POSITIVE TECHNOLOGIES

ptsecurity.com

Алексей Новиков

А свежий ли у вас SOC?

Или кто мониторит мониторящего

Disclaimer

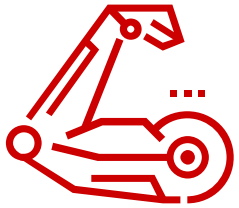
POSITIVE TECHNOLOGIES

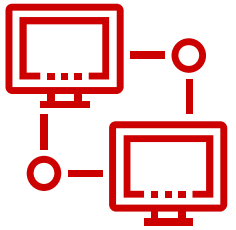
Я не буду говорить о:

- Процессах и моделях зрелости в вакууме
- Best practice (MITRE и прочие)
- Ценностях для бизнеса

PT Expert Security Center

POSITIVE TECHNOLOGIES





Более 50 полномасштабных расследований	**У трети был SOC**
Инцидент произошёл	X
Инциденту больше месяца*	X
Обнаружен по факту кражи денег	X

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

Статистика за год

POSITIVE TECHNOLOGIES

68%

узнали об инциденте
в результате
ретроспективного анализа

Defensive

2%

обнаружили
действия RedTeam

Offensive

Классификация SOC исходя из выявленных проблем

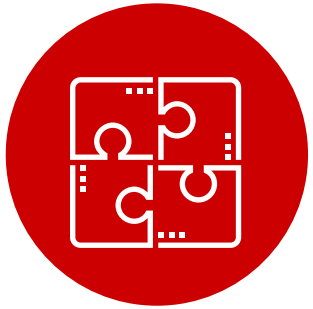
POSITIVE TECHNOLOGIES

Аутсорсинговый SOC

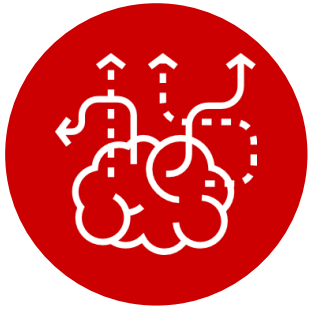
Государственный сектор

SOC в коммерческой структуре

IT SOC



SOC в начале строительства



Те самые 2%

Аутсорсинговый SOC

POSITIVE TECHNOLOGIES

Проблемы

- Сокращают трудозатраты
- Шаблонизация
  - Типовые playbook
  - Типовой инструментарий
  - Типовые компетенции
- Непонимание инфраструктуры
- Кажется, что дорого

Решения

- Quis custodiet ipsos custodies?
- Требования по кастомизации сервиса
- Требования по используемым технологиям
- Red Team

Государственный сектор = ГосСОПКА

POSITIVE TECHNOLOGIES

Проблемы

- Персонал
- Ограничения СЗИ и IT
- Тяготение к «бумажной» безопасности
- Опасные инциденты – не громкие

Решения

- «Учиться, учиться и еще раз учиться» ©
- Дублирование решений?
- Red team
- Ретроспективный анализ инцидентов

SOC в коммерческой структуре

POSITIVE TECHNOLOGIES

Проблемы

- Непрофильное подразделение
- Замыленный взгляд
- Конфликт IT и ИБ
- ИБ – якорь для бизнеса?

Решения

- Подождать пока не случится инцидент?
- Red Team

IT компания

POSITIVE TECHNOLOGIES

Проблемы

- Инфраструктура развивалась без требований ИБ
- Ограничения СЗИ и IT
- Не понимание ИБ контекста

Решения

- Проще все построить с нуля
- Red Team
- Ретроспективный анализ происходящего

Начало строительства

POSITIVE TECHNOLOGIES

Проблемы

- Персонал
- Ограничения СЗИ и IT
- Подходы и практика

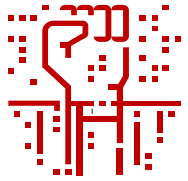
Решения

- Путь осилит идущий
- Red Team
- Правильные технологии
- Ретроспективный анализ

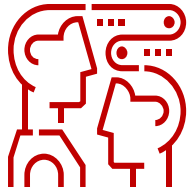
Summary

POSITIVE TECHNOLOGIES

Ретроспектива



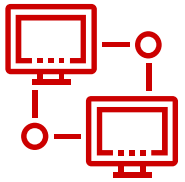
Взгляд со стороны и оценка построенной защиты



Не бояться прибегнуть к помощи

Summary

POSITIVE TECHNOLOGIES



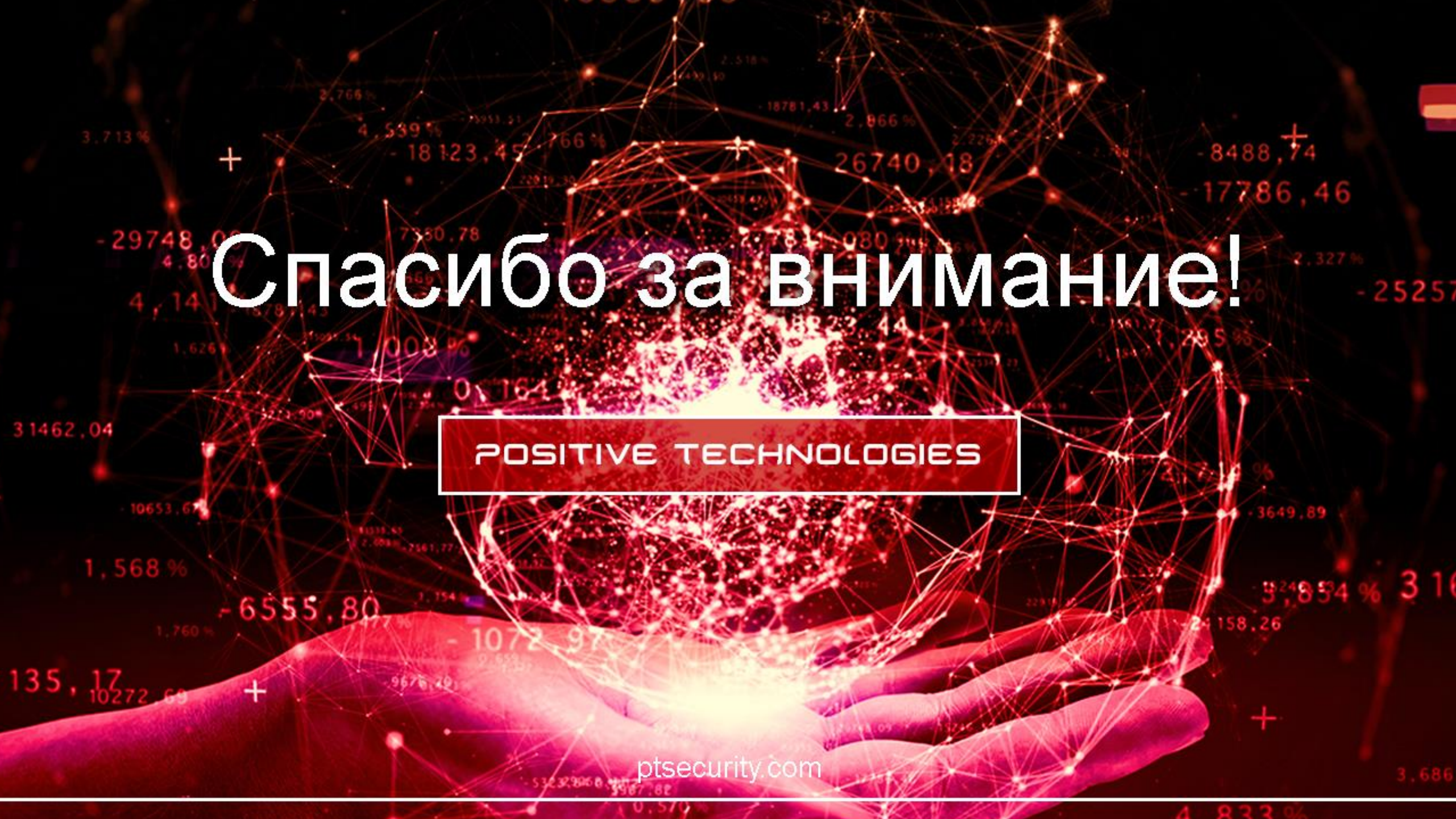
Трафик

Объекты

Ретроспектива

Решение PT для выявления сложных угроз и целевых атак

- Время обнаружения сокращается
- Финансовые потери снижаются
- Эффективность SOC повышается


Спасибо за внимание!
POSITIVE TECHNOLOGIES
ptsecurity.com