О компании Positive Technologies

Защищаем крупные информационные системы от киберугроз:

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

20 лет

опыта исследований и разработок

1200 сотрудников:

инженеров по ИБ, разработчиков, аналитиков и других специалистов

250 экспертов

в нашем исследовательском центре безопасности

200+

обнаруженных уязвимостей нулевого дня в год

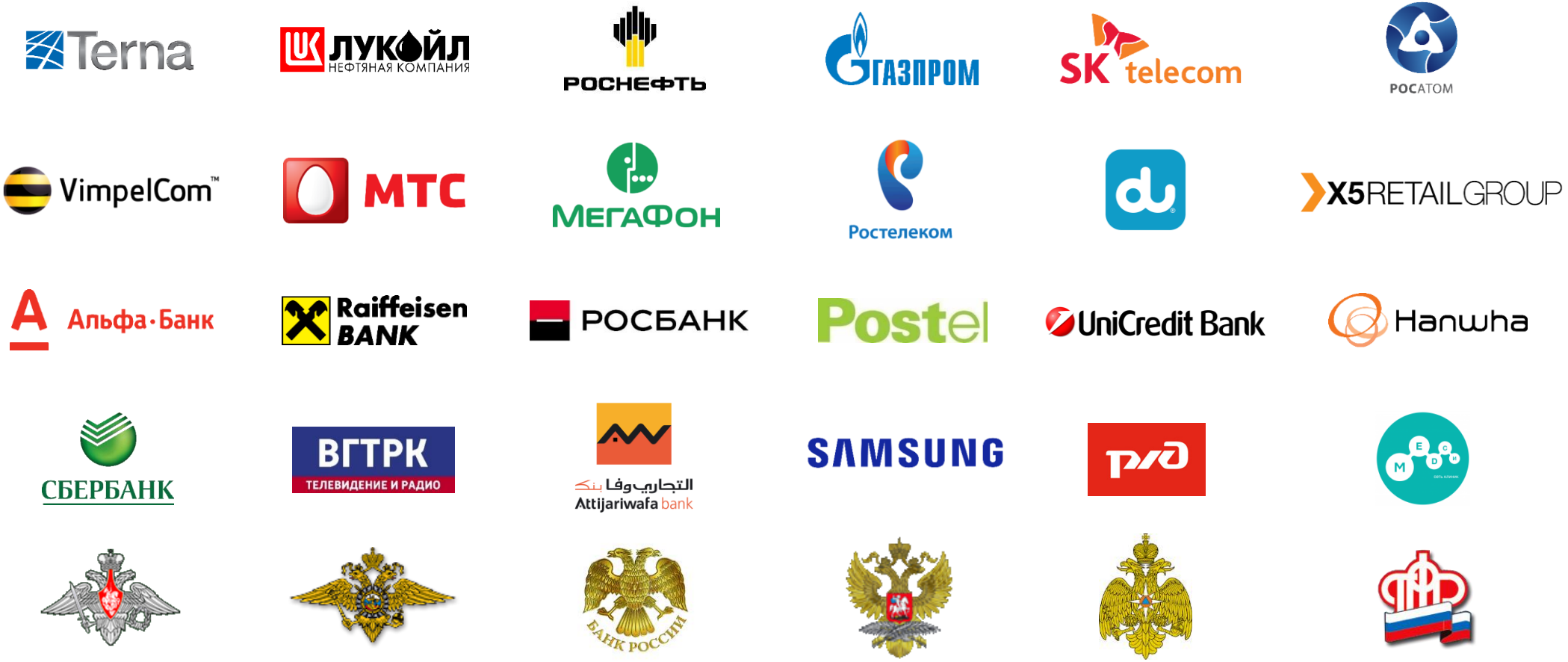
200+

аудитов безопасности корпоративных систем делаем ежегодно

50%

всех уязвимостей в промышленности и телекомах обнаружили наши эксперты

Реализованные проекты

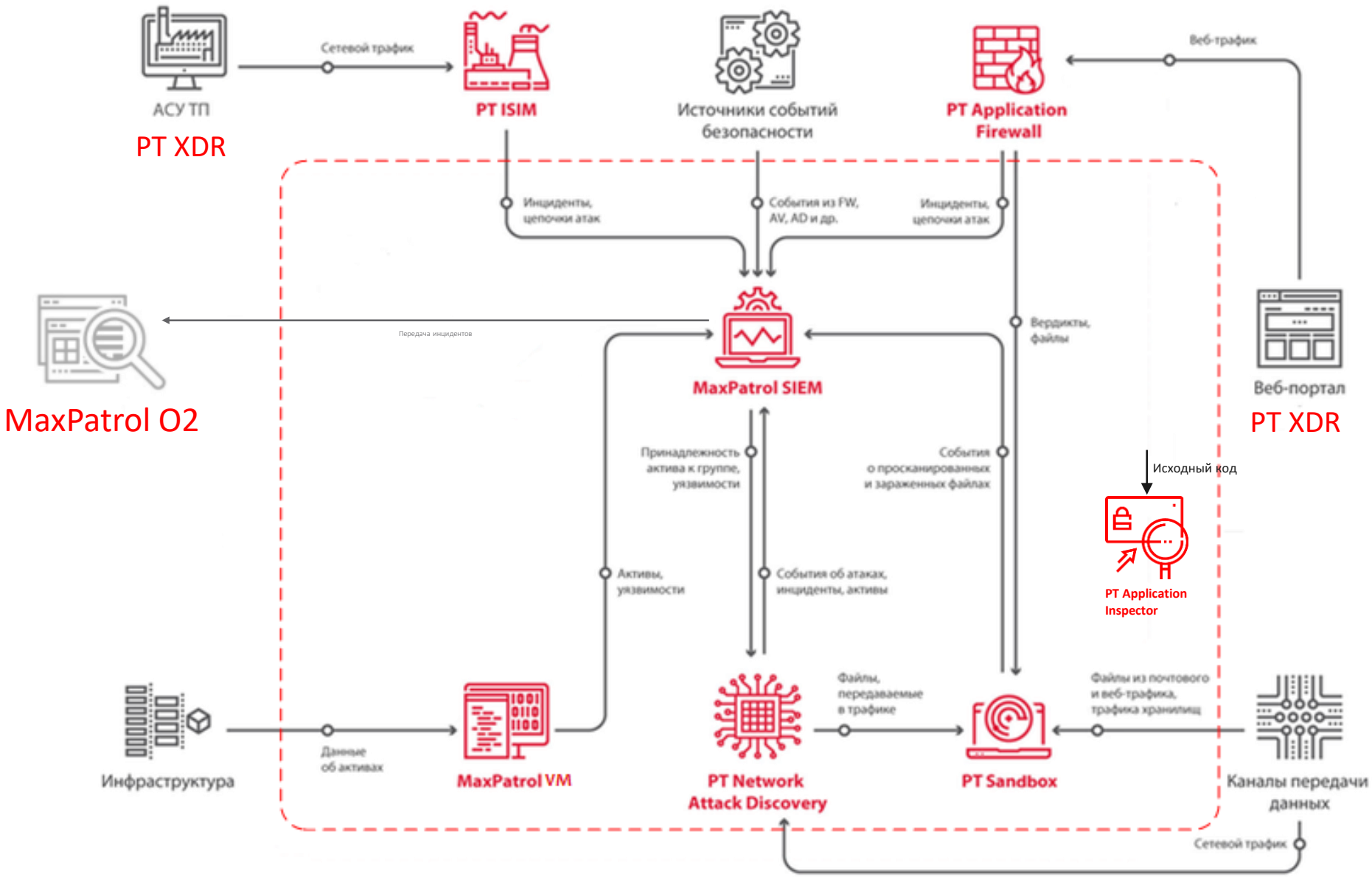


Продуктовое портфолио

Продукты

- MaxPatrol VM
- MaxPatrol SIEM
- PT XDR
- PT Sandbox
- PT MultiScanner
- PT Network Attack Discovery
- PT ISIM
- PT Application Firewall
- PT Application Inspector
- PT BlackBox
- ПТ Ведомст-венный центр
- PT Platform 187
- MaxPatrol 8
- XSpider

У нас комплексный подход

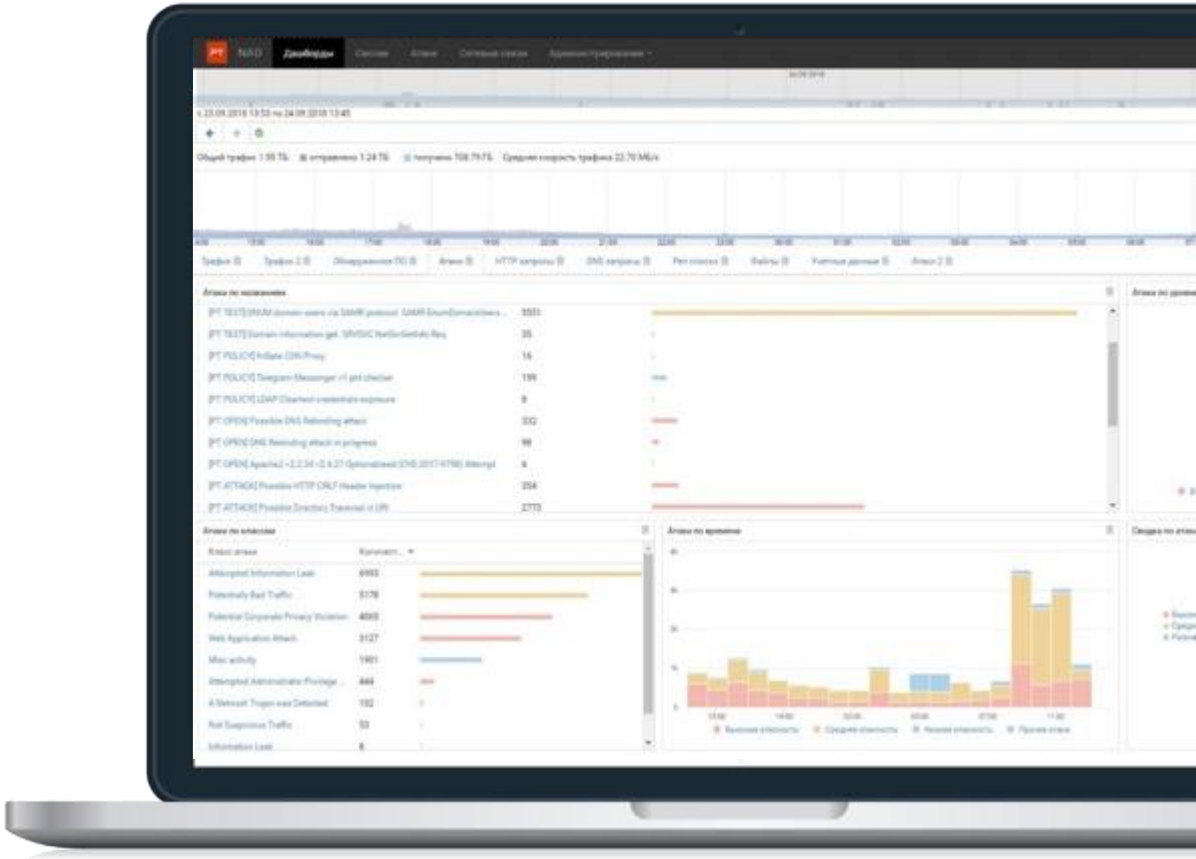


Почему NAD?

PT Network Attack Discovery

Система глубокого анализа сетевого трафика для выявления атак на периметре и внутри сети по поведению

- Ретроспективный анализ трафика для поиска сложных угроз
- Обнаруживает скрытые угрозы в сети по большому количеству признаков (IoA)
- Дает понимание, что происходит в сети, и позволяет проконтролировать соблюдение регламентов ИБ
- Повышает эффективность работы SOC, помогает восстановить цепочку атаки и разобраться в произошедшем инциденте
- Контроль политик ИБ
- Выявление атак внутри и на периметре
- Выявление скрытых угроз
- Расследование атак
- Выполнение требований законодательства



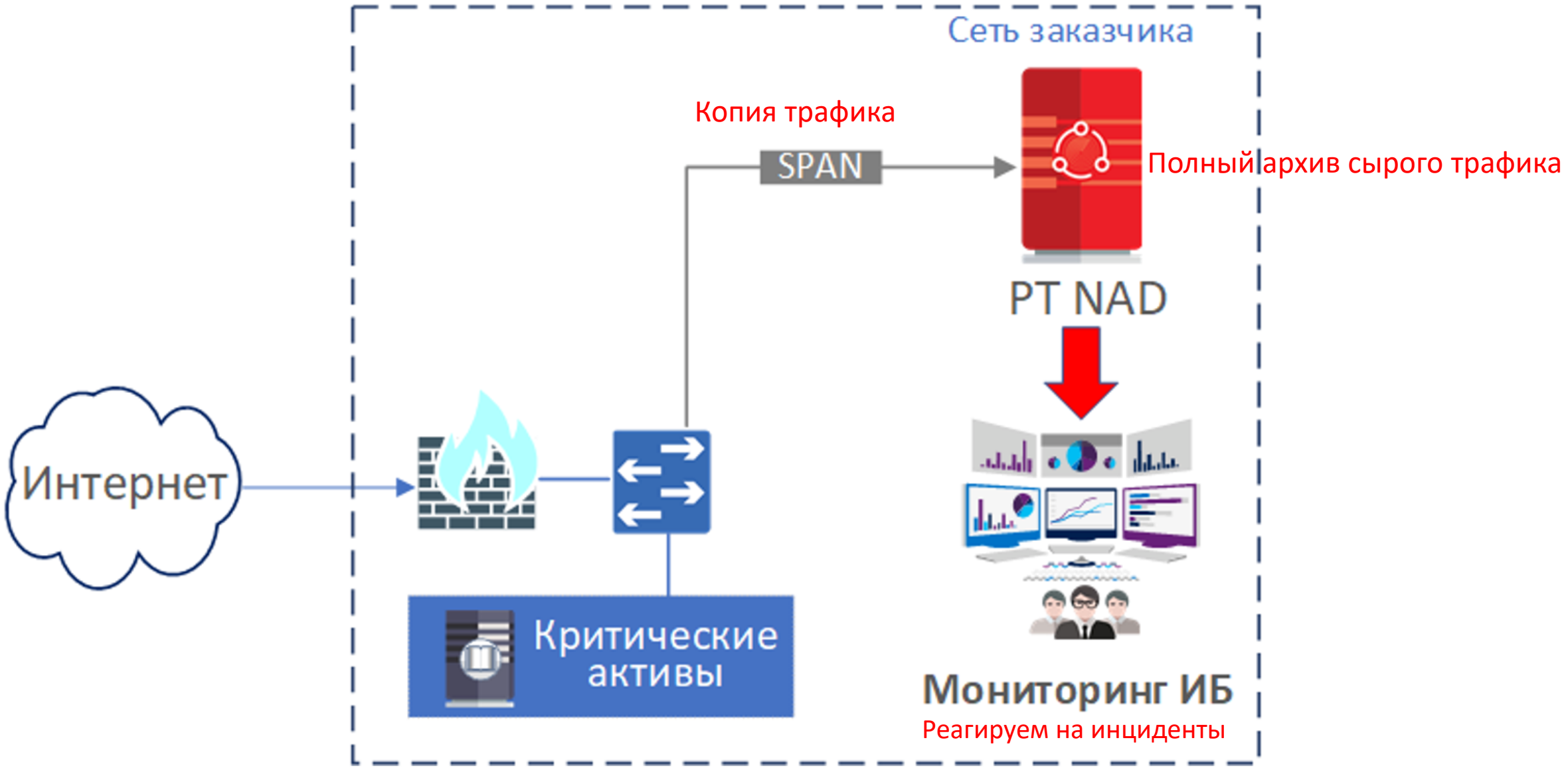
Ретроспективный
анализ трафика

Решение выявляет

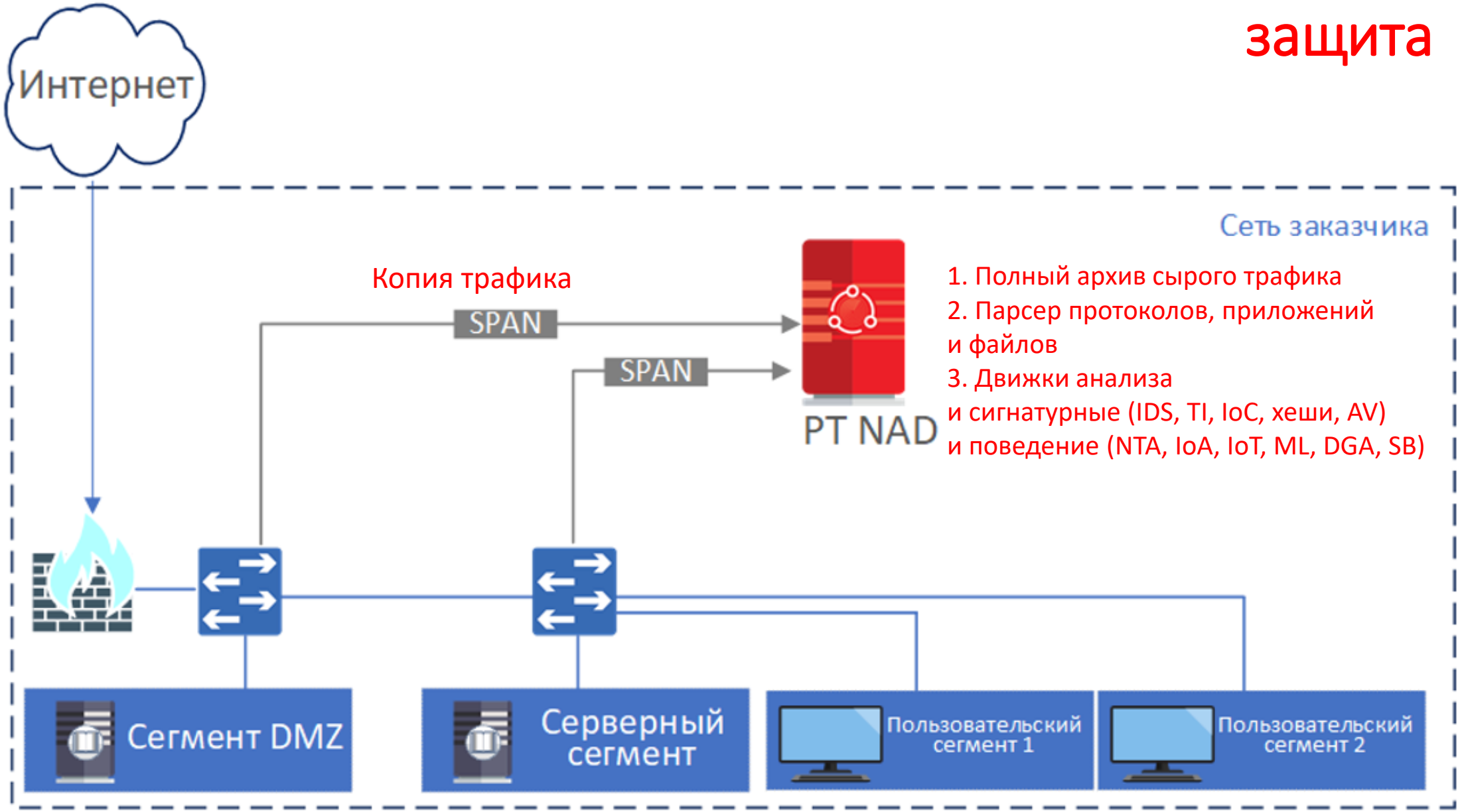
- Горизонтальное перемещение злоумышленника
- Угрозы в зашифрованном трафике
- Связь с автоматически сгенерированными доменами DGA
- Нарушения регламентов ИБ
- Хакерский инструментарий
- Эксплуатацию уязвимостей в сети
- Активность вредоносного ПО
- Признаки атак, не обнаруженных ранее
- Сокрытие активности от средств защиты

Архитектура решения

Минимум рекомендуем защищать критичные активы



Идеально – защитить все сегменты, где требуется защита



Сетевые брокеры и TAP – упрощают пилот и эксплуатацию, но требуют дополнительных расходов в проекте

SPAN – бесплатно для заказчика, но его не хотят включать сетевые администраторы на своих устройствах

Запись сырого трафика

1. Запись трафика на скорости 10 Гбит/с (1,25 Гбайт/с).

Кто еще может это делать так быстро? Гарда и Касперский не могут

Хранение 1-3 дня полезно для разбора инцидентов

Хранение 7-30 дней имеет смысл только для траты бюджета

Разбор приложений

2. Анализ приложений.
Распознавание vs Анализ.
1200 параметров приложений используется. Кто еще так делает? Никто. Конкуренты давят на то, что они распознают больше приложений. НО это не та задача, которая стоит перед NDR/NTA.

Экспертиза

Анализ атак - хакеры ловят хакеров. Мы знаем как ломать, мы знаем как осуществляются APT атаки и мы это используем чтобы ловить других хакеров

КИБЕРБЕЗОПАСНОСТЬ - ЭТО ИНВЕСТИЦИИ В R&D

https://www.ptsecurity.com/ru-ru/research/

- Мы самый большой исследовательский центр в Восточной Европе. Более 150 экспертов мирового уровня по защите SCADA- и ERP-систем, веб-приложений, банковских и телекоммуникационных технологий ежегодно проводят исследования, тестирования на проникновение, анализ угроз и уязвимостей.
- Мы занимаемся
  - обнаружением новых угроз
  - threat hunting
  - поиском zero-day уязвимостей
  - reverse-engineering вредоносного ПО
  - анализом кода
  - анализом поведения хакерских группировок и их тактик, техник и процедур
  - поиском уязвимостей аппаратных решений
- Результаты работы используются для обновления баз угроз Positive Technologies, совершенствования существующих алгоритмов и разработки новых продуктов и решений

Продвинутый инструмент вашего ИБ отдела

Максимально **быстро обнаружить присутствие** злоумышленника в сети и воссоздать **полную картину атаки** и **сохранить трафик для** детального расследования.

Решаемые задачи:

- Предотвращение проникновения в инфраструктуру через основные векторы атак;
- Максимально быстрое **выявление присутствия** злоумышленника в сети;
- Повышение **эффективности расследований** благодаря возможности детального восстановления путей перемещения злоумышленника в сети;
- **Выявление слабых мест защит**ы и получение экспертных рекомендаций для повышения уровня защищенности.

Продвинутый инструмент вашего ИТ отдела

Максимально **быстро обнаружить источник проблемы в сети**

Решаемые задачи:

- Кто грузит сеть или Интернет канал?
- Есть ли «левые» DHCP?
- Кто обходит средства удаленного подключения (TeamViewer, SSH туннели)
- Кто избежал правил по изоляции и сегментации? Например гостевой вай фай иногда становился внутренним, потому что админы косячат с правилами. Можно отследить когда там появляются подключения к внутренним адресам.
- Кто сливает данные? когда у тебя кто-то выкачивает все исходные коды или Wiki - это большой трафик
- Кто использует сервис, который надо ИТ службе отключить или переделать? Например хочешь отключить LDAP и перейти на LDAPS, вроде всех предупредил, системы переконфигурировал, а как быть уверенным? Заглянул, проверил, что таких подключений больше нет.

КГ НИЦ

«Калининградский государственный научно-исследовательский центр информационной и технической безопасности» (КГ НИЦ) использует систему анализа трафика и выявления атак PT Network Attack Discovery с 2018 года. Тогда мы начинали строить региональный центр безопасности (security operations center, SOC) для защиты органов государственной власти Калининградской области от хакерских атак. С 2020 года SOC функционирует как государственная информационная система «Центр управления безопасностью».

Незаменимой частью центра стал PT NAD. Он дает специалистам SOC около 70% полезной информации об инцидентах, выявленных в органах власти Калининградской области. Нам нравится, что он глубоко разбирает трафик и детально отображает, что происходит в подключенных к мониторингу сетях. Несколько серьезных инцидентов мы выявили благодаря сигналам в PT NAD о подозрительных соединениях.

Вместе со специалистами PT Expert Security Center мы оперативно расследовали сложные запутанные атаки на региональные органы власти и приняли меры по предотвращению их развития.

https://www.ptsecurity.com/upload/corporate/ru-ru/products/nad/36-kg-nic-2.pdf

ВГТРК

Уже в ходе пилотного проекта с помощью PT NAD специалистам ОЗИ ВГТРК удалось обнаружить в корпоративной сети **несколько действующих ботнетов** и другую скрытую вредоносную активность. Вскоре после перехода на боевую систему было выявлено и оперативно ликвидировано несколько программ-майнеров. В результате проекта ВГТРК получила удобный инструмент для контроля вредоносной активности в сетевом трафике и возможность для выполнения требований регуляторов — в частности, новых требований к операторам связи и интернет-проектам, предусмотренных Федеральным законом № 35-ФЗ «О противодействии терроризму».

https://www.ptsecurity.com/upload/corporate/ru-ru/products/nad/NAD-VGTRK-CS-rus.pdf

«PT Network Attack Discovery (PT NAD) — полезный инструмент для мониторинга безопасности сети. После внедрения продукта мы почти моментально увидели первые результаты, которые помогли нам снизить риски безопасности и улучшить защищенность инфраструктуры».

Сотрудникам службы ИБ удалось вывести IT-ресурсы из тени. С помощью PT NAD они обнаружили несколько «теневых» приложений (shadow IT), установка которых не была одобрена IT-отделом.

Антон Мельник, начальник управления ИБ АО «Объединенная энергетическая компания»

https://www.ptsecurity.com/upload/corporate/ru-ru/products/nad/PT-NAD_oehk.pdf