Актуальные вопросы безопасности опорных сетей мобильных операторов

Dmitry Kasymov
dkasymov@ptsecurity.com

ptsecurity.com

Ключевые риски и зафиксированные инциденты

Что может сделать злоумышленник:

- ✓ Отказ в обслуживании - неработоспособность сети и отдельных сервисов
- ✓ Отключение от сети и сервисов отдельных абонентов и групп абонентов
- ✓ Перехват пользовательского трафика - голосовых вызовов и SMS
- ✓ Компрометация персональных данных и «цифровой личности» абонентов, в т.ч. публичных персон и гос. служащих
- ✓ Получение данных о местоположении абонента, статистики его звонков и т.д.
- ✓ Кража денег со счетов абонентов и у оператора

За последнее время зафиксировано существенное увеличение количества атак со стороны украинских операторов:

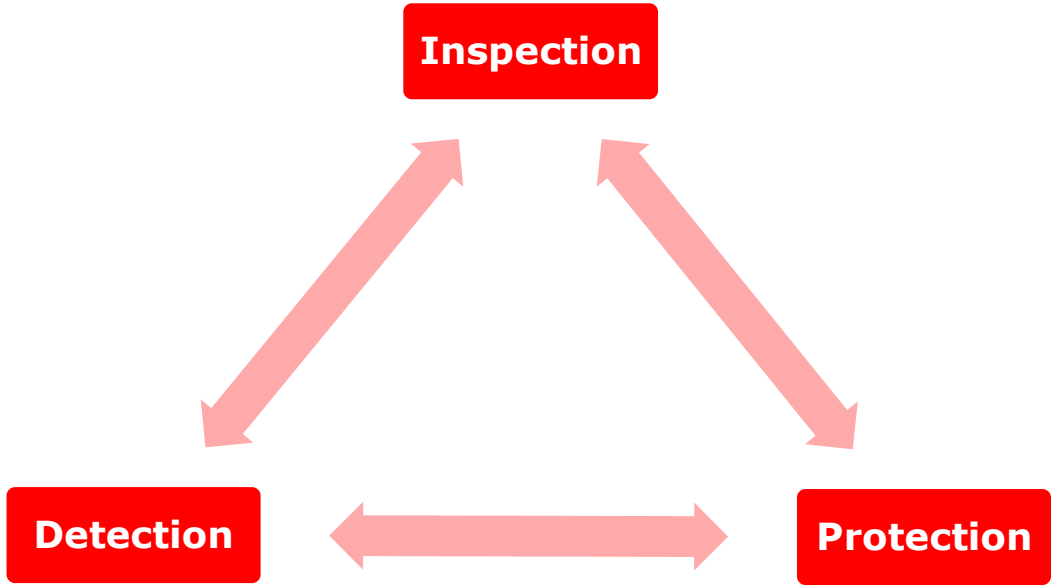
- ✓ Перенос абонентов в роуминг – Fake relocation
- ✓ Массовая рассылка SMS и обзвон абонентов с призывами к противоправным действиям

Отсутствие адекватного реагирования на возросшие угрозы безопасности может привести к массовой реализации инцидентов, связанных с нарушением работоспособности опорной сети и компрометацией данных абонентов

Безопасность сигнальных сетей

с Positive Technologies

Возможность посмотреть на сигнальную сеть глазами злоумышленника. Получение информации о потенциальных уязвимостях сигнальной сети

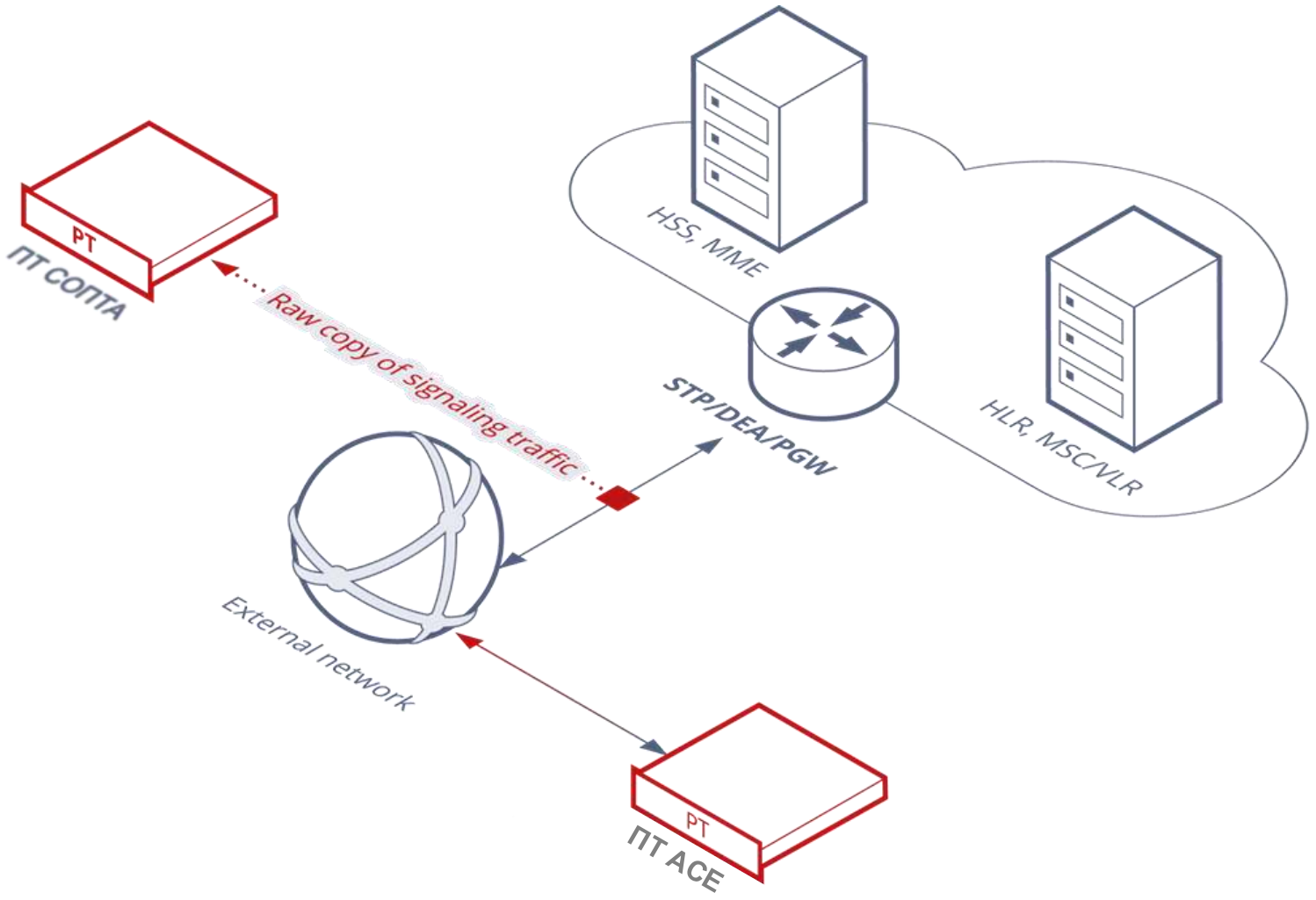


Постоянное выявление нелегитимного трафика в режиме реального времени имеет важнейшее значение для обнаружения атак на ранних стадиях и проверки эффективности принятых мер безопасности

Защита сигнальной сети обеспечивающая полное соответствие рекомендациям GSMA и защиту от актуальных атак сигнальной сети оператора

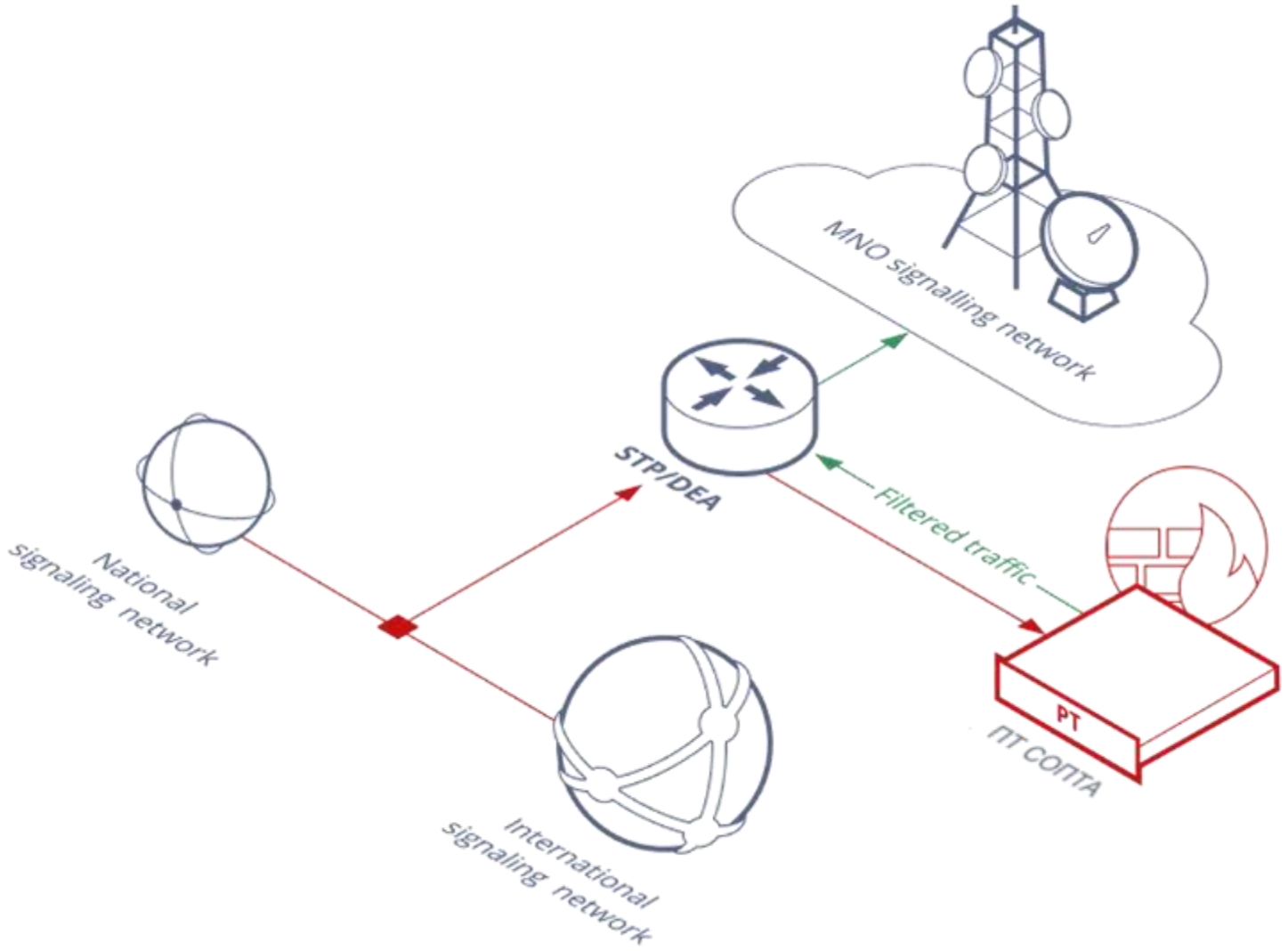
Inspection — Telecom VM

- Информация об существующих и потенциальных уязвимостях
- Рекомендации по улучшению безопасности сигнальной сети
- Возможность посмотреть на сигнальную сеть глазами злоумышленника.



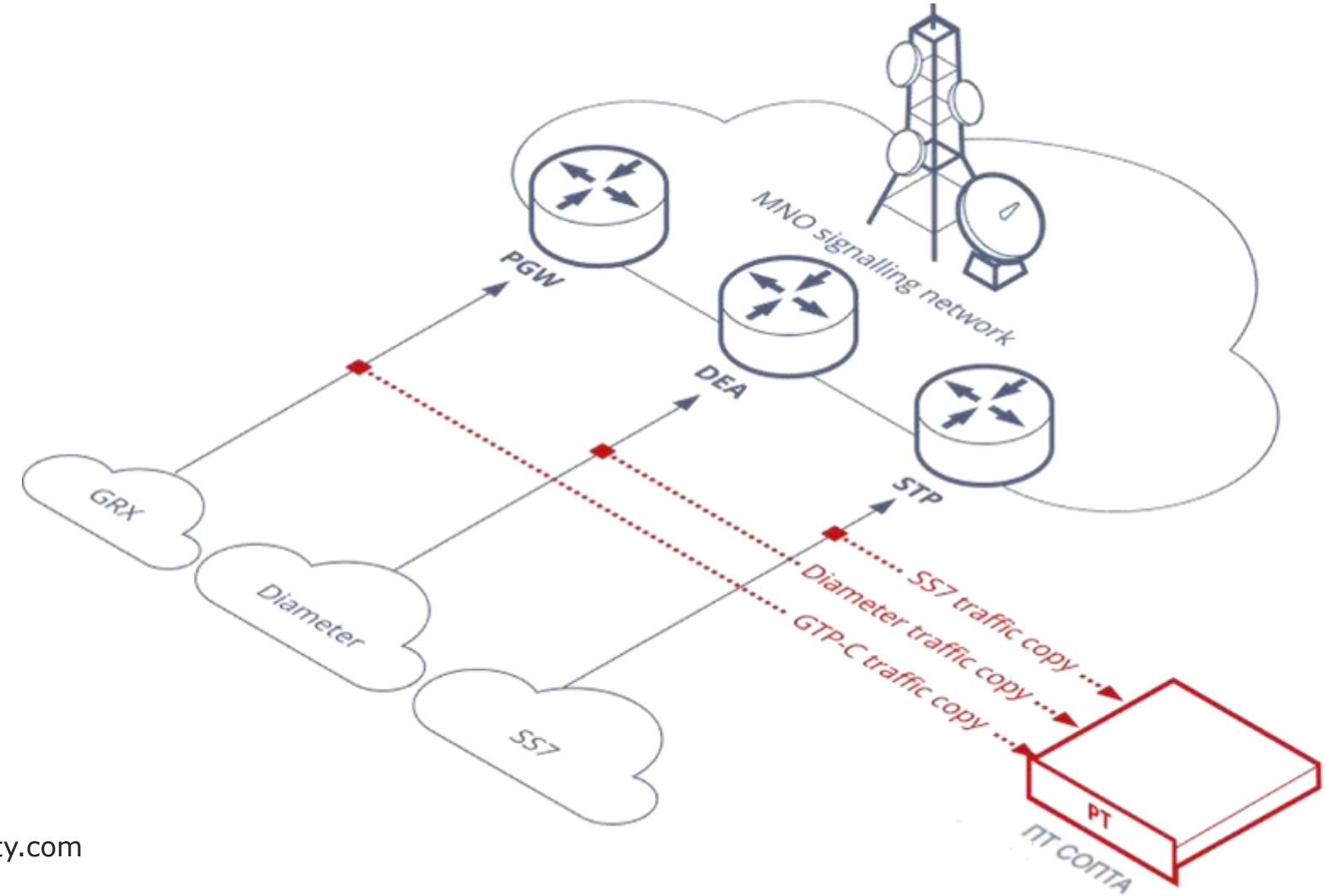
Protection — СОПТА NgFW

- **Защита** от атак злоумышленников
- **Защита** от ошибок в конфигурации
- **Больше безопасности** меньшими усилиями
- Постоянно обновляемая **база знаний**



Detection — СОПТА IDS

- **Пассивный анализ** копии сигнального трафика
- **Выявление** нелегитимного сигнального трафика и атак. Список активных источников атак.
- **Анализ и приоритизация** реальных угроз для сети и абонентов



Рекомендации

Рекомендации

Для сохранения надлежащего уровня предупреждения, выявления и блокирования атак через сигнальные сети на стороне оператора связи необходимо:

1. Своевременно оценивать эффективность инструментов выявления атак через сигнальные сети SS7 и Diameter, что позволяет своевременно обнаруживать атаки на отдельных абонентов мобильной связи и инфраструктуру оператора
2. Проводить периодические внешние аудиты безопасности сигнальных сетей
3. В случае выявления уязвимых мест, оперативно осуществлять модернизацию настроек телекоммуникационного оборудования, например запрещать сигнальные сообщения, которые не используются для организации связи между операторами, но могут применяться при проведении атак на сети операторов связи
4. Отрабатывать процедуры с применением инструментов безопасности, позволяющих оперативно блокировать атаки через сигнальные сети
5. Регулярно проводить киберучения с целью проверки уровня защищенности сигнальных сетей

Рекомендации

В Российской Федерации необходимо создание нормативной базы и единой системы сбора и аналитической обработки информации об атаках через сигнальные сети на инфраструктуру и абонентов мобильных операторов связи, а также подключение ее к ГосСОПКА

Спасибо!

Positive Technologies

ptsecurity.com

Контакты

Дмитрий Финогенов
Советник генерального директора
Positive Technologies
Моб.: +7(916)509-79-32
Эл. почта: dfinogenov@ptsecurity.com

Дмитрий Касымов
Технических менеджер
Моб.: +7(903)105-53-49
Эл. почта: dkasymov@ptsecurity.com