POSITIVE TECHNOLOGIES

Моновендорный подход в решении ключевых задач ИБ

PT Platform QALQAN и Beren для небольших инфраструктур

Алексей Титов
Центр Компетенций, Positive Technologies

(c) от экспертов международного уровня в вопросах кибербезопасности

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

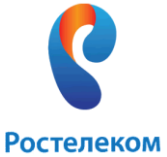
200+
аудитов безопасности корпоративных систем делаем ежегодно

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

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.

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

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

«А ВЗЛОМАЮТ ЛИ НАС?»

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]

60% атак
в 2019 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: итоги 2019 года. Positive Technologies
2. Взломать любой ценой: сколько может стоить APT. Positive Technologies
3. 2019 Cost of a Data Breach Report, Ponemon institute

Проблемы в ИБ организаций

Система безопасности выстраивается в основном только в головной организации… и то, по бумажному принципу

Отсутствие компетентных специалистов ИБ и недостаточный объем бюджета на ИБ

Нет централизованного мониторинга и контроля состояния защищенности в организации

В некоторых учреждениях отсутствуют необходимые СЗИ

Нижние уровни инфраструктуры не защищены, для хакеров – это свободный вход в инфраструктуру всей организации

Обособленные подразделения могут не соответствовать требованиям законодательства в сфере ИБ

Некорректная настройка СЗИ или выставление настроек по умолчанию

Традиционные СЗИ НЕ ПАНАЦЕЯ

PROXY
WAF
VPN
SSL
IDS
TLS
Domain Policy
Endpoint Protection
NGFW
FireFox
PAM
VLAN
Segmentation LAN
IDM
ANTI SPAM
AntiVirus

Как решить проблемы и причем тут мониторинг?

ПОСТОЯННО И ТЩАТЕЛЬНО НАБЛЮДАТЬ ЗА АКТИВАМИ ИНФРАСТРУКТУРЫ

ЗНАЧИТЕЛЬНО СНИЖАЕТСЯ ВЕРОЯТНОСТЬ РЕАЛИЗАЦИИ КИБЕРУГРОЗ

ФАКТ ВЗЛОМА ОПЕРАТИВНО ВЫЯВЛЯЕТСЯ

ЕСТЬ ВРЕМЯ ДЛЯ ПРИНЯТИЯ КОМПЕНСИРУЮЩИХ МЕР ПО МИНИМИЗАЦИИ УЩЕРБА

Ключевые задачи для собственников (владельцев) КВОИКИ

Выстраивать процессную модель ИБ

Организация мониторинга – непростая задача

Нужны
люди, технологии,
процессы и деньги

Решение
от Positive Technologies

ptsecurity.com

PT Platform QALQAN

PT Platform QALQAN

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

Для небольших инфраструктур

Возможно подключение до 250/500 сетевых узлов

Четыре полноценных продукта в одном

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

Подходит для постепенного масштабирования

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

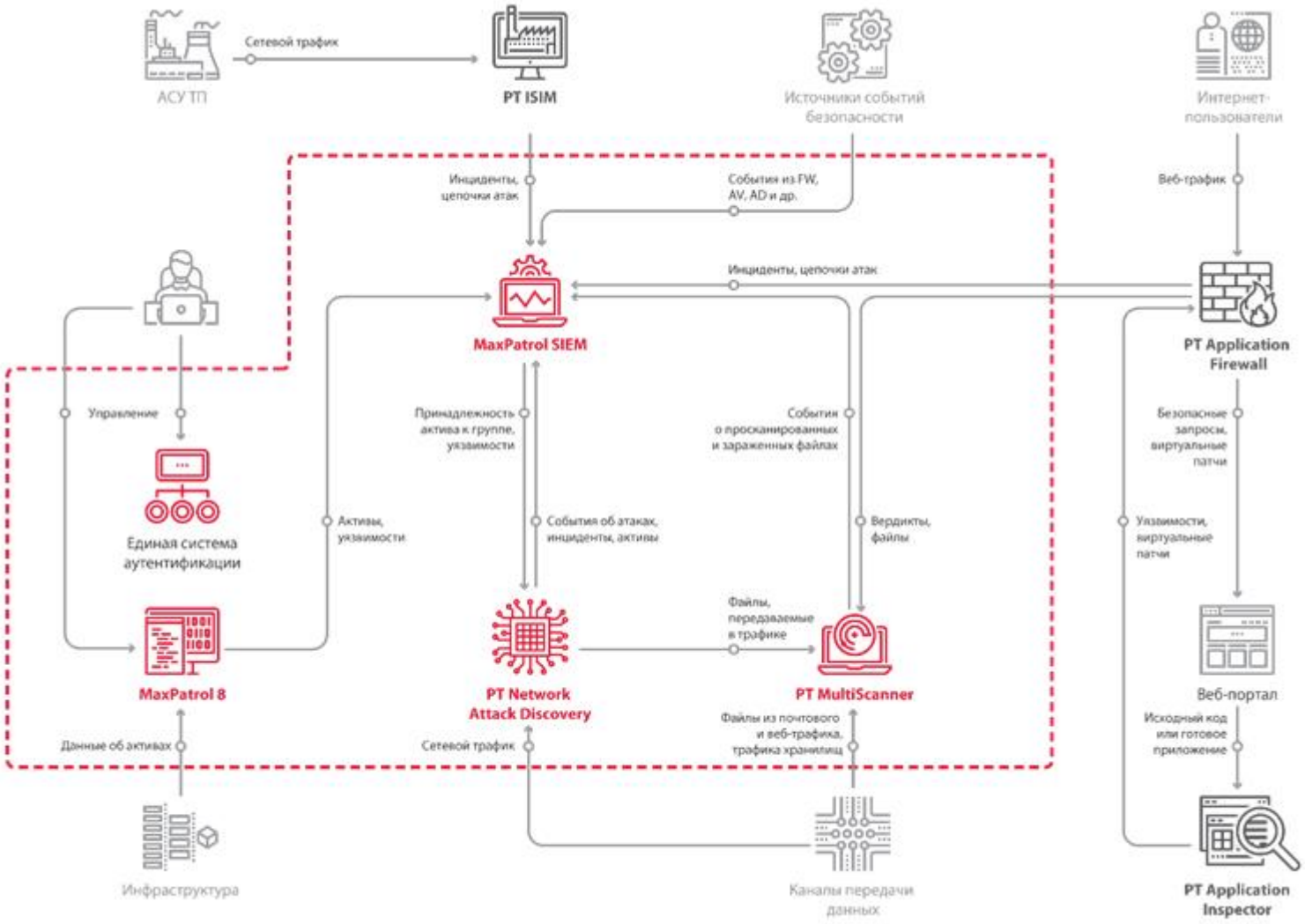
Состав PT Platform QALQAN

	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
- Доп. хранилище до 36 ТБ

Как работает PT Platform QALQAN



- **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.

PT Platform BEREN

PT Platform BEREN

Программно-аппаратный комплекс для мониторинга удаленной инфраструктуры

Для аутсорсинга небольших, удаленных

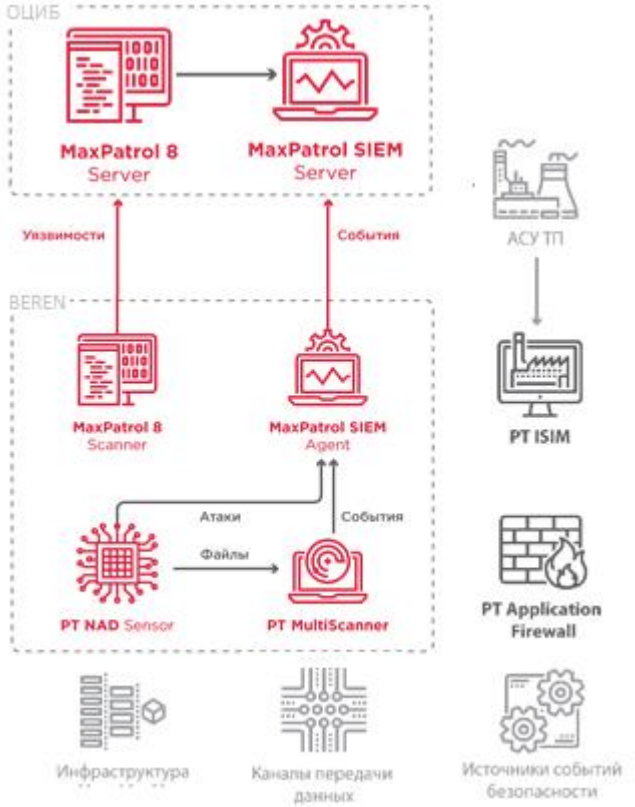
Возможно подключение
до 1000 сетевых узлов в качестве источников

Компоненты сбора данных

На сервере развернуты MaxPatrol 8 Scanner, MaxPatrol SIEM Agent, PT NAD Sensor и PT MultiScanner

Состав и принцип работы PT Platform BEREN

Компоненты	Решаемые задачи
MaxPatrol SIEM Agent	Сбор событий безопасности для передачи на сервер MaxPatrol SIEM
MaxPatrol 8 Scanner	Аудит защищенности и выявление уязвимостей
PT NAD Sensor	Анализ сетевого трафика и выявление атак
PT MultiScanner	Выявление вредоносных программ



Состав Решения

MaxPatrol 8

- Все в одном: средство автоматизированного анализа защищенности и контроля соответствия
- Поиск уязвимостей и ошибок конфигурации компонентов ИС
- Контроль соответствий фактических настроек ИС установленным требованиям
- Более 120 встроенных, сгруппированных стандартов и возможность создания собственных
- Ежедневно обновляемая база знаний

PT NAD

Глубокий анализ сетевого трафика

Определяет более 70 протоколов и разбирает до уровня L7 включительно 30 наиболее распространенных из них

Выявление сетевых атак

Использует 3000+ сигнатур, IOC, разработанных экспертами Positive Technologies, и репутационные списки

Возможность интеграции с другими средствами

В комплексе с PT MaxPatrol SIEM продукт помогает выстроить эффективную систему выявления атак и инцидентов

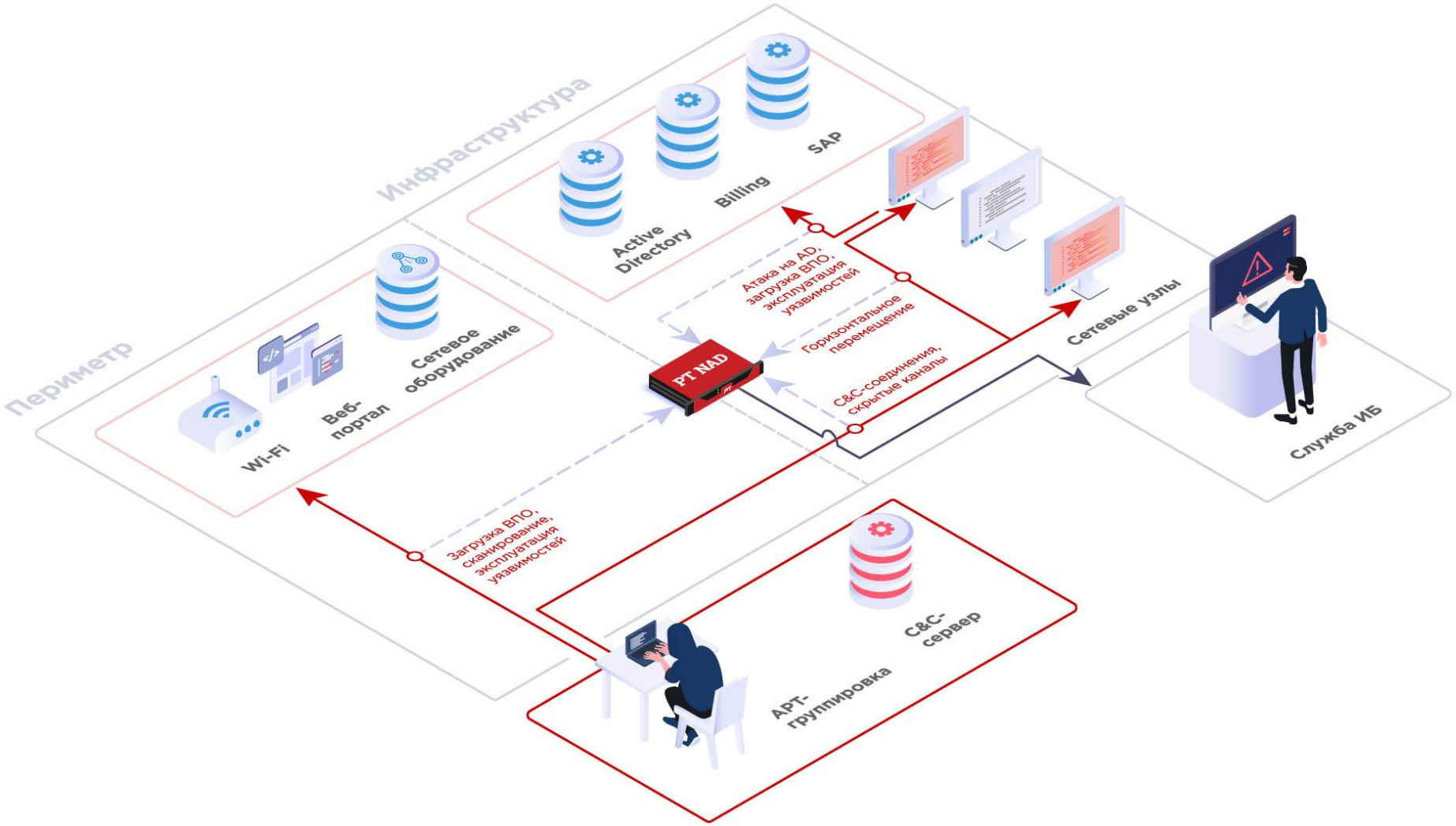
Фактура при расследованиях атак

Дает глубокое понимание контекста атаки за счет того, что хранит сырой трафик и 1200 параметров сессий без ограничений по времени

PT NAD

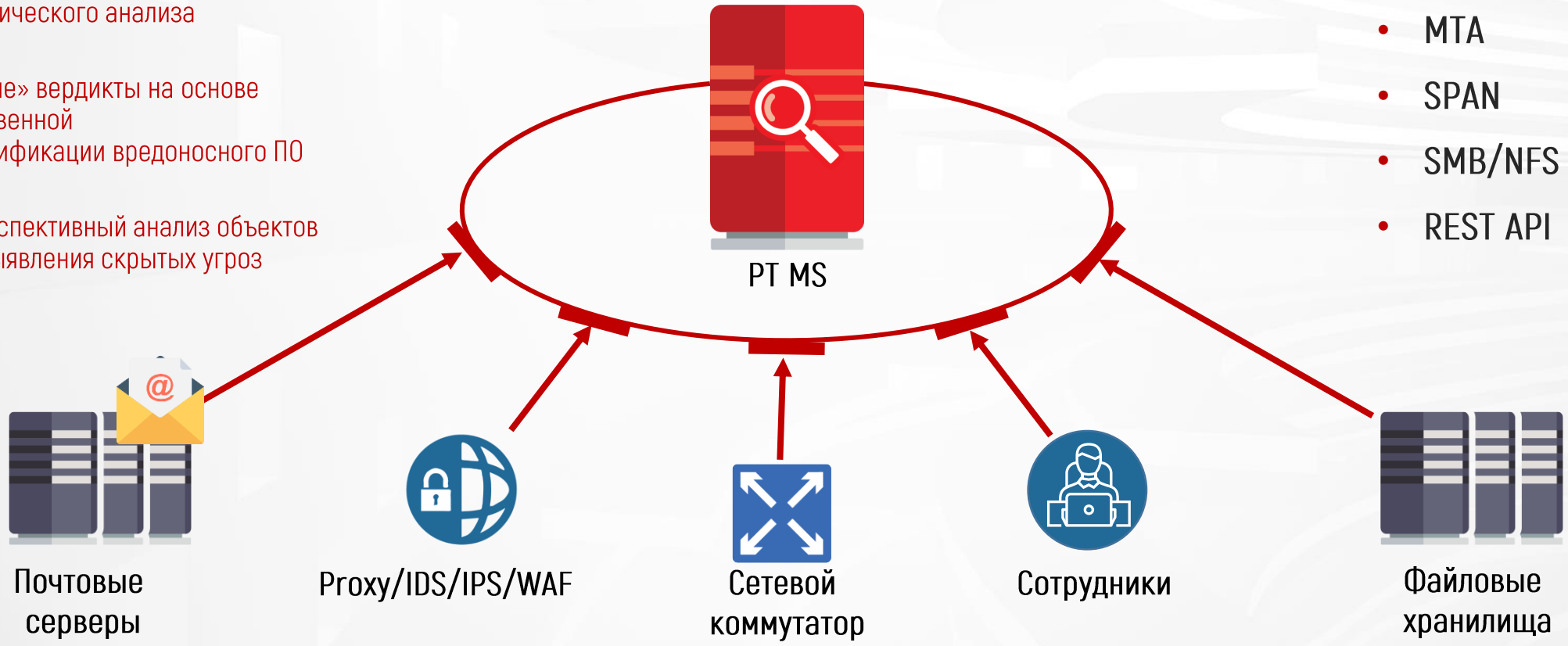
PT NAD захватывает и разбирает трафик на периметре и в инфраструктуре.

Это позволяет выявлять активность злоумышленника и на самых ранних этапах проникновения в сеть, и во время попыток закрепиться и развить атаку внутри сети



PT MultiScanner

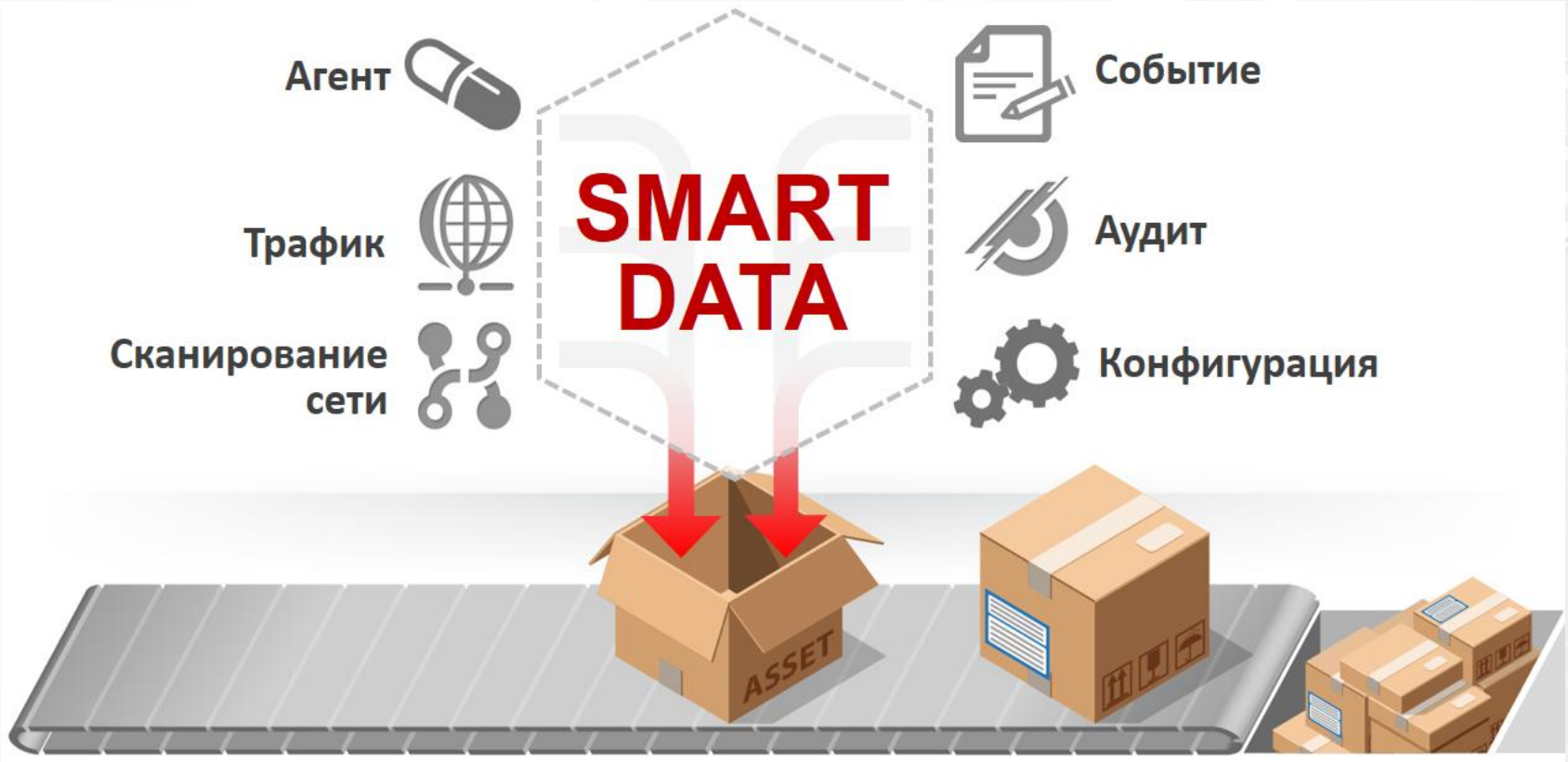
- Гарантированный рост вероятности детекта за счет нескольких AV-движков, репутационных списков и статического анализа
- «Умные» вердикты на основе собственной классификации вредоносного ПО
- Ретроспективный анализ объектов для выявления скрытых угроз



- ICAP
- SMTP (BCC)
- MTA
- SPAN
- SMB/NFS
- REST API

MaxPatrol SIEM

- Автоматически строит полную модель IT-инфраструктуры.
- Постоянно обогащается новыми данными об IT-активах.
- Автоматически идентифицирует IT-активы даже после изменения IP и MAC-адреса и других характеристик.



MaxPatrol SIEM

MaxPatrol SIEM автоматически адаптируется к изменениям IT-ландшафта.

Создает корреляциина основе данных IT-активов и динамических групп активов, а не логов.

Правила корреляции продолжают выявлять угрозы после появления нового оборудования или изменения конфигурации сетевых узлов.

Решение задач ИБ с помощью PT Platform QALQAN и Beren

ptsecurity.com

Кейс #1

01

Злоумышленник
эксплуатирует уязвимость

02

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

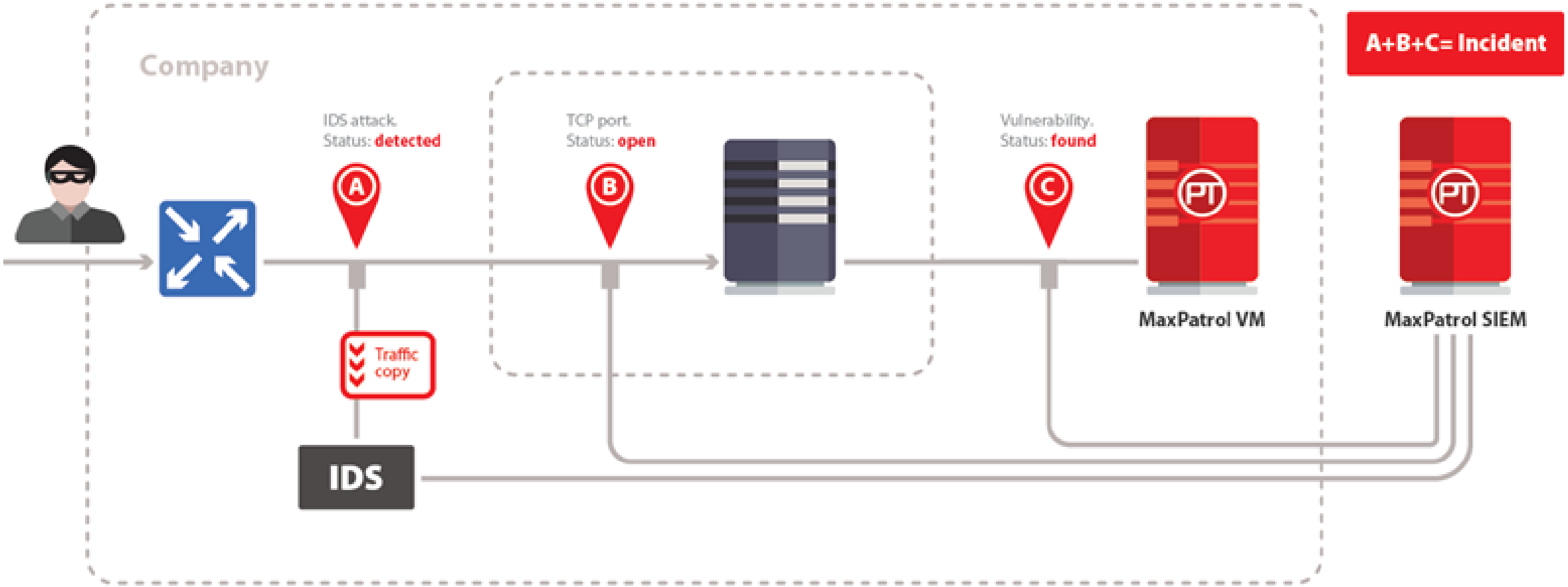
03

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

04

MaxPatrol SIEM выявляет инциденты
и уведомляет оператора ИБ

Кейс #1. Особенности активоцентрического подхода в корреляциях MaxPatrol SIEM



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

Кейс расследования атаки

01 Аналитик ОЦИБ с помощью **PT Platform BEREN** обнаружил, аномальную активность на сетевых узлах КВОИКИ: попытки подбора учетных данных к контроллеру домена и передачу подозрительного ПО между сетевыми узлами

02 Аналитик выяснил, что это подозрительное ПО не детектируется антивирусными базами антивирусов в PT Multiscanner на BEREN и загрузил его для исследования в **PT Sandbox**, развернутый в ОЦИБ.

03 Получил IP-адреса C&C-серверов злоумышленников.

04 Передал в **MaxPatrol SIEM Server** IP-адреса, чтобы проверить, были ли события с их участием на других КВОИКИ.

05 **MaxPatrol SIEM** выявил активность этого вредоносного ПО на двух других объектах. Аналитики локализовали угрозу.

06 Инциденты отправили в НКЦИБ, который передал сведения о них в другие ОЦИБ и ведомства.

PT Platform QALQAN

Поэтапное развитие мониторинга

01 → Мониторинг небольшой инфраструктуры

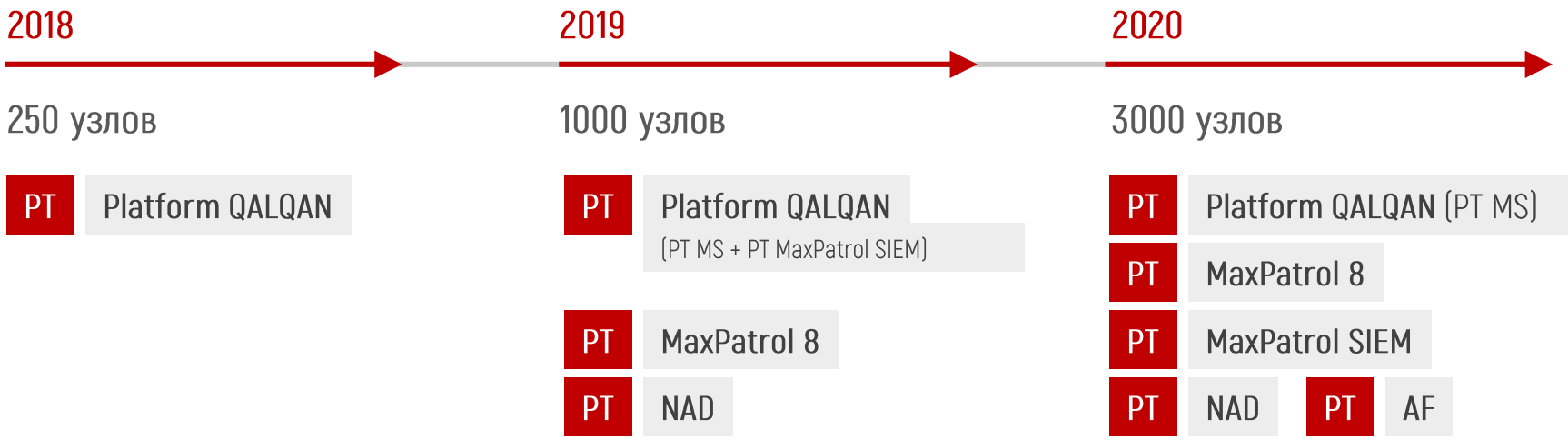
02 → Накопление опыта

03 → Организация процессов реагирования

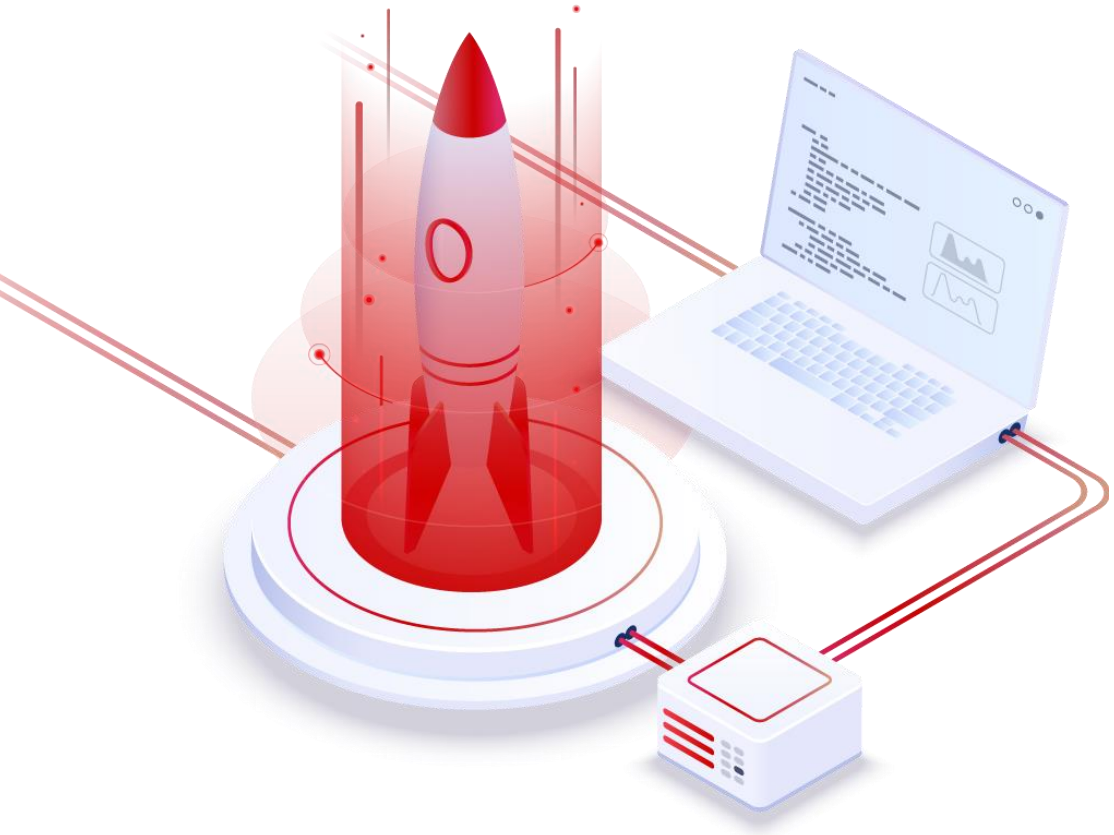
04 → Расширение области мониторинга

Расширение области мониторинга

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



Преимущества подхода



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

Сертификаты соответствия

Продукт	Требования	№ сертификата соответствия
MaxPatrol SIEM	СТ РК ГОСТ Р ИСО/МЭК 15408-3-2006. ОУД4.	КСС № 1452620
MaxPatrol 8	СТ РК ГОСТ Р ИСО/МЭК 15408-3-2006. ОУД4.	КСС № 1452619
PT Network Attack Discovery	СТ РК ISO/IEC 15408-3-2017. ОУД 4.	КСС № 1452638
PT MultiScanner	СТ РК ГОСТ Р ИСО/МЭК 15408-3-2006. ОУД4.	КСС № 1452623
PT ISIM	СТ РК ГОСТ Р ИСО/МЭК 15408-3-2006. ОУД4.	КСС № 1452622
PT Application Firewall	СТ РК ГОСТ Р ИСО/МЭК 15408-3-2006. ОУД4.	КСС № 1452618
PT Application Inspector	СТ РК ГОСТ Р ИСО/МЭК 15408-3-2006. ОУД4.	КСС № 1452621

Спасибо за внимание!

Время вопросов...