
# Как построить эффективный SOC?

**Татьяна Зверева,**
менеджер по продвижению продуктов

ptsecurity.com

# Вопрос не в том, взломают ли вопрос в том - когда

**В 2 раза**

выросло число компаний, которые стали жертвами целевых атак в 2017 году

**90%**

компаний взламываются от одного до пяти дней

**9 из 10**

жертв не замечают факт взлома

**200 дней**

составляет среднее время обнаружения компрометации

# Как защититься?

Постоянно и тщательно наблюдать за активами инфраструктуры

SOC

Результат:

- Значительно снижается вероятность реализации киберугроз
- Факт взлома оперативно выявляется
- Есть время для принятия компенсирующих мер по минимизации ущерба

# SOC – это …

SOC - **центр процесса** управления уязвимостями, выявления и управления инцидентами ИБ, расследования и реагирования на них, threat hunting.

Минимальный перечень **инструментария**: SIEM, VM, IDS/ IPS, Threat Hunting Platform, IRP (SOAR), песочницы.

Необходимая часть SOC - **эксперты** подразделения, которые отслеживают ситуацию в инфраструктуре и в мире, реагируют и расследуют инциденты.

*(с) многие уважаемые аналитические агентства, институты*

# Задачи SOC

**SOC**

- экспертная команда, которая глубоко понимает современный ландшафт киберугроз в мире и адаптирует систему ИБ под новые угрозы

- Предотвращает инциденты
- Выявляет целенаправленные атаки на инфраструктуру
- Снижает время обнаружения и реагирования на инцидент
- Помогает использовать средства ИБ с максимальной результативностью

# 7 типовых ошибок при построении SOC

1. **Недостаточный уровень зрелости ИБ**
   Из систем защиты только межсетевой экран и антивирусная защита

2. **Небольшая команда**
   Подразделение ИБ состоит из 2-х человек, один из которых – начальник

3. **Передача всего процесса на аутсорс**
   У внутренних специалистов нет понимания IT-инфраструктуры

4. **Неверное толкование SOC**
   Закупили SIEM, мониторы и решили, что это SOC

5. **Неправильное планирование**
   Купили сразу все необходимые СЗИ и решили их одновременно внедрить

6. **Неправильное ресурсное планирование**
   Долго взращивают внутреннюю экспертизу или резко увеличивают штат дорогими экспертами

7. **Бездумное применение мировых практик**
   Не адаптируют рекомендации под свои процессы

POSITIVE TECHNOLOGIES

# Чем мы полезны

# Как мы помогаем



## Экспертиза

Наша экспертиза поможет вам выстроить эффективные процессы, понять актуальные угрозы и шаги для повышения уровня защищенности



## Сервисы

Снизим ваши затраты на персонал за счет сервисов экспертного мониторинга, тестов на проникновение, расследования инцидентов, threat hunting



## Продукты

Поможем создать оптимальный для вас SOC на базе экосистемы продуктов по кибербезопасности Positive Technologies

# Почему мы

Делаем:

| | | |
|---|---|---|
| **Аудиты безопасности** | Хакеры знают, как вас можно взломать | Узнайте реальные вектора атак на ваши системы |
| **Расследование атак** | Хакеры сидят в инфраструктуре до 3 лет | Поможем выявить взломанные узлы и сервисы |
| **Продукты безопасности** | Количество и сложность векторов атак растет | Строим SOC для выявления атак. 70% средств в типовом SOC - продукты PT |

**17**

лет опыта исследований и разработок

**250**

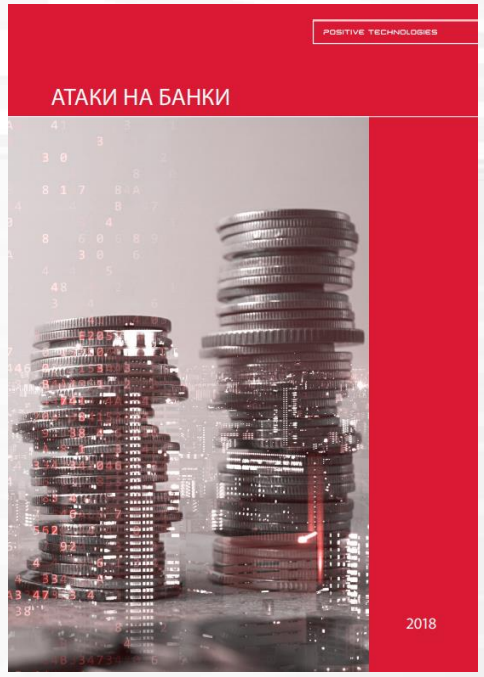
экспертов в нашем исследовательском центре — одном из крупнейших в Европе

**1000**

клиентов банковской и телеком- сфер, госсектора, промышленной отрасли

# Исследования и расследования

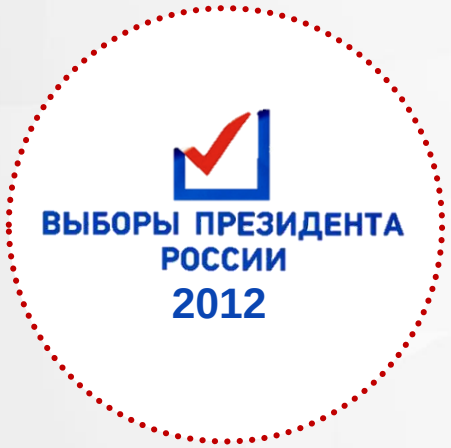



ptsecurity.com/ru-ru/research/analytics

# Почему мы

## Опыт работы в глобальных инфраструктурах:






POSITIVE TECHNOLOGIES

# Наш подход к построению SOC

# Двигаемся постепенно

**0** Аудит периметра

**1** Защита периметра

**2** Защита внутренней инфраструктуры

**3** Продвинутые методы защиты

**4** Обучение специалистов SOC

# Аудит периметра

## Задачи:

- Инвентаризация внешних информационных систем
- Анализ типовых уязвимостей внешних информационных систем

## Продукты:

**Сервис Advanced Border Control**

## Результат:

Знаете:

- как выглядит периметр глазами внешнего нарушителя
- какие «белые пятна» необходимо устранить

# Защита периметра

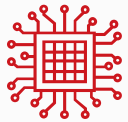
## Задачи:

- Выявление атак на периметре
- Выявление вредоносного ПО на периметре
- Обнаружение атак на публичные сервисы

## Продукты:

**PT Application Firewall**

**PT MultiScanner**



**PT Network Attack Discovery**

## Результат:

Закрыты основные вектора атак извне:

- веб,
- почта,
- пользовательский трафик

# Защита внутренней инфраструктуры

## Задачи:

- Инвентаризация  и выявления уязвимостей внутренних ИС
- Выявление вредоносного ПО внутри инфраструктуры
- Выявление следов компрометации в трафике
- Анализ событий безопасности и выявление инцидентов
- Обнаружение атак в АСУ ТП

## Продукты:

**MaxPatrol 8**

**PT Network Attack Discovery**

**PT MultiScanner**

**MaxPatrol SIEM**

**PT ISIM**

## Результат:

- Построена и автоматически обновляется полная картина IT-инфраструктуры
- Автоматически выявляются инциденты и атаки в корпоративной и специфических (АСУ ТП) инфраструктурах

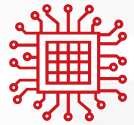
# Продвинутые методы защиты

## Задачи:

- Анализ исходного кода
- Расследование инцидентов
- Ретроспективный анализ сетевого трафика
- Динамический анализ вредоносного ПО
- Оценка соответствия стандартам
- Регулярная оценка защищенности
- Threat Intelligence и Threat Hunting

## Продукты:

**PT Application Inspector**



**PT Network Attack Discovery**

**PT MultiScanner**

**MaxPatrol SIEM**

**MaxPatrol 8**

**Pentest**

## Результат:

- Снижаются риски взлома веб-приложений и инфраструктуры в целом
- Выстроен процессный подход к расследованию и выявлению атак
- Инфраструктура соответствует внутренним и внешним стандартам ИБ

# Обучение специалистов SOC

## Задачи:

- Обучение реагированию на инциденты
- Обучение расследованию инцидентов
- Обучение использованию продуктов в SOC

## Сервисы:

**PT Expert Security Center**

## Результат:

Повышается уровень экспертизы:

- сотрудников I линии в выполнении задач по непрерывному мониторингу
- сотрудников I линии и II линий в расследовании и реагировании на инциденты

# Оценка эффективности SOC

ежемесячно в течение года


| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| Совместно | Positive Technologies | Positive Technologies | Совместно | Совместно |
| Выявляем актуальные угрозы | Формируем перечень векторов атак, реализующих выявленные угрозы | Реализуем каждый из векторов атак | Оцениваем корректность отработки средств защиты, процессов и команды | Корректируем настройки систем защиты, компонентов инфраструктуры, процессов реагирования на инциденты |

**Результат:**

Повышается эффективность процессов выявления и реагирования на инциденты, выполняется SLA

# Команда SOC

**Руководитель SOC**

**1-я линия:**
Первичная оценка инцидентов, отработка ложных срабатываний, обработка по плейбукам

**2-я линия:**
Глубокое расследование инцидентов

**3-я линия:**
Глубокий анализ артефактов инцидентов

**Аналитики:**
Написание плейбуков, внутренний TI

# Собираем команду SOC

1

Определяете руководителя SOC из существующей команды

2

Набираете специалистов I линии реагирования

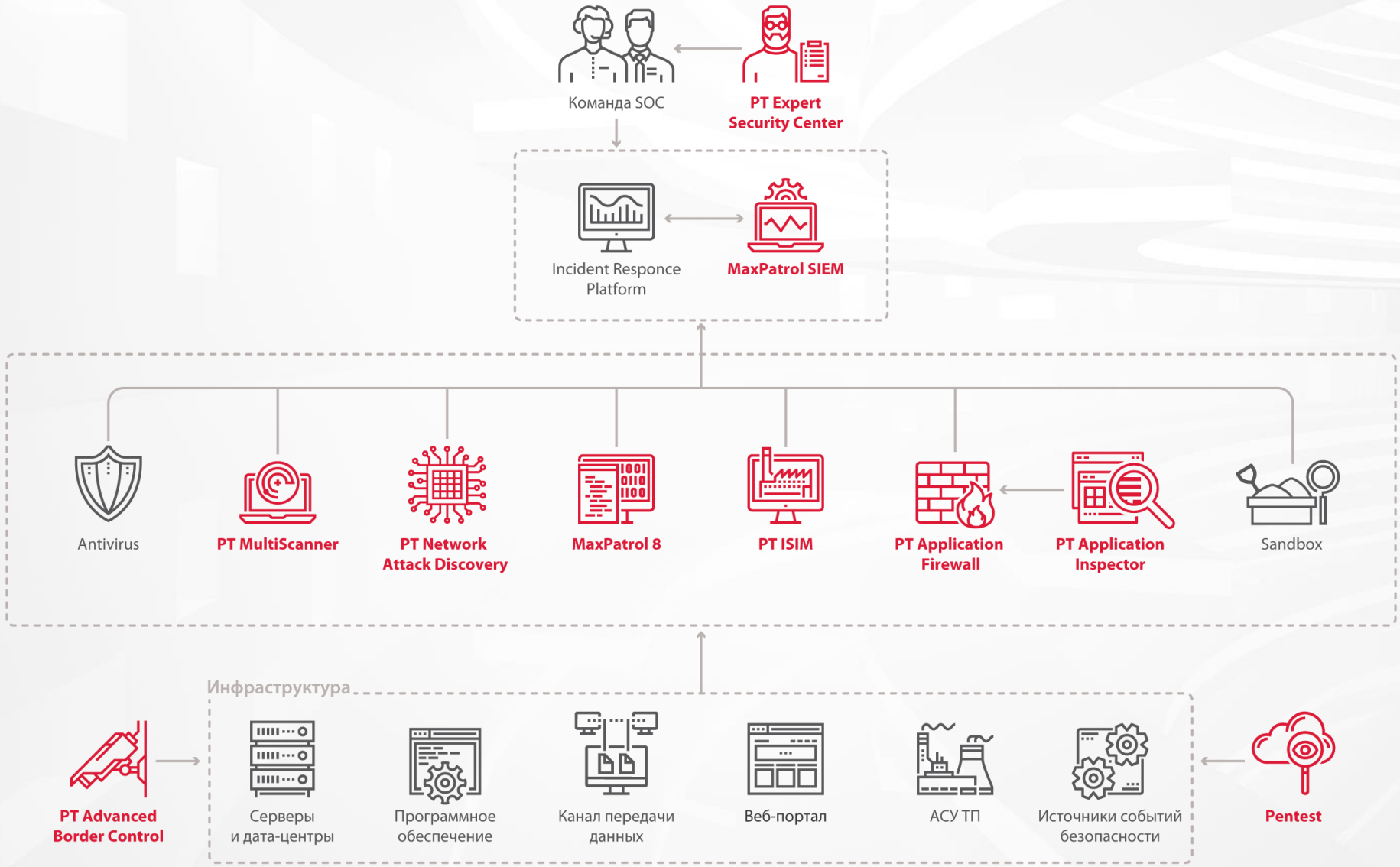
3

II и III линии реагирования в первый год на специалистах PT ESC*

Параллельно взращивается экспертиза внутренней команды

*экспертный центр мониторинга Positive Technologies Expert Security Center

# Архитектура Positive SOC



# Результаты Positive SOC

Минимизация потерь от инцидентов

Развитие внутренней экспертизы

Отсутствие «полочного» ПО (shelfware)

Повышение трудозатрат злоумышленника на вход

Выявление и своевременное реагирование на актуальные угрозы:

- Отсутствие «белых пятен» в инфраструктуре
- Мониторинг актуальных уязвимостей и их оперативное устранение
- Оперативное выявление критичных инцидентов
- Ретроспективное выявление следов компрометации


Свяжитесь с нами:
+7 495 744 01 44
sales@ptsecurity.com
ptsecurity.com