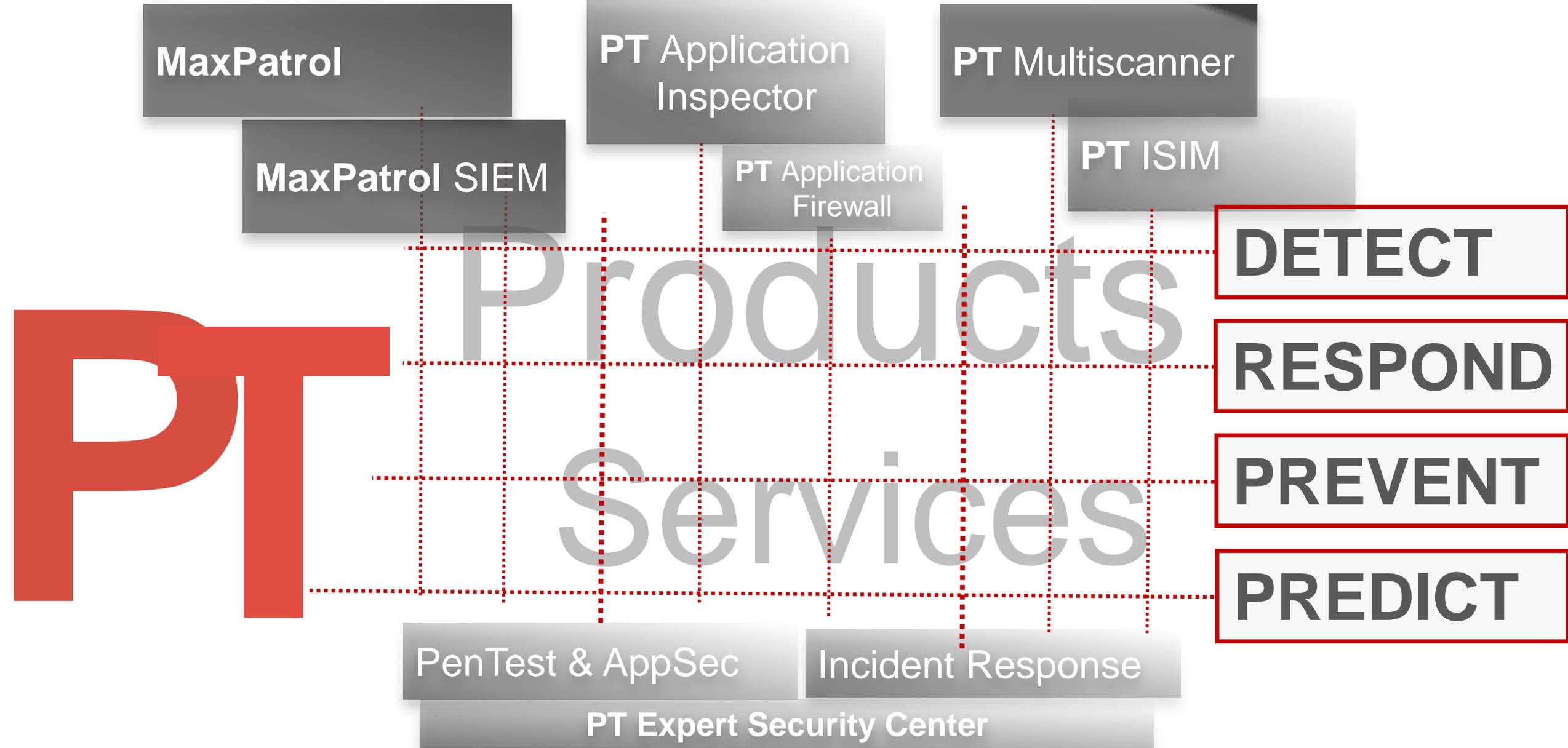


Алексей Качалин

До, после и во время безопасного обмена сообщениями

POSITIVE TECHNOLOGIES

ptsecurity.com



- Мессенджер – Spearfishing 2.0
 - Больше доверия чем почте, СМС
 - Распространение атаки - крайне эффективно
- Массовый эффект – сбор информации о миллионах пользователей
- Передаваемые файлы, архив переписки – кто станет следующей Хилари Клинтон?
- Мессенджер – не метод экстренной связи (но это не точно)

Модель угроз, рассматривающая мессенджер как приложение, использующее СКЗИ – это правильно, но достаточно ли?

- Выведение из строя – в заданное время, по команде
 - Отдельных клиентов
 - Всего сервиса
- Массовые рассылки
 - Спам
 - Информационные атаки (вбросы, подстрекательство)
- Неотказуемость
- Разведка, массовый сбор информации о пользователях и организациях
 - Слежка за пользователями (в т.ч. по метаданным)
- Доверие к владельцу/разработчику сервиса
 - Доступ к данным
 - Внесение изменений в функционал клиента

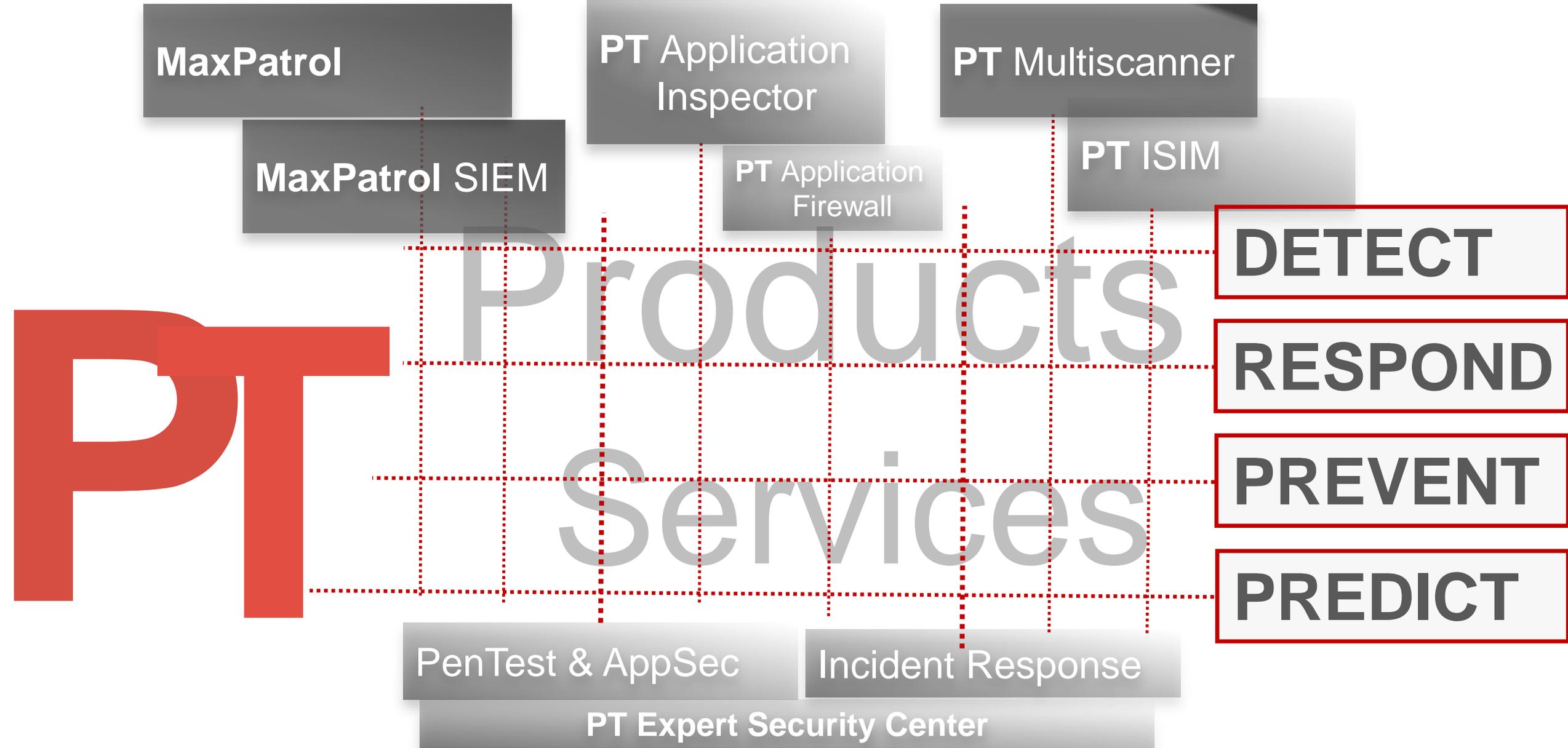
- Пользователь – человеческий фактор
- Операторы сервиса – злоупотребления привилегированных пользователей
- Разработчик
- Оператор связи
- Клиентская часть
 - Аппаратная платформа (мобильные устройства)
 - Мобильное приложение
 - ...
- Инфраструктура оператора сервиса
 - ...
- Каналы доступа

Компенсирующие средства защиты возможны – если не игнорировать возможные уязвимости и угрозы

- Безопасная разработка
 - Предотвращение внесение уязвимостей
 - Оперативное устранение уязвимостей
- Анализ защищенности инфраструктуры
- Контроль компрометации инфраструктуры разработчиков и сервисов распространения приложений
- Мониторинг атак на инфраструктуру и пользователей
 - Контроль передаваемых файлов, ссылок

- Мессенджер – эффективный инструмент, необходимый государству и обществу
 - «Рабочее» и «домашнее» использование
- Акцент на безопасности и доверии
- Разработка требований и рекомендаций по безопасности
 - Учет существующих требований
 - Рекомендации регуляторов для проекта ГМ
 - Рекомендации экспертов и практиков
- Поэтапное повышение требований
- Формирование и развитие рынка
 - Плавный переход на ГМ

- Расширить понимание актуальных угроз
 - Специфика уязвимостей и угроз
 - Ограничение методов защиты/контроля
 - Специфика моделей нарушителя
- ...с точки зрения криптографической защиты и других аспектов практической безопасности



POSITIVE TECHNOLOGIES

Positive Technologies Products & Services

<https://www.ptsecurity.com/>

Positive Research & Security Announcements

<http://securitylab.ru>

Positive Hack Days Security Conference

PHDays.com

PHDays 7. 2017 May, 23-24th



**Alexey
Kachalin**

AKachalin@ptsecurity.com

POSITIVE TECHNOLOGIES: EXPERTS IN SECURITY OFFENSE & DEFENSE



POSITIVE TECHNOLOGIES

ptsecurity.com