POSITIVE TECHNOLOGIES

PT Platform RS

Создай свой мини-SOC

Реализация требований законодательства
для небольших инфраструктур

ptsecurity.com

О компании Positive Technologies

17 лет
опыта исследований и разработок

900 сотрудников:
инженеров по ИБ, разработчиков, аналитиков и других специалистов

250 экспертов
в нашем исследовательском центре безопасности

200+
обнаруженных уязвимостей нулевого дня в год

200+
аудитов безопасности корпоративных систем делаем ежегодно

50%
всех уязвимостей в промышленности и телекомах обнаружили наши эксперты

Защищаем крупные информационные системы от киберугроз:

- создаем продукты и решения
- проводим аудиты безопасности
- расследуем инциденты
- исследуем угрозы

Нам доверяют

Наши проекты

2018 МАРТА
ВЫБОРЫ ПРЕЗИДЕНТА РОССИИ

Задача
Усилить защищенность веб-портала ЦИК РФ во время проведения выборов.

Что сделано
Проверили защищенность веб-портала, внедрили PT Application Firewall для выявления и блокировки атак, провели мониторинг безопасности в день выборов.

Результат
Выявлены критичные уязвимости, обеспечена безопасность веб-портала и блокировка атак в режиме реального времени.

FIFA WORLD CUP
RUSSIA
2018

Задача
Обеспечить защиту сервисов, необходимых для перемещения болельщиков, регистрации компаний-перевозчиков и набора волонтеров.

Что сделано
Создали контур безопасности и проводили непрерывный мониторинг защищенности всей инфраструктуры.

Результат
Обеспечено непрерывное функционирование всех информационных систем

ptsecurity.com

phd
Positive
Hack
Days

Ежегодный международный форум по практической безопасности, который собирает более 6000 участников.

В рамках форума мы организуем 30-часовую кибербитву за контроль над эмуляцией городской инфраструктуры между командами атакующих и защитников. Формат соревнования максимально приближен к реальности.

Во время кибербитвы SOC на базе наших продуктов мониторит инфраструктуру и выявляет атаки.

phdays.com

Аналитика и расследования

Выпускаем более

20 исследований в год

Ежеквартальные отчеты об актуальных киберугрозах и трендах, прогнозы, расследования активности хакерских группировок, отраслевые исследования

ptsecurity.com/ru-ru/research/analytics

Вопрос не в том, взломают ли вопрос в том — когда

Преступники все чаще прибегают к сложным и многоэтапным техникам, включающим в себя взлом инфраструктуры компаний-партнеров, заражение ресурсов производителей ПО или комбинацию нескольких методов в рамках одной атаки[1]

С разового взлома и кражи денежных средств **фокус сместился на долгосрочное пребывание в сети заказчика** с целью похищения информации[1]

55% атак
в 2018 году составили целенаправленные атаки[1]

57% региональных компаний в 2018 году столкнулись с фишингом в адрес сотрудников[2]

206 дней
составляет среднее время обнаружения компрометации[3]

1. Актуальные киберугрозы — 2018. Тренды и прогнозы, Positive Technologies
2. Взломать любой ценой: сколько может стоить APT, Positive Technologies
3. 2019 Cost of a Data Breach Report, Ponemon institute

Зачем вам SOC?

SOC — центр мониторинга кибербезопасности

Задачи SOC:

- Предотвращает инциденты
- Выявляет целенаправленные атаки на инфраструктуру
- Снижает время обнаружения и реагирования на инцидент
- Помогает использовать средства ИБ с максимальной результативностью

Построение SOC — непростая задача

Нужны
люди, технологии,
процессы и деньги

Решение
от Positive Technologies

ptsecurity.com

PT Platform RS

PT Platform RS

Программно-аппаратный комплекс для реализации основных задач SOC и выполнения требований законодательства по защите информации

Для небольших инфраструктур

Возможно подключение
до 250 или до 500 сетевых узлов

Четыре продукта в одном

На сервере развернуты MaxPatrol SIEM, PT NAD, PT MultiScanner и MaxPatrol 8

Подходит для постепенного масштабирования

Возможно поэтапно перейти с enterprise-версии продуктов для мониторинга всей необходимой инфраструктуры

Состав PT Platform RS

	Компоненты	Решаемые задачи
	**MaxPatrol SIEM**	Дает полную видимость IT-инфраструктуры и выявляет инциденты информационной безопасности
	**MaxPatrol 8**	Дает объективную оценку состояния защищенности всей информационной системы
	**PT Network Attack Discovery**	Выявляет признаки атак в сетевом трафике на периметре и в инфраструктуре
	**PT MultiScanner**	Производит анализ файлов, передаваемых из PT NAD, а также в почтовом, сетевом и веб-трафике, на предмет угроз

Опциональное подключение:

- PT ISIM
- PT Application Firewall
- PT Application Inspector
- ПТ Ведомственный центр
- Доп. хранилище до 36 ТБ

Как построить SOC

с помощью PT Platform RS

ptsecurity.com

Двигаемся постепенно

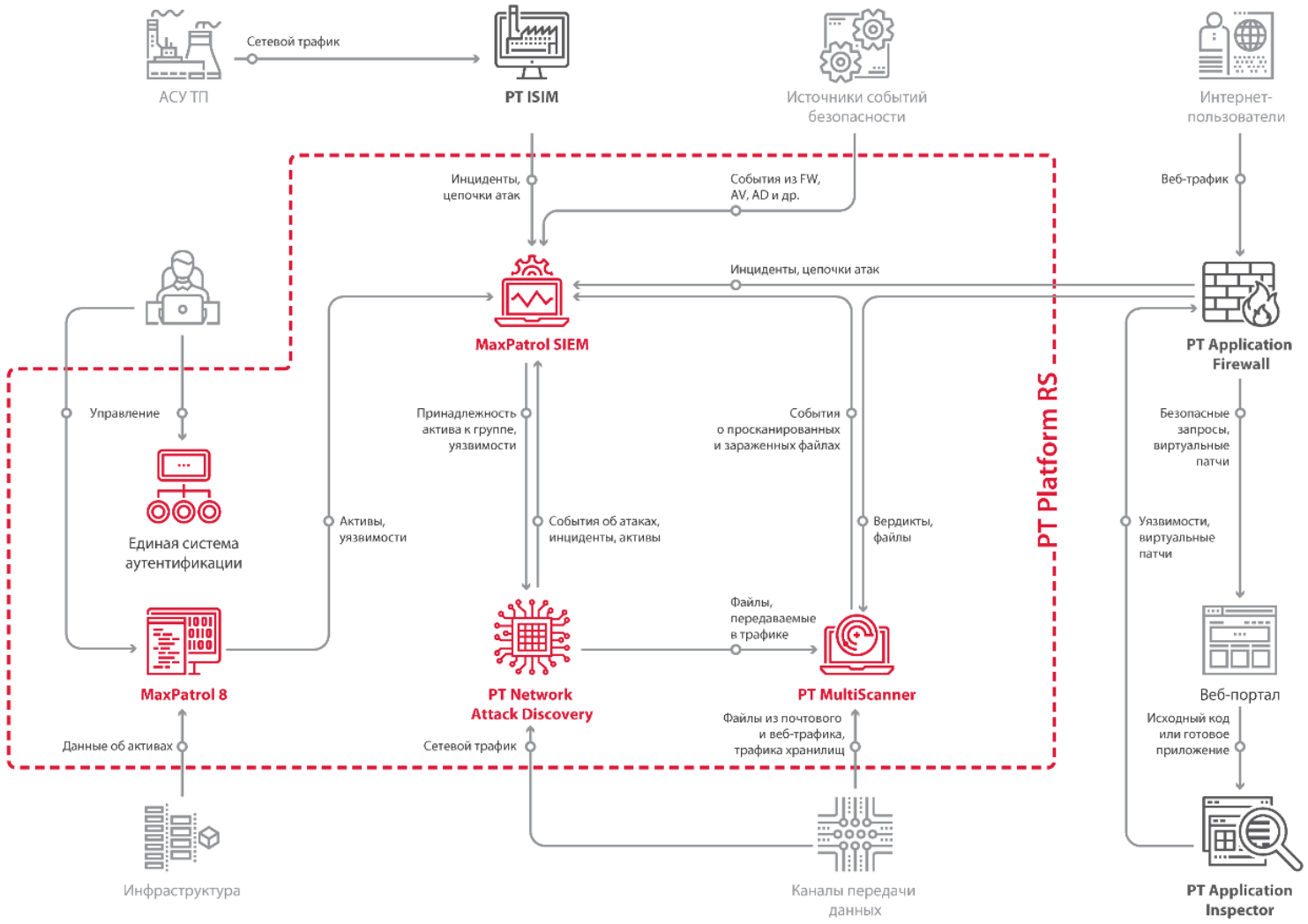
01 Мониторинг небольшой инфраструктуры

02 Накопление опыта

03 Организация процессов реагирования

04 Расширение области мониторинга

Как работает PT Platform RS



- **MaxPatrol SIEM** формирует модель защищаемой IT-инфраструктуры. Модель обогащается данными из MaxPatrol 8 и PT NAD о конфигурации, уязвимостях, ПО и аппаратном обеспечении IT-активов.
- **MaxPatrol SIEM** собирает события ИБ из различных источников, в т.ч. из PT NAD и PT MultiScanner, и по правилам выявляет инциденты.
- Для выявления вредоносного контента **PT NAD** передает файлы из трафика в PT MultiScanner. В случае обнаружения зараженного файла, PT MultiScanner сообщает об инциденте в MaxPatrol SIEM.

Кейс #1

01

Злоумышленник эксплуатирует уязвимость

02

PT NAD выявляет подозрительную активность после запуска эксплойта и передает файлы на проверку в PT MultiScanner

03

PT MultiScanner выявляет ВПО из трафика и передает событие в MaxPatrol SIEM

04

MaxPatrol SIEM выявляет инциденты и уведомляет оператора ИБ

Кейс #2

01

Злоумышленник
рассылает письма
с вирусом

02

Вирус попал
в инфраструктуру

03

PT MultiScanner
выявляет ВПО
и передает событие
в MaxPatrol SIEM

04

MaxPatrol SIEM
выявляет инциденты
и уведомляет
оператора ИБ

Расширение области мониторинга

Пример проекта:
Калининградская область строит региональный центр кибербезопасности на базе продукта PT Platform 187

Команда SOC

Руководитель SOC

1-я линия

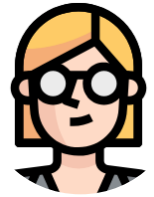
Первичная оценка инцидентов, отработка ложных срабатываний, обработка по плейбукам

2-я линия

Глубокое расследование инцидентов

3-я линия

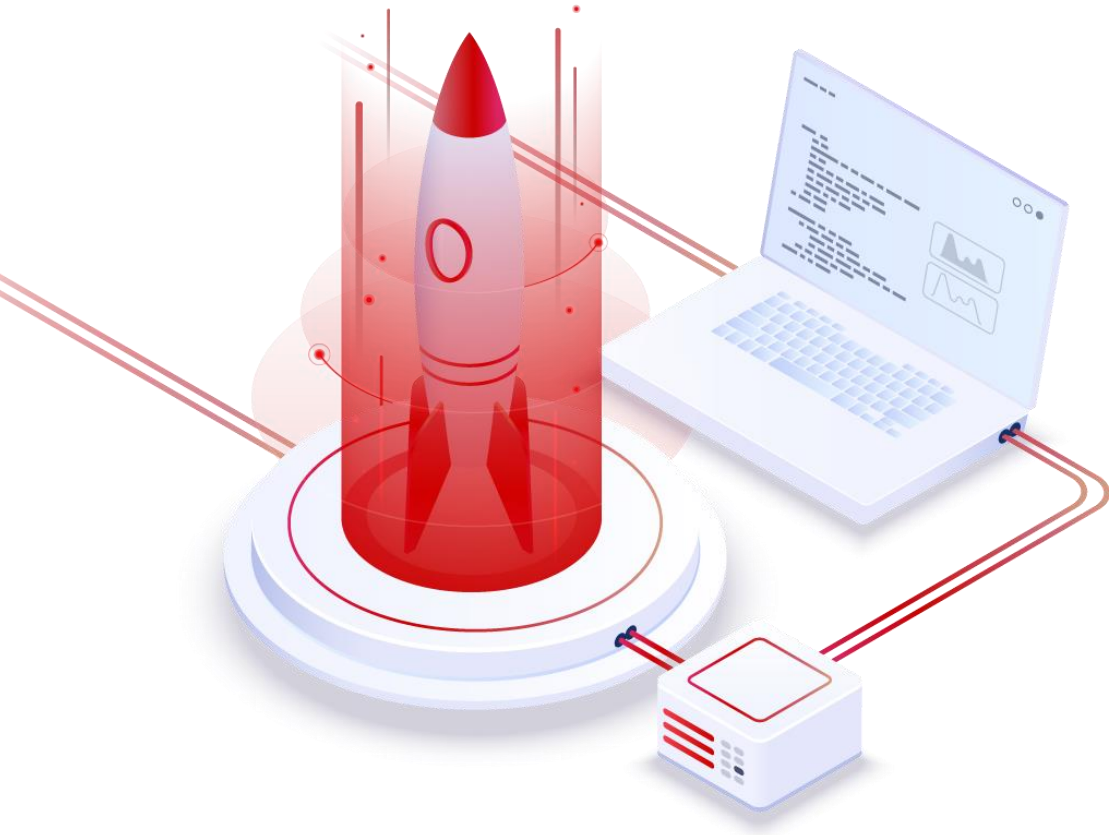
Глубокий анализ артефактов инцидентов



Аналитики

Написание плейбуков, внутренний TI

Преимущества подхода

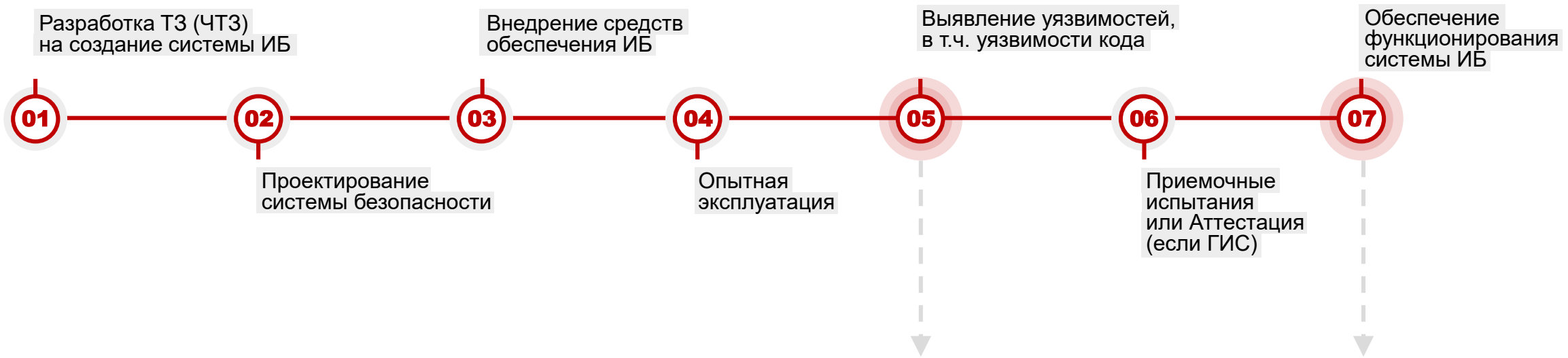


- Возможность распланировать бюджет
- Постепенное развитие внутренней экспертизы
- Тренировка на малой инфраструктуре для выстраивания процессов ИБ
- Отсутствие «полочного» ПО (shelfware)

Покрытие требований ФСТЭК России

ptsecurity.com

Создание системы ИБ



Продукты Positive Technologies

- MaxPatrol 8
- PT Application Inspector
- PT Application Firewall

Приказы ФСТЭК России: безопасность ГИС, ПДн, КИИ

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

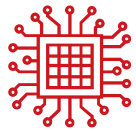
MaxPatrol 8

АУД.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

Приказы ФСТЭК России: безопасность ГИС, ПДн, КИИ

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

Реестр российского ПО и сертификаты ФСТЭК

В реестре российского ПО:

PT	MaxPatrol 8
PT	MaxPatrol SIEM
PT	Network Attack Discovery
PT	MultiScanner

Сертификаты ФСТЭК России:

PT	MaxPatrol 8	сертификат № 2922
PT	MaxPatrol SIEM	сертификат № 3734
PT	Network Attack Discovery	сертификат № 4042
PT	MultiScanner	coming soon

Результаты применения

Результаты применения

Реализация ключевых задач SOC:

- Отсутствие «белых пятен» в инфраструктуре
- Мониторинг актуальных уязвимостей и их оперативное устранение
- Оперативное выявление критичных инцидентов
- Обнаружение атак как на периметре, так и внутри сети
- Оперативная локализация вирусных угроз в трафике, в почте и в файловых хранилищах
- Ретроспективное выявление следов компрометации

Результаты применения

Реализация ключевых задач SOC:

- Отсутствие «белых пятен» в инфраструктуре
- Мониторинг актуальных уязвимостей и их оперативное устранение
- Оперативное выявление критичных инцидентов
- Обнаружение атак как на периметре, так и внутри сети
- Оперативная локализация вирусных угроз в трафике, в почте и в файловых хранилищах
- Ретроспективное выявление следов компрометации

Выполнение требований по безопасности:

- значимых объектов КИИ (приказы ФСТЭК № 235 и 239)
- информации в ГИС (приказ ФСТЭК № 17),
- персональных данных (приказ ФСТЭК № 21)

Конфигурации
PT Platform RS

ptsecurity.com

Конфигурации
PT Platform RS

PT Platform RS 250

Количество подключаемых узлов для мониторинга в MaxPatrol SIEM и MaxPatrol 8	до 250
Пропускная способность PT NAD	до 100 Мбит/с
Пропускная способность PT MultiScanner	до 3000 файлов в час
Состав ПАК	Сервер + ПО

Конфигурации
PT Platform RS

PT Platform RS 500

Количество подключаемых узлов для мониторинга в MaxPatrol SIEM и MaxPatrol 8	до **500**
Пропускная способность PT NAD	до **1000** Мбит/с
Пропускная способность PT MultiScanner	до **7000** файлов в час
Состав ПАК	**Сервер + ПО**

Как получить
PT Platform RS

ptsecurity.com

Как получить пилот

1 неделя

Подписание NDA, заполнение анкеты об инфраструктуре, подготовка источников событий ИБ

4 недели

Разворачивание одного или двух компонентов PT Platform RS на пилотном сегменте, подключение источников и настройка компонентов

2 недели

Пилотирование

1 неделя

Отчет по итогам пилота

ДО 2 МЕСЯЦЕВ

Продолжим знакомство:

По вопросам стоимости, заказа пилота:

Григорий Тимофеев

Руководитель направления продаж

+7 937 625 26 46