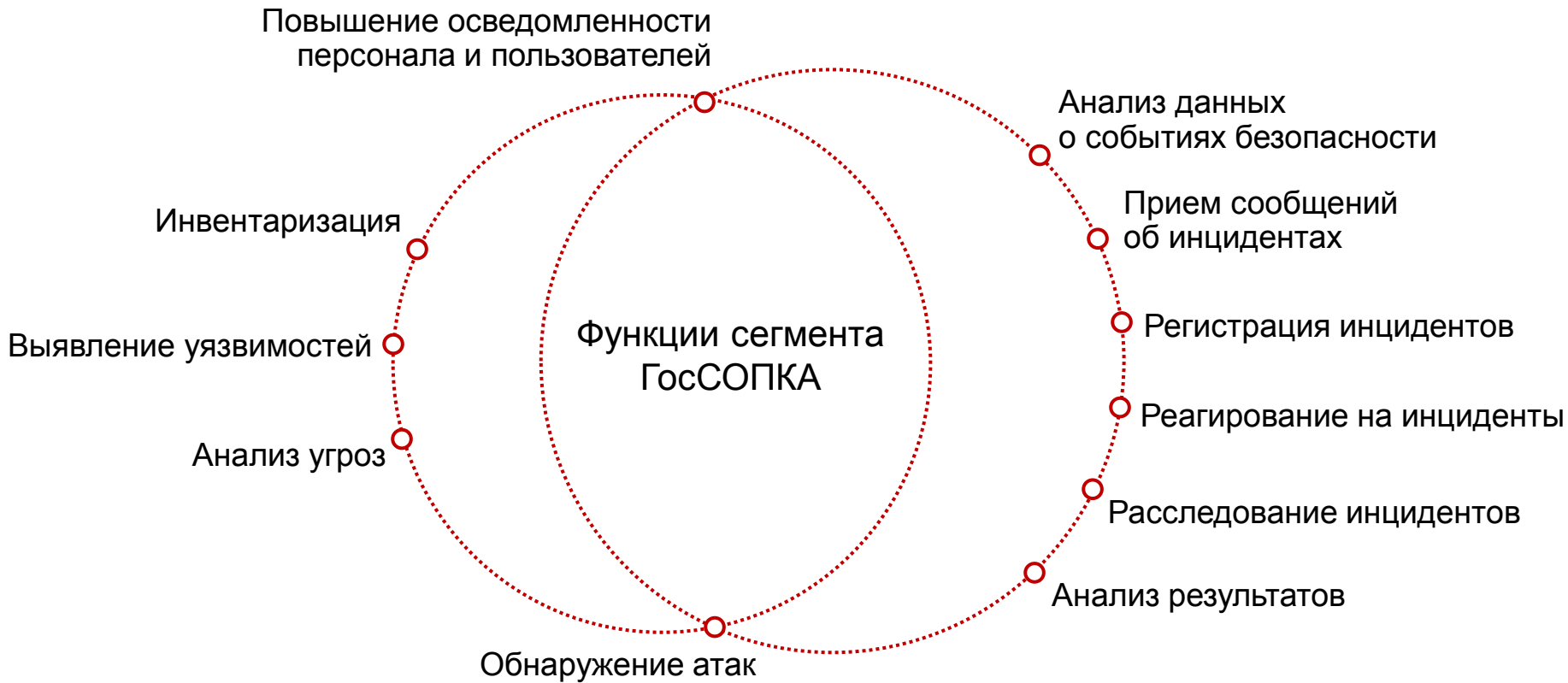
Методические рекомендации ФСБ России по построению центров ГосСОПКА



MaxPatrol 8

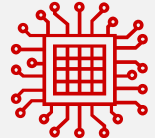


MaxPatrol SIEM





PT MultiScanner



PT Network Attack Discovery

Методические рекомендации ФСБ России по построению центров ГосСОПКА

POSITIVE TECHNOLOGIES



Приняты:

Приказ ФСБ России от 24.07.2018 № 366
о Национальном координационном центре
по компьютерным инцидентам»

Приказ ФСБ России от 24.07.2018 № 367
об утверждении Перечня информации,
представляемой в ГосСОПКА, и Порядка
представления информации в ГосСОПКА

Приказ ФСБ России от 24.07.2018 № 368
об утверждении Порядка обмена информацией о
компьютерных инцидентах

Проекты:

Приказ ФСБ России об утверждении Требований
к средствам ГосСОПКА

Приказ ФСБ России об утверждении порядка,
технических условий установки и эксплуатации средств
ГосСОПКА

Приказ ФСБ России об утверждении Порядка
информирования ФСБ России о компьютерных
инцидентах, реагирования на них, принятия мер по
ликвидации последствий компьютерных атак



MaxPatrol SIEM

Средства ГосСОПКА

в части предоставления
детализированных данных о
конкретном инциденте

- Сбор и первичная обработка событий ИБ из различных источников
- Автоматический анализ событий ИБ и выявление инцидентов
- Ретроспективный анализ событий ИБ

Проект требований ФСБ России к средствам ГосСОПКА: предупреждение

POSITIVE TECHNOLOGIES

ПРОДУКТЫ POSITIVE TECHNOLOGIES

- Сбор и обработка сведений об инфраструктуре:
инвентаризационная + справочная информация
- Сбор и обработка сведений об уязвимостях
и недостатках в настройке ПО
- Учет угроз безопасности информации



**ПТ Ведомственный
центр**



MaxPatrol 8



MaxPatrol SIEM

Проект требований ФСБ России к средствам ГосСОПКА: ликвидация

POSITIVE TECHNOLOGIES

- Учет и обработка инцидентов
- Управление процессами реагирования на инциденты и ликвидации последствий
- Взаимодействие с НКЦКИ
- Информационно-аналитическое сопровождение

ПРОДУКТЫ POSITIVE TECHNOLOGIES



**ПТ Ведомственный
центр**



MaxPatrol SIEM

Средства ГосСОПКА

в части предоставления
детализированных данных о
конкретном инциденте

Проект требований ФСБ России к средствам ГосСОПКА: визуализация

POSITIVE TECHNOLOGIES

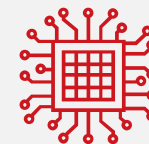
ПРОДУКТЫ POSITIVE TECHNOLOGIES



MaxPatrol SIEM



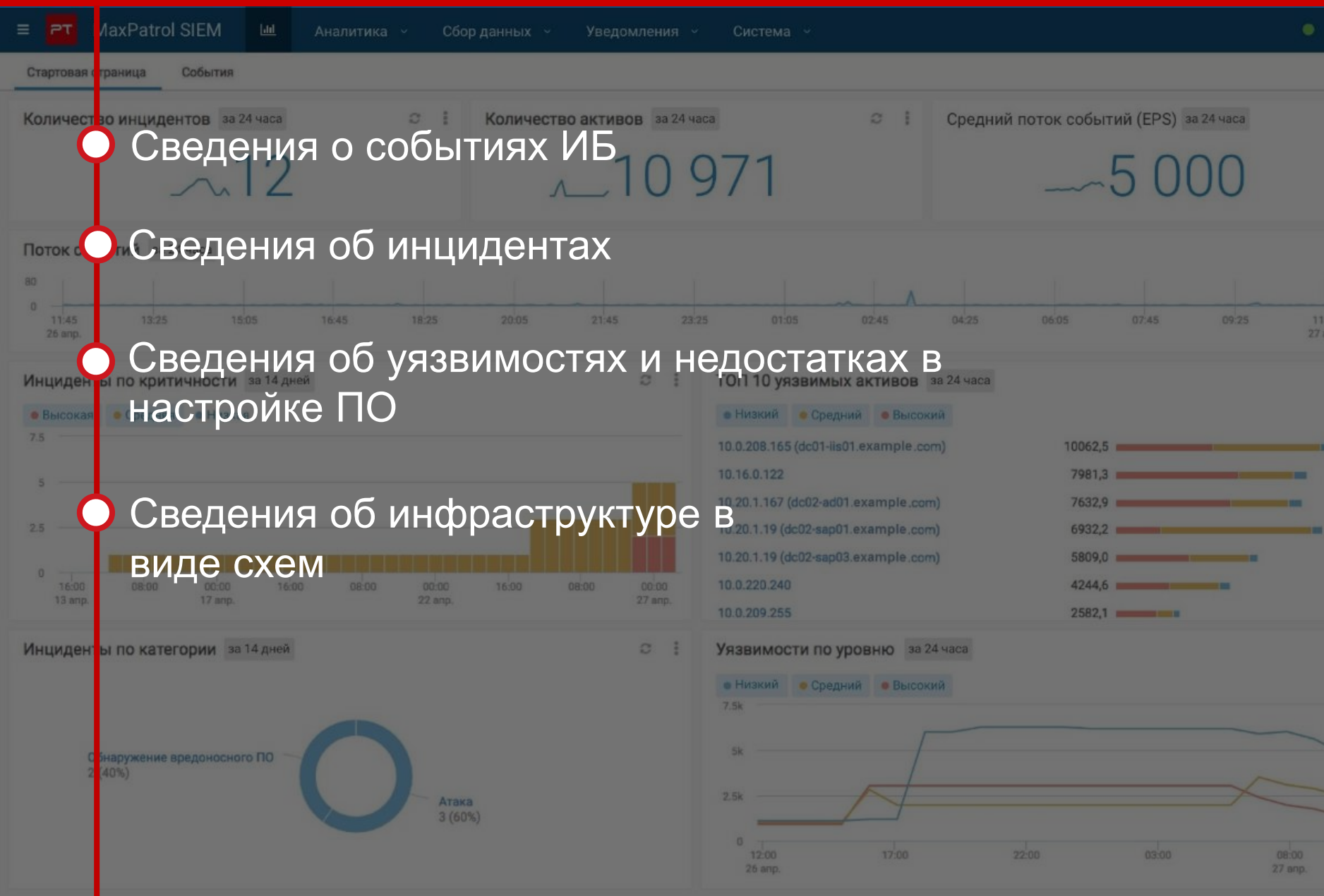
MaxPatrol 8



PT Network Attack
Discovery



ПТ Ведомственный
центр



- Построение сводных отчетов и их экспорт
- Выбор параметров, по которым строятся таблицы, графики, диаграммы
- Автоматическое формирование отчетов по расписанию и отправка в адреса
- Хранение загружаемой информации в течение заданного периода времени
- Экспорт информации

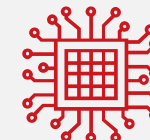
ПРОДУКТЫ POSITIVE TECHNOLOGIES



MaxPatrol SIEM



MaxPatrol 8



PT Network Attack Discovery



PT MultiScanner



ПТ Ведомственный центр

- Информация направляется в НКЦКИ не позднее 24 часов с момента обнаружения инцидента
- Один из способов организации обмена – подключение к технической инфраструктуре НКЦКИ
- Обмен между субъектами КИИ только через ГосСОПКА
- Получение от НКЦКИ ответов на запросы не более 5 дней

ПРОДУКТЫ POSITIVE TECHNOLOGIES



ПТ Ведомственный центр

Обмен в соответствии с форматами представления информации о компьютерных инцидентах в ГосСОПКА

- Первичный анализ КИ
- Проведение мероприятий в соответствии с Планом реагирования
- Запрос содействия ФСБ России в соответствии с Регламентом взаимодействия
- Восстановление функционирования и проверка работоспособности значимого объекта КИИ
- Информирование НКЦКИ не позднее 48 часов после завершения расследования

ПРОДУКТЫ POSITIVE TECHNOLOGIES



**ПТ Ведомственный
центр**

Средства ГосСОПКА

в части предоставления
детализированных данных о
конкретном инциденте

И напоследок...



Соответствие
законодательству



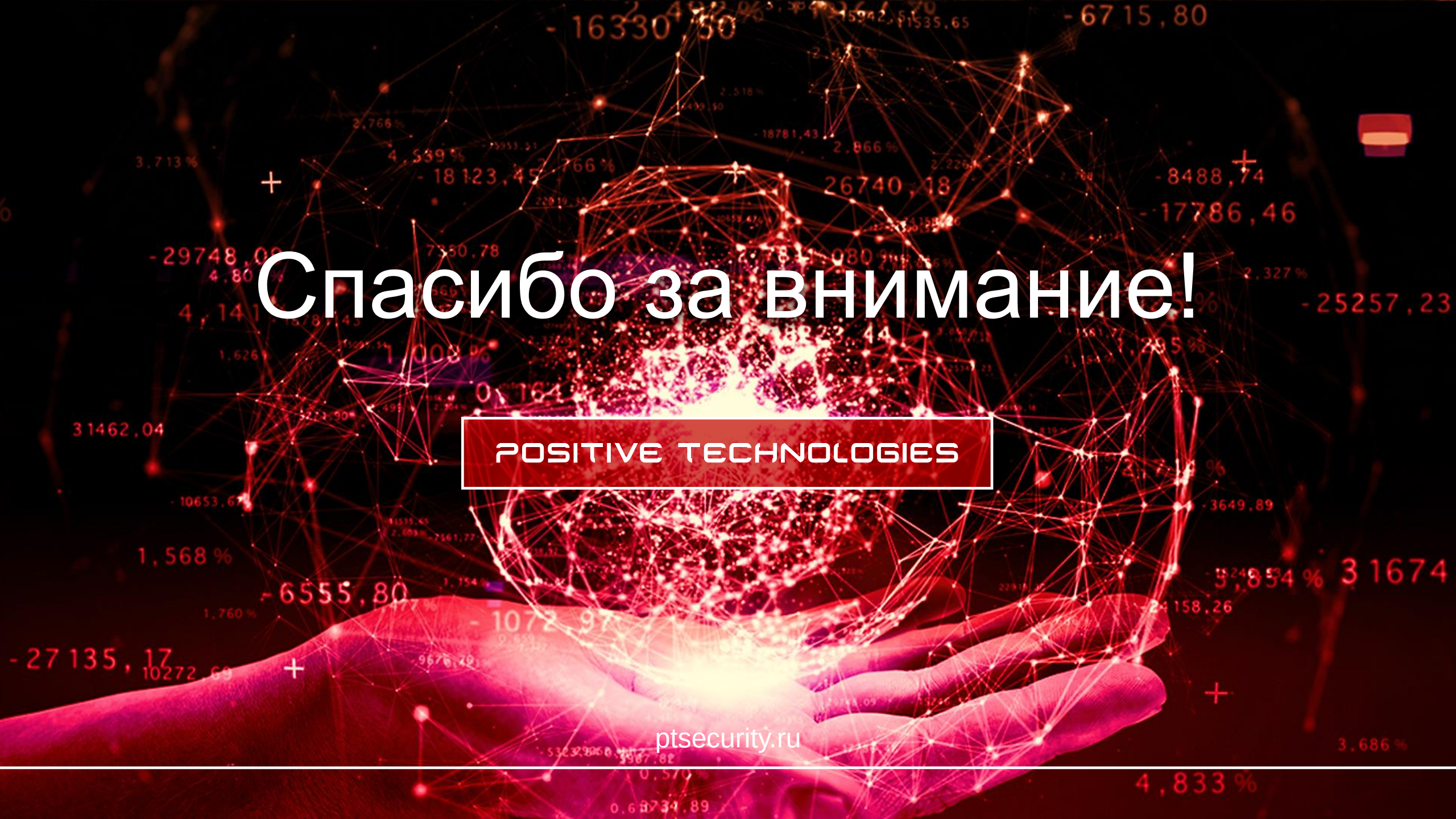
Взаимодействие
с НКЦКИ



Быстрая
инсталляция



Единая система
авторизации



Спасибо за внимание!

POSITIVE TECHNOLOGIES

ptsecurity.ru