POSITIVE TECHNOLOGIES

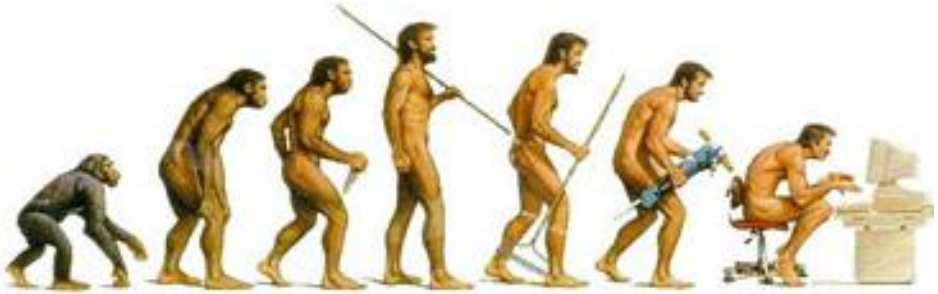
POSITIVE TECHNOLOGIES

Топология в MaxPatrol SIEM

Сергей Павлов

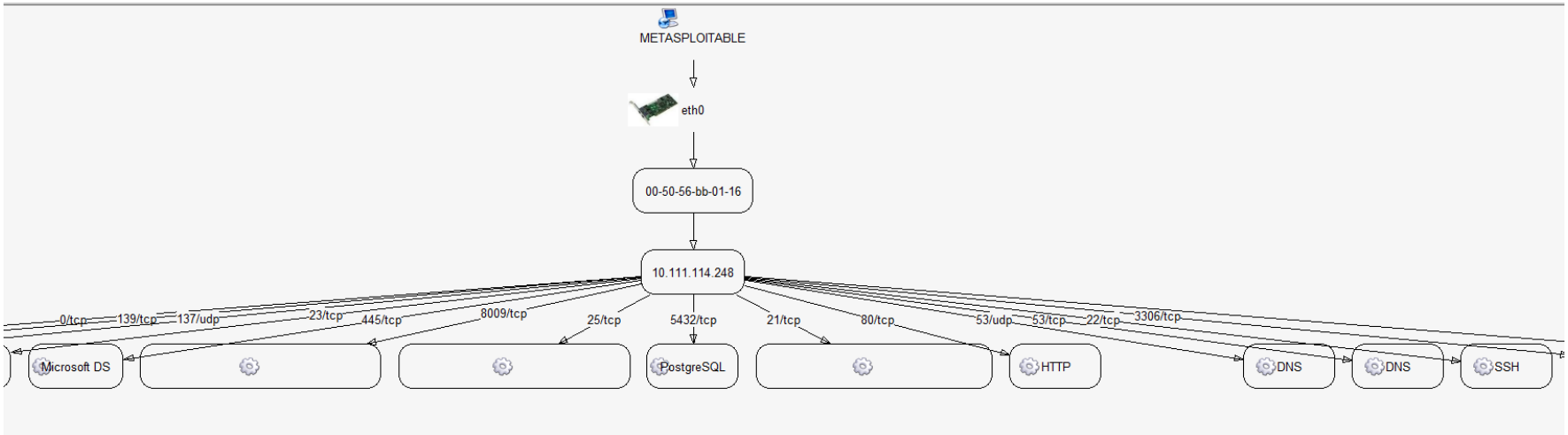
Positive Technologies

Предыстория



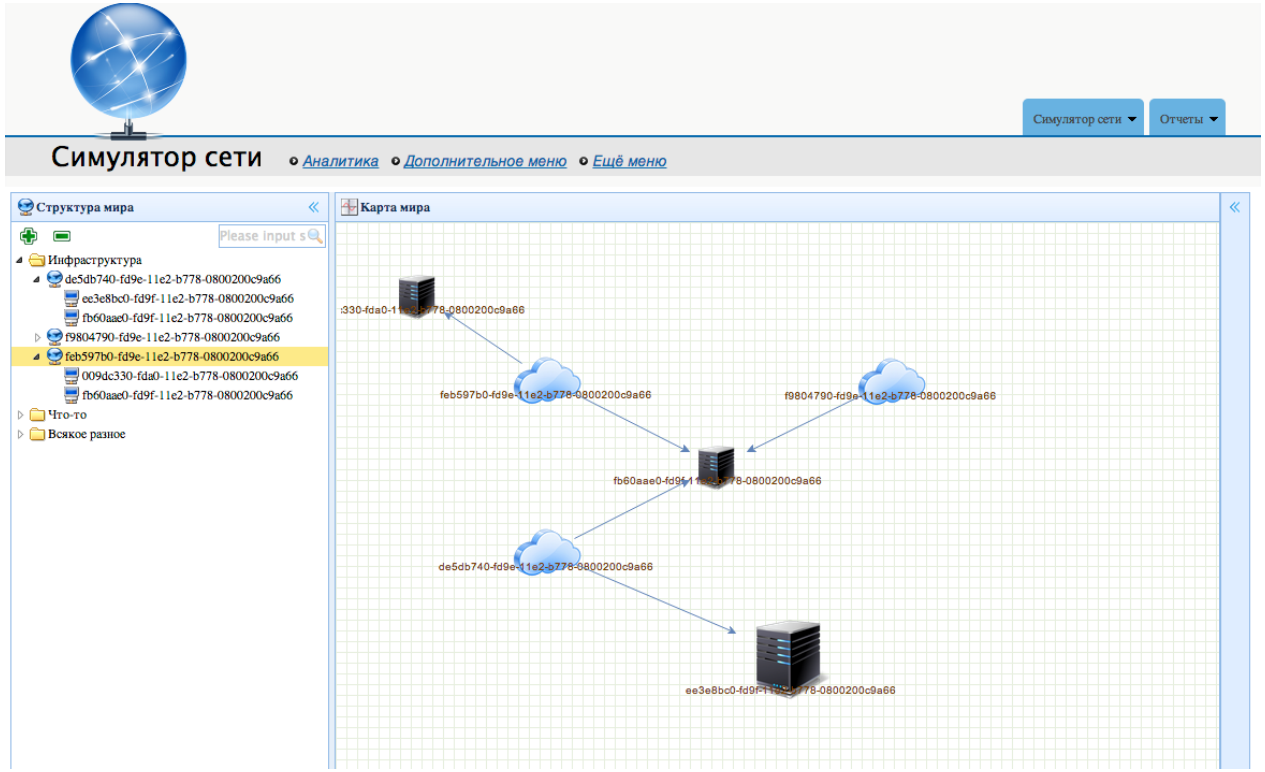
История создания продукта
Проект Sampo (2012 год)

- Источник: данные MaxPatrol 8
- Концепт: модель OSI



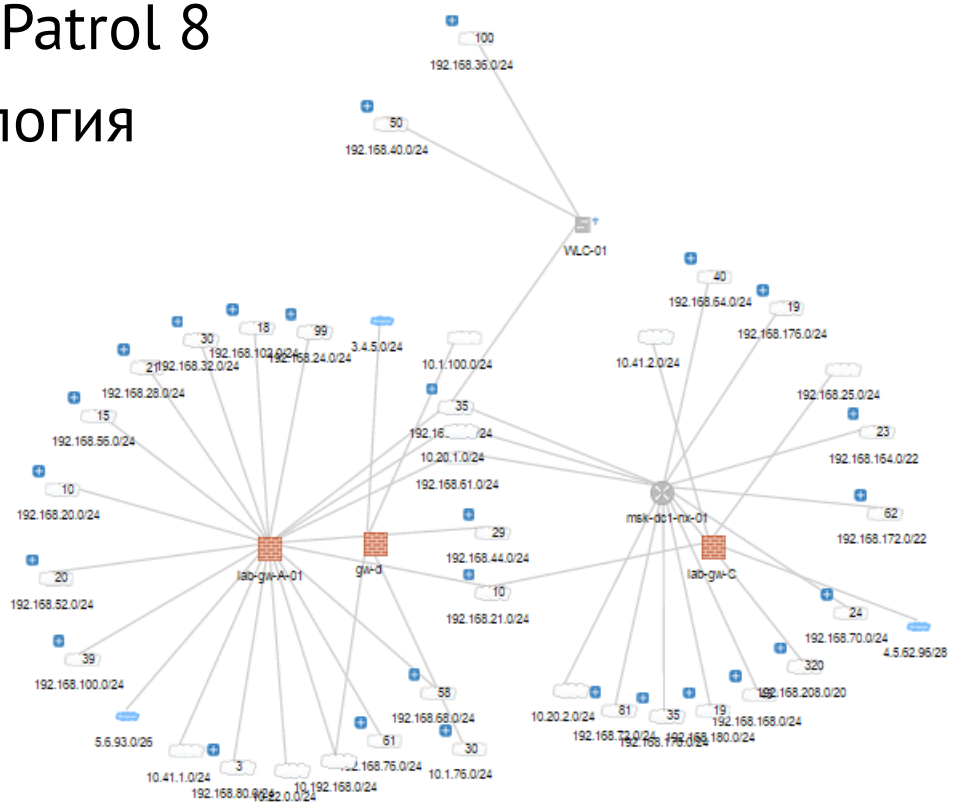
История создания продукта. Проект Network Analyzer (2013год)

- Источник: данные MaxPatrol 8
- Концепт: сетевая топология



История создания продукта. Проект MaxPatrol Topology (2014 год)

- Источник: данные MaxPatrol 8
- Концепт: сетевая топология



Результаты.

Плюсы

- Успешным проектом признан «MaxPatrol Topology».
- В качестве источника для карты сети нужны данные MaxPatrol 8, который у Вас уже есть ;)
- Более 20 клиентов протестировали данное решение.

Минусы

- Карта сети строится только для сетевого оборудования
- Нет полноценной интеграции с MaxPatrol 8

И еще немного про MaxPatrol Topology.

Только сегодня и только сейчас можно получить дистрибутив на безвозмездной основе

Что для этого нужно?

— Активированный MaxPatrol 8

— Отправить письмо на spavlov@ptsecurity.com

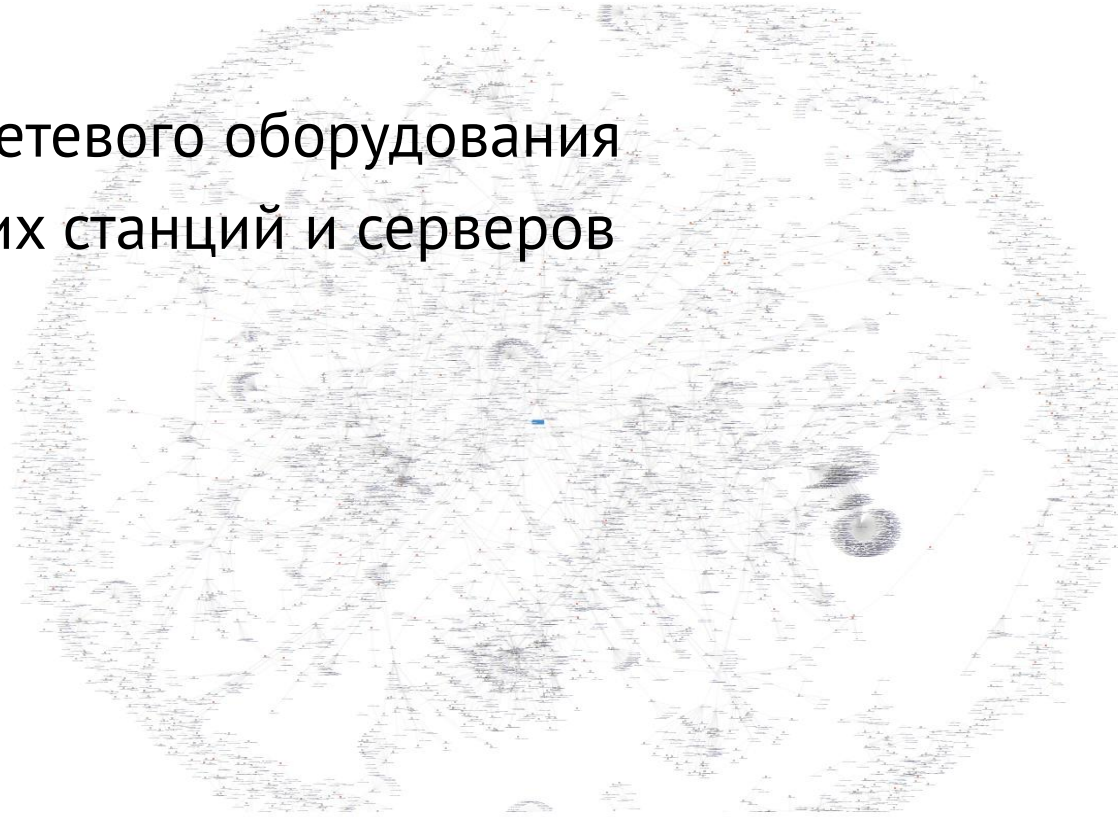
- В письме указать номер лицензии MaxPatrol 8
- Название вашей компании

Примеры MaxPatrol Topology. Средняя сеть.

- 200 единиц сетевого оборудования
- 50 000 рабочих станций и серверов
- 1 000 сетей

Примеры MaxPatrol Topology. Большая сеть

- Более 5 000 единиц сетевого оборудования
- Более 150 000 рабочих станций и серверов
- Более 6 000 сетей

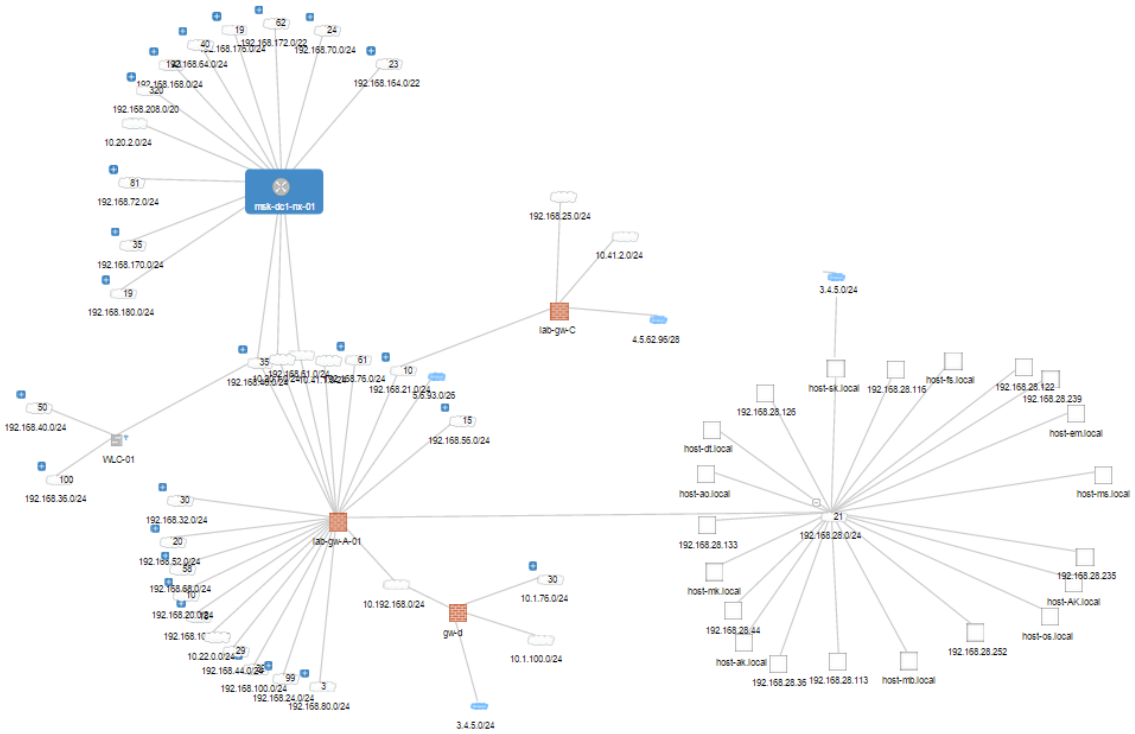


Подведя итоги. Цели построения карты сети

- Активное построение карты сети
- Ведение актуальной информации по топологии сети
- Инвентаризация оборудования
- Внедрение средств безопасности
- Планирование и развитие инфраструктуры сети
- Отображение объектов, нарушающих политику безопасности
- Выявление внешних каналов связи
- Идентификация источников атаки

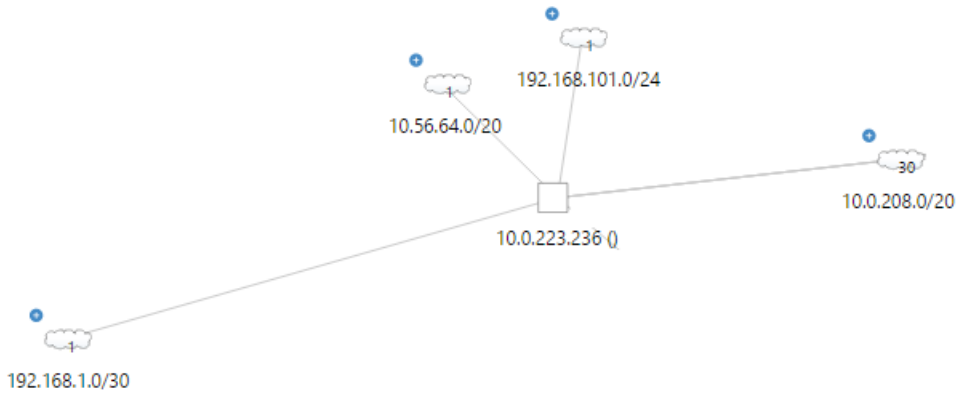
Цели построения карты сети

- Контроль изменений
- Выявление внешних каналов связи
- Выявление проблемных участков сети



Цели построения карты сети

- Выявление «левых» IP-адресов
- Нарушение границ сети



Цели построения карты сети

- Фильтрация узлов по уязвимостям (CVE, CVSS)
- Отображение самых критичных узлов, в том числе и по инцидентам
- Отображение узлов по различным критериям
- Отображение узлов по ответственным
- Просчет достижимости между узлами
- Вектора атак

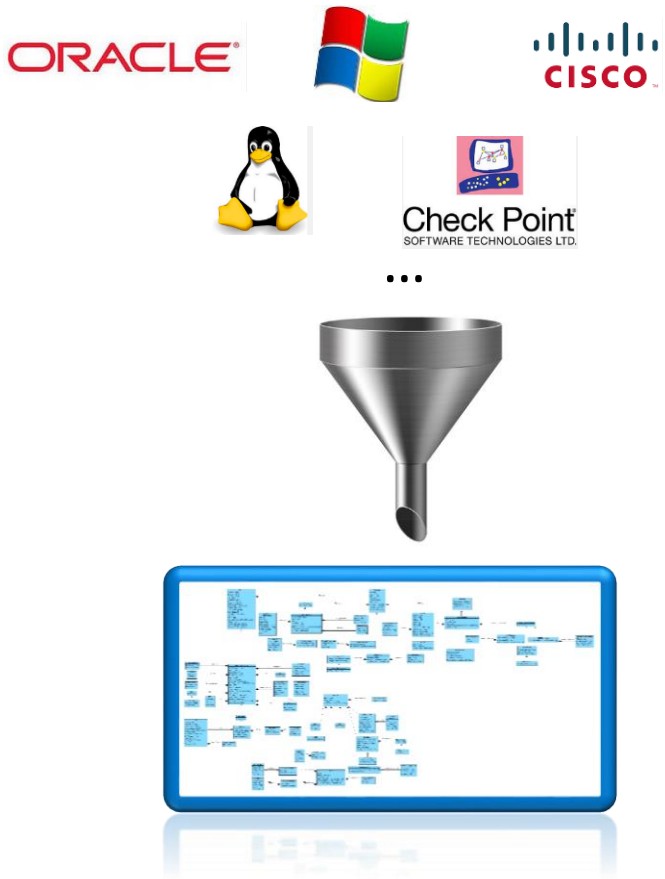
И НАКОНЕЦ! Топология в MaxPatrol SIEM

— Рассмотрим

- Процесс накопления базы знаний
- Взаимодействие компонентов
- Несколько примеров с построением карты сети

Процесс накопления базы знаний

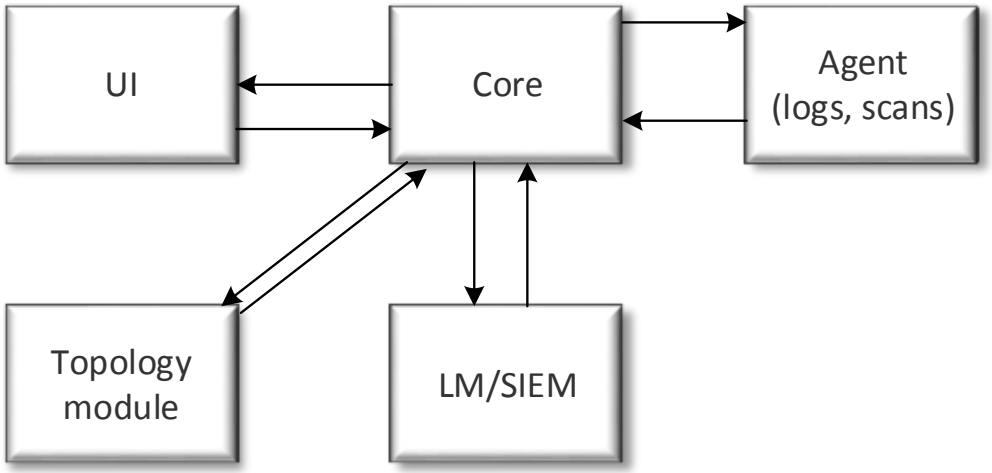
— Данные всех систем приводятся в унифицированный вид



Унифицированная модель представления данных

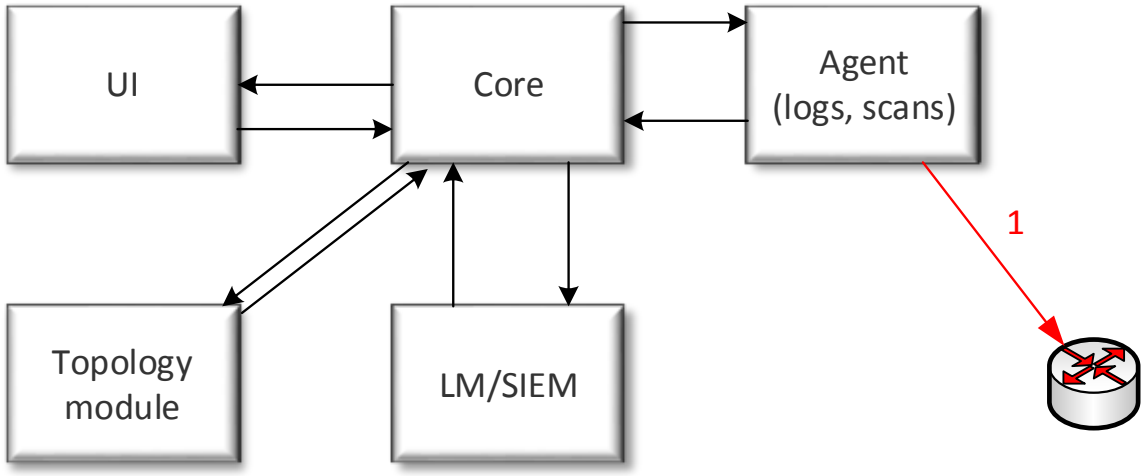
Взаимодействие компонентов MPX

— Core
— PTKB
— Agent
— SIEM
— UI



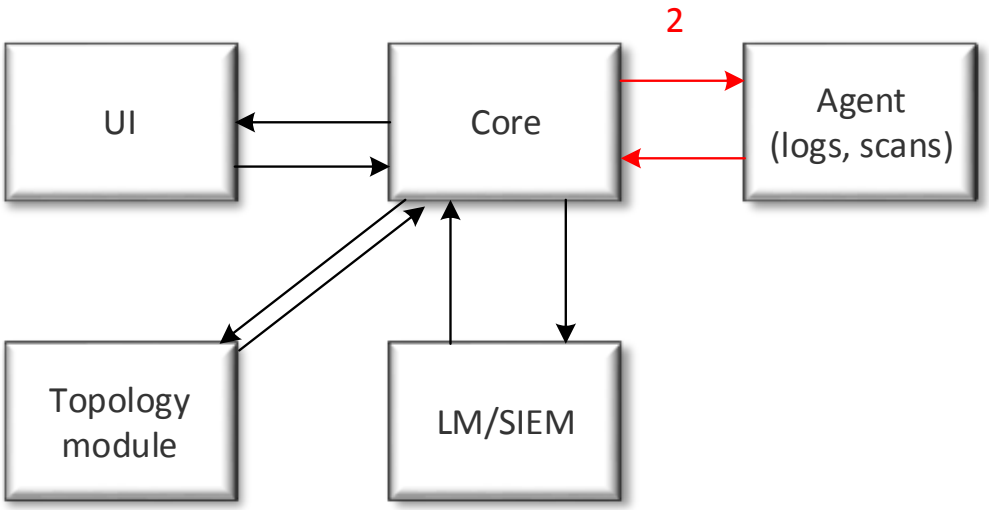
Взаимодействие компонентов.

Шаг 1. Сканирование конечной цели



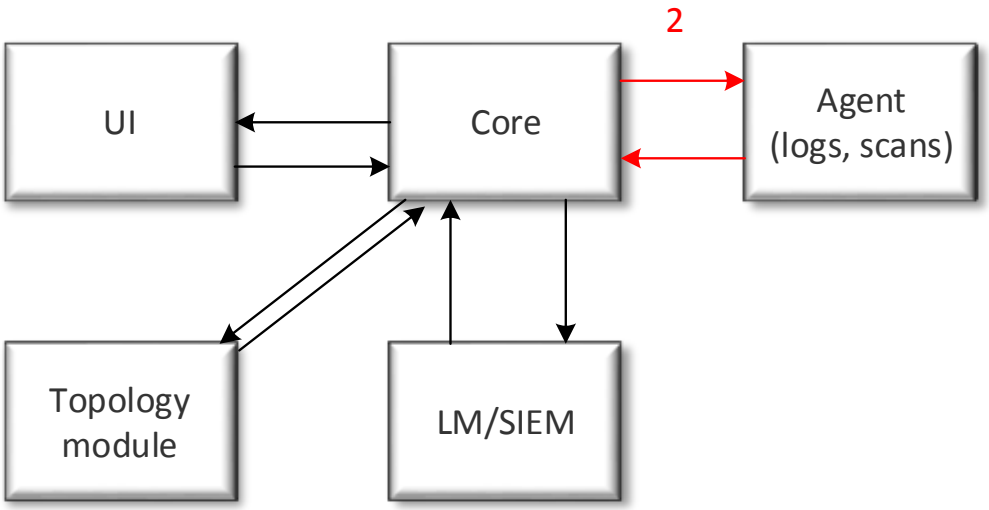
Взаимодействие компонентов.

Шаг 2. Передача данных от агента к ядру



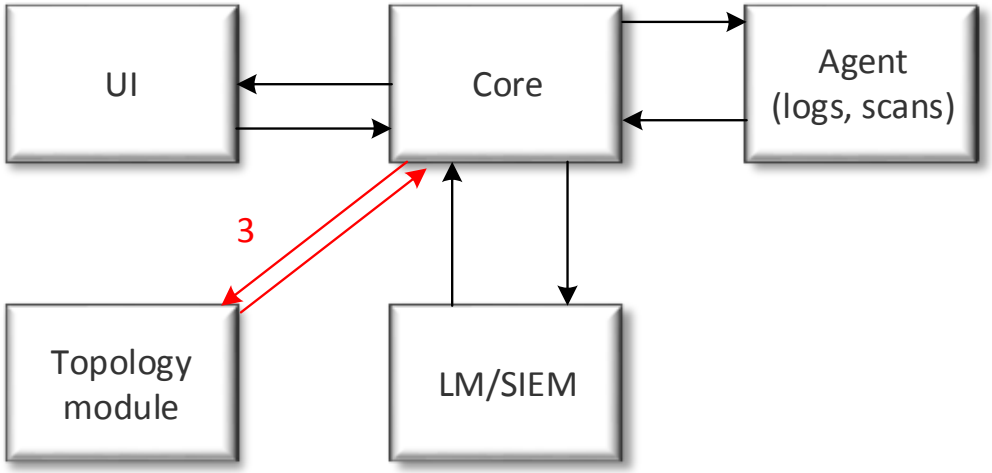
Взаимодействие компонентов.

Шаг 2. Передача данных от агента к ядру



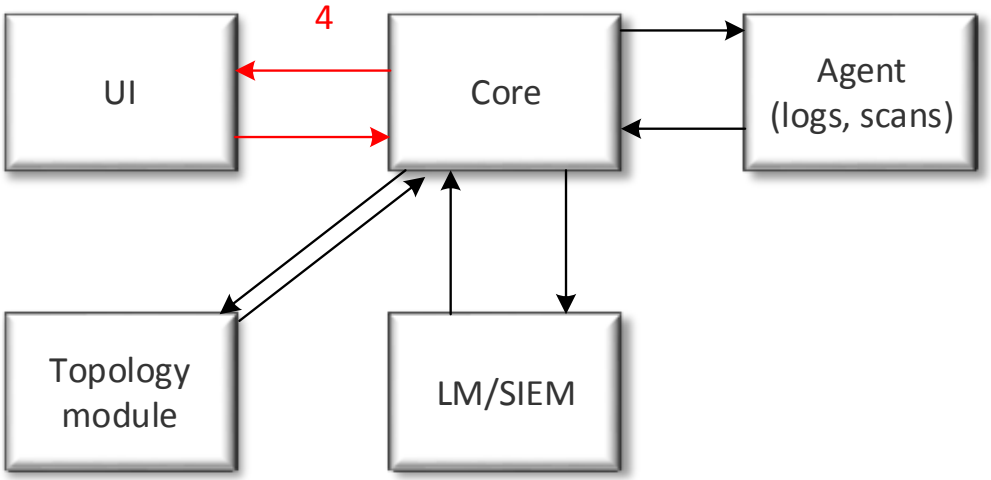
Взаимодействие компонентов.

Шаг 3. Дополнительная обработка информации.



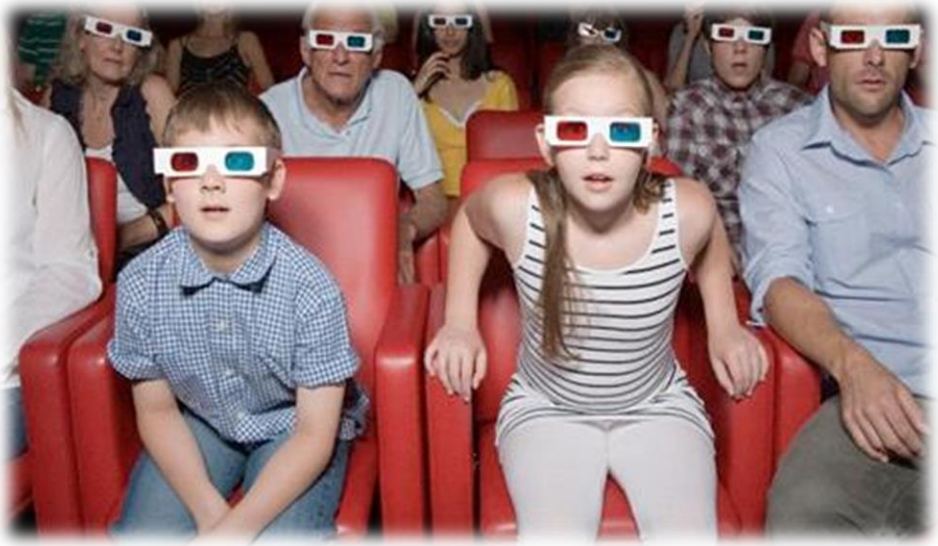
Взаимодействие компонентов.

Шаг 4. Вывод информации в UI



Видео

Пример построения карты сети в MaxPatrol X



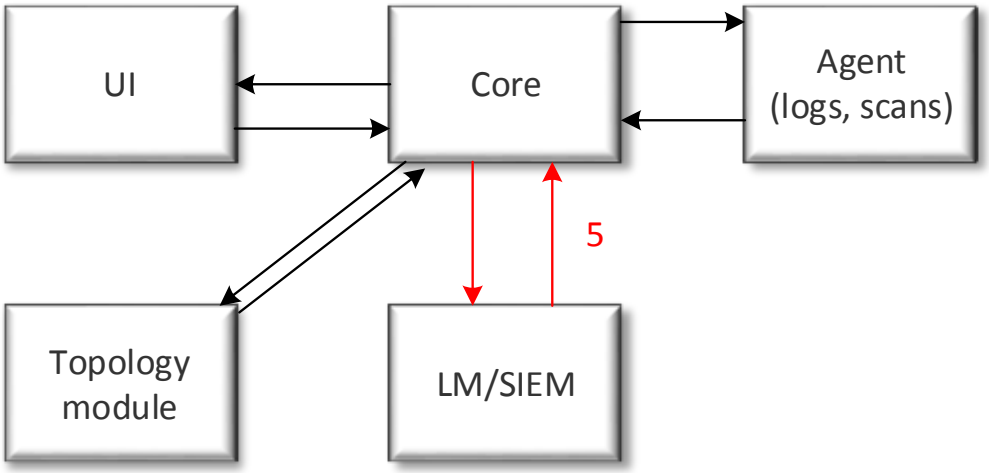
А причем же здесь SIEM?

Отвечаем. SIEM помогает нам решить несколько задач:

- Добавление/удаление устройств
- Обновление статуса сервиса
- Обновление информации о пользователях
- Изменение конфигурации
- Отображение инцидентов на карте сети

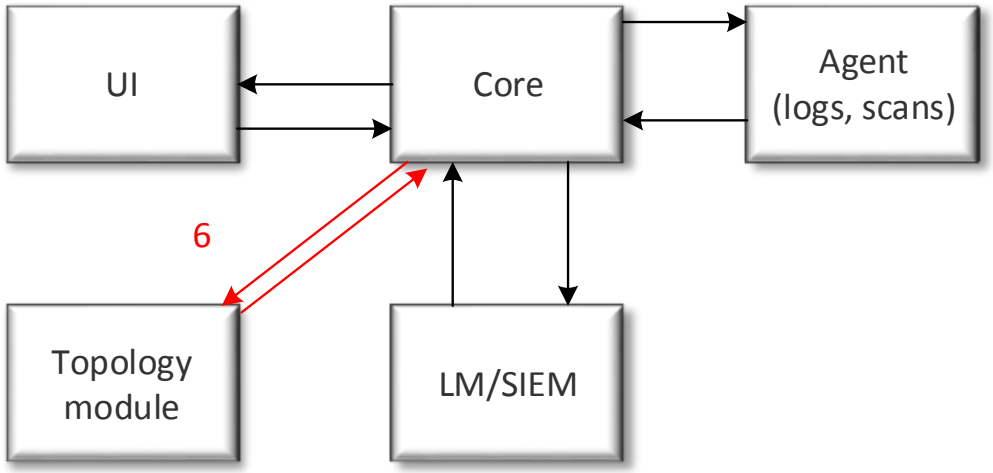
Взаимодействие компонентов.

Шаг 5. Обновление данных по событиям



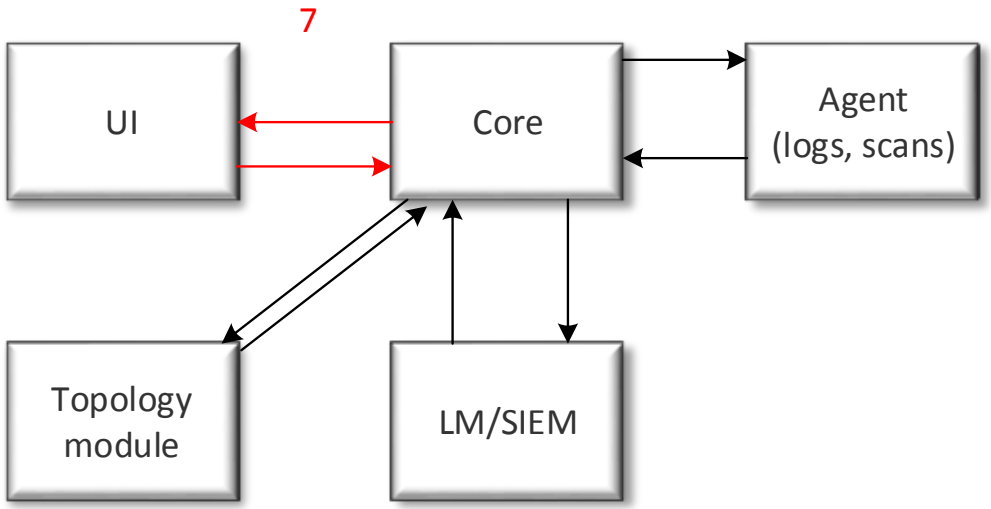
Взаимодействие компонентов.

Шаг 6. Дополнительная обработка информации.



Взаимодействие компонентов.

Шаг 7. Вывод информации в UI



Еще видео

Вопросы

Конец рассказа
Спасибо за внимание

Сергей Павлов

Директор по сетевым технологиям

Positive Technologies

spavlov@ptsecurity.com

POSITIVE TECHNOLOGIES