Использование DPI и SIEM в корпоративном мониторинге и предотвращении атак

POSITIVE TECHNOLOGIES

А вы уверены, что вашу сеть ещё не взломали?

Целями использования систем DPI и SIEM являются:

- своевременное обнаружение несанкционированных изменений
- снижение возможного ущерба от инцидентов ИБ за счет предотвращения и/или оперативного реагирования на них
- поддержка принятия обоснованных решений в области ИБ
- ретроспективный анализ инцидентов
- формирование доказательной базы при расследовании инцидентов

DPI – технология глубокого анализа сетевых пакетов и их фильтрация

Что происходит в сети?

- Какие сервисы появляются в сети
- Установлены ли обновления
- Нет ли хостов с известными уязвимостями
- Есть ли аномалии в трафике
- Какой трафик преобладает

SIEM - Security Information and Event Management

SIEM - Система, позволяющая собирать и анализировать событиями ИБ поступающие от различных устройств инфраструктуры таких как firewall, IDS, антивирусы, маршрутизаторы, VPN и т.д.

SIEM - Security Information and Event Management

SIEM – Не панацея!
Не предотвращает, а уведомляет!

Внедрение SIEM и DPI

1 этап

- Обследуется инфраструктура
- Принимается решение о способе внедрения
- Формируется ТЗ на внедрение dpi сенсора или siem
- Идёт обсуждение и обоснование необходимости, утверждение ТЗ
- Назначается ответственный и сроки исполнения

Внедрение SIEM и DPI

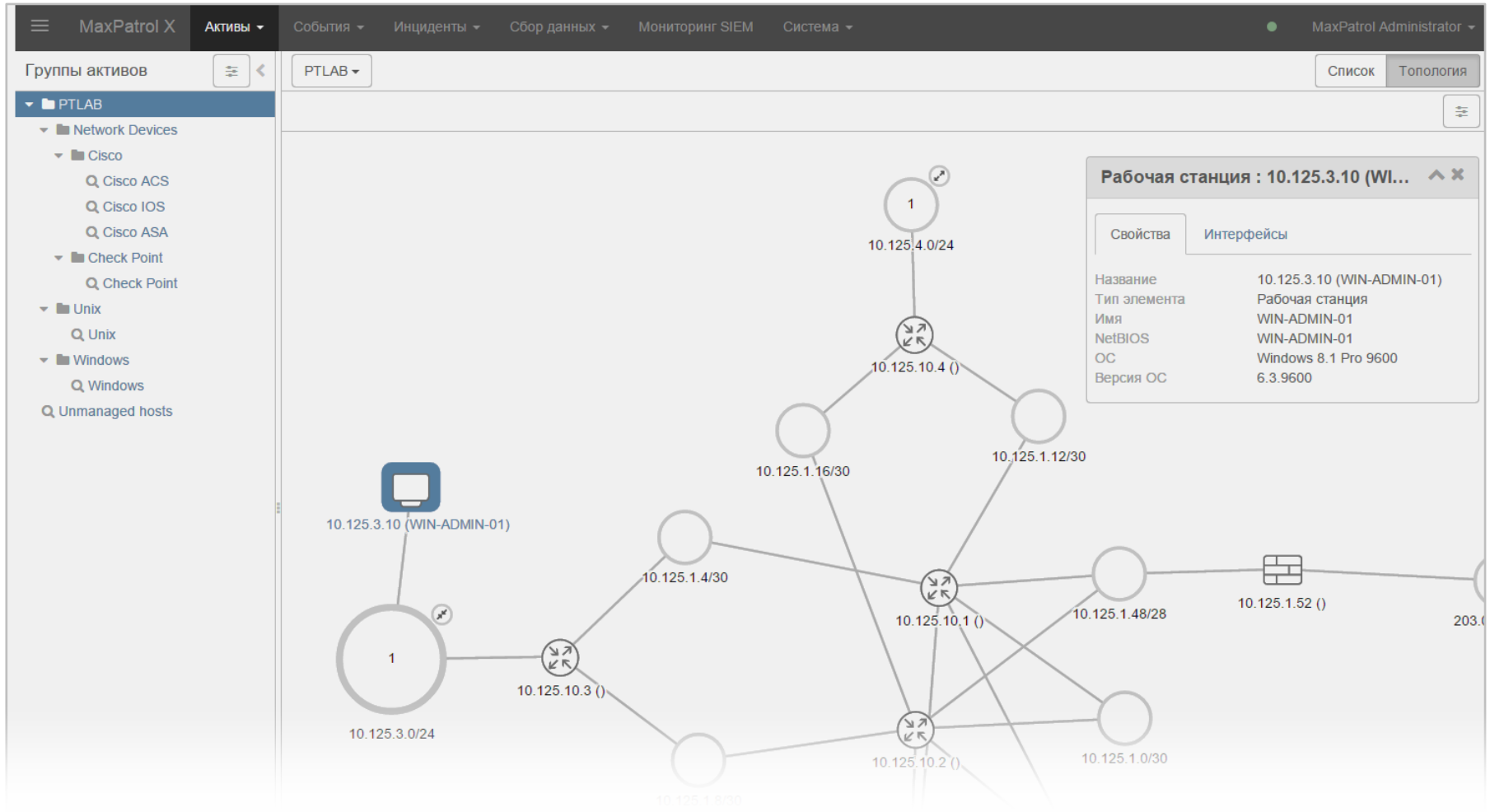
2 этап

- Установка сервера и настройка источников
- Написание корреляционных правил под вашу инфраструктуру
- Использование системы в тестовом режиме
- Использование готового сервиса

В первый раз!

- Зачем? Почему? Куда?
- Противостояние
- Споры и ограничения

На примере MP SIEM + PT Network Attack Discovery

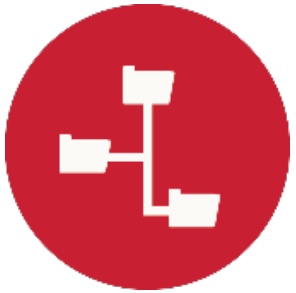


- Наглядное взаимодействие
- Группировки по определённым признакам

Автоматизация

Уведомления

Инциденты



Многоуровневые корреляции

Ретроспективный анализ

Сбор данных

Мониторинг

Спасибо!

POSITIVE TECHNOLOGIES