Что нам стоит SOC построить?

SIEM для людей или люди для обслуживания SIEM?

Владимир Бенгин

Руководитель отдела поддержки продаж

Positive Technologies

POSITIVE TECHNOLOGIES

ptsecurity.com

SOC – «Не знаю, сможем ли, но точно хочу!»

POSITIVE TECHNOLOGIES

- Модный тренд
- Это лучший способ обеспечения #реальнойИБ и оперативного выявления атак
- Дорого и трудоемко, но это возможность разобраться с тем хаосом, который творится внутри организации

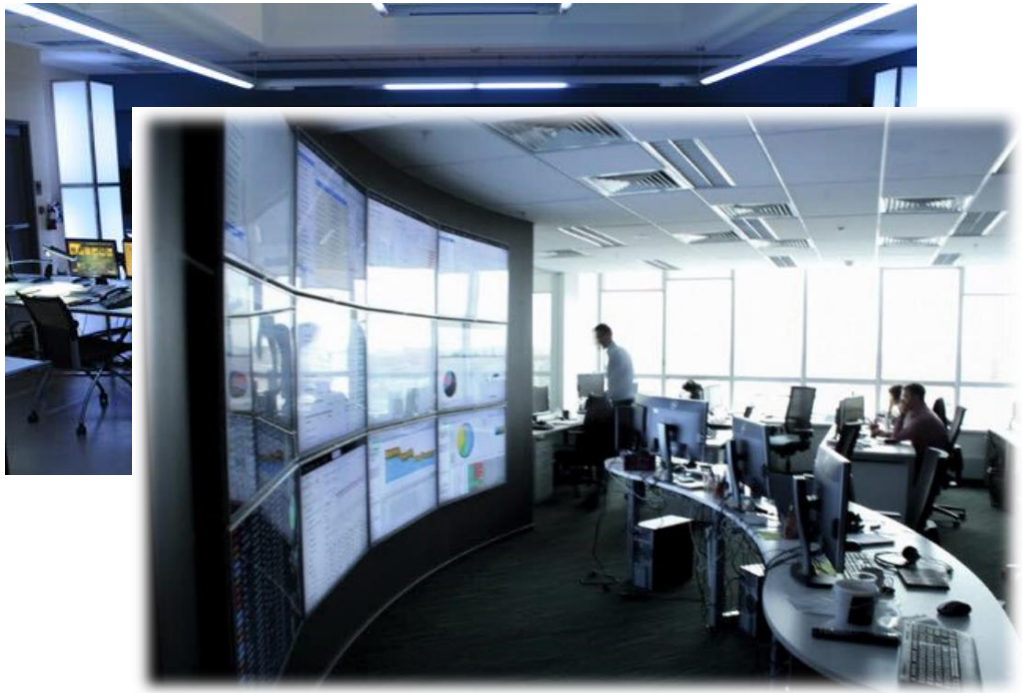
SIEM-система – ключевой технологический элемент SOC:

- Единая точка контроля ИБ и работы средств СЗИ, интегрированная в ИТ-инфраструктуру
- Унификация поступающей информации и её перекрестный анализ в едином интерфейсе
- Средство выявления и расследования инцидентов ИБ

Security Operations Center: ожидания

POSITIVE TECHNOLOGIES

- Ситуационный центр с красочными графиками и отчетами
- Защита от большинства актуальных угроз ИБ, в т.ч. использующих уязвимости нулевого дня
- Выявление и расследование инцидентов с соблюдением SLA
- Небольшая но эффективная команда, (по пару человек на пару линий реагирования)



С чего начинаем. Шаг №1

POSITIVE TECHNOLOGIES

Первоочередная задача – сбор и систематизация информации об ИТ-инфраструктуре

- Опрос системных администраторов
- Использование различных средств по поиску и инвентаризация сетевых узлов
- Интеграция средств инвентаризации с SIEM

С чего начинаем. Шаг №1

POSITIVE TECHNOLOGIES

Первоочередная задача – сбор и систематизация информации об ИТ-инфраструктуре

- Опрос системных администраторов
- Использование различных средств по поиску и инвентаризация сетевых узлов
- Интеграция средств инвентаризации с SIEM
- **Классификация и упорядочивание**

Инфраструктура постоянно меняется!

- Мониторинг задач по сбору
- Настройка задач сбора с новых устройств
- Постоянная адаптация задач под изменяющиеся условия

POSITIVE TECHNOLOGIES

Инфраструктура постоянно меняется!

- Мониторинг задач по сбору
- Настройка задач сбора с новых устройств
- Постоянная адаптация задач под изменяющиеся условия
- **ПРАВИЛА КОРРЕЛЯЦИИ!**

Непрекращающийся процесс внесения изменений

POSITIVE TECHNOLOGIES

ПО обновляется → Обновляем формулы нормализации

Появляется новые приложения → Пишем новые формулы нормализации

Изменились формулы нормализации → Меняем правила корреляции

……

2-3 года и SIEM приходиться внедрять повторно

Не только лишь одни логи

POSITIVE TECHNOLOGIES

Интеграция различных систем ИБ с SIEM

- Системы класса Vulnerability Management
- Configuration Management
- Asset Management
- …

Двусторонняя интеграция, например обратная интеграция с Vulnerability Management

Нужно создать экспертизу с нуля собственными силами

- SIEM даёт лишь инструментарий
- Никто кроме самого заказчика не знает что именно нужно выявлять

Спасение утопающих — дело рук самих утопающих!

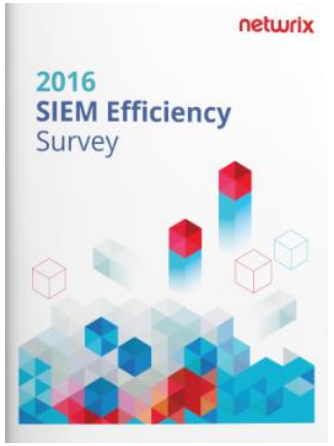
Security Operations Center: реальность

POSITIVE TECHNOLOGIES

Варианты:

- «Пока не получилось» «Ещё не успели построить» «В процессе набора команды» «Выстраиваем процессы»
- «Получилось… Очень красивые графики и отчётность для руководства!»
- «Мы гордимся тем, что построили. Правда за это время штат увеличился в несколько раз.»

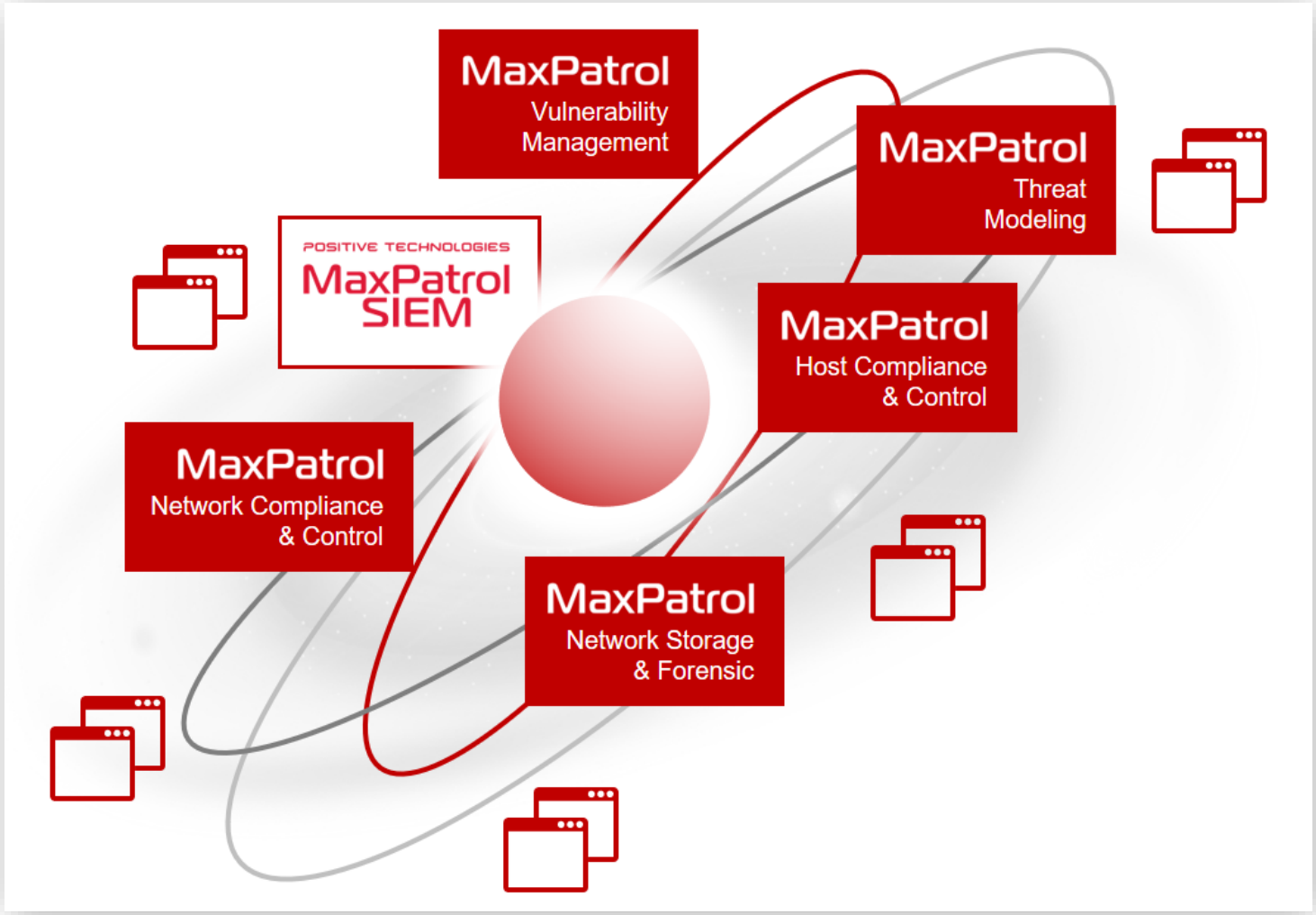
Большинство из задач команды выглядят рутинно, а значит должны были быть автоматизированы



- **69% респондентов ищут возможность сократить стоимость SIEM**
- **Разрастание персонала – главная причина увеличения стоимости SIEM**

MaxPatrol SIEM

POSITIVE TECHNOLOGIES



- Встроенный полноценный Asset Management
- Единая платформа для множества классов решений
- Адаптация к изменяющейся инфраструктуре
- Постоянная поддержка источников от производителя в рамках ТП

- РТКВ, стоит бросить круг утопающим!

Спасибо!

POSITIVE TECHNOLOGIES

ptsecurity.com