www.ssecline.com

Стетоскоп

Актуальные проблемы информационной безопасности

- Кибератаки на активы предприятия
- Доверие к персоналу
- Анонимность трафика
- Расследование инцидентов ИБ
- Соответствие требованиям законов
- Сложность сбора доказательной базы

Финансовый ущерб

- Статистика за 2015-2016 год
  - Рост количества вредоносного ПО составил более 60%*
  - Совокупный ущерб от кибератак в России составил 550-600 млрд. рублей**;
  - Ущерб, наносимый организациям вследствие DDoS-атак, в среднем равен $40 тысячам в час***

*Check Point, **Сбербанк, ***Incapsula

Решение Стетоскоп

- Максимальный контроль сетевого трафика
  - Возможность полного сохранения трафика
  - Сохранение расшифрованного трафика (SSL/TLS)
  - Индексация и классификация трафика
  - Контекстный анализ трафика
  - Обработка трафика в реальном времени
  - Ретроспективный анализ контента
  - Блокировка подозрительного контента
  - Экспорт расшифрованного трафика
  - Гибкая система отчетов и оповещений

Основные возможности

- Сохранение всего сетевого потока, включая расшифрованные соединения SSL/TLS, с возможностью экспорта (pcap)
- Индексация и классификация трафика по различным параметрам (адресам, протоколам, контенту)
- Контекстный анализ по требуемым параметрам
- Блокирование нежелательного трафика в реальном времени (утечки, WEB-серфинг, атаки)
- Перенаправление расшифрованного трафика на внешние анализаторы (offline/online)
- Управление событиями: задание порогов трафика, статистических эталонов взаимодействия, фильтров оповещений оператора
- Гибкая система отчетов: от сообщений пользователя и статистики до сетевых пакетов

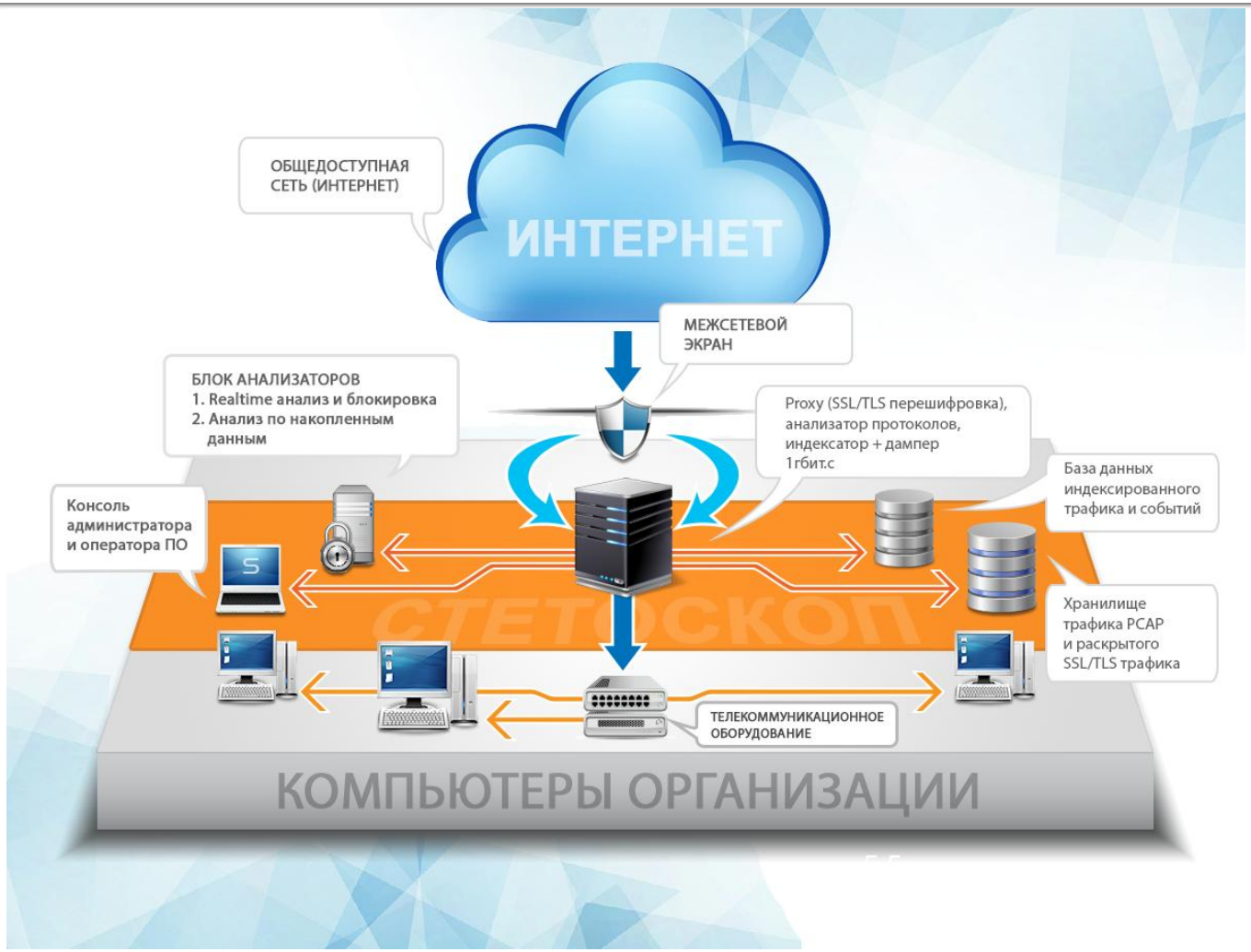
Назначение программы

- Расследование инцидентов и сбор доказательной базы
- Визуальное и автоматизированное выявление сетевых аномалий: Scan, DDoS, Bruteforce, подозрительная сетевая активность, отказ сетевого оборудования
- Анализ контента и блокировка по заданным сигнатурам
  - Анализ содержимого передаваемых данных: почта, WEB, сервисы обмена сообщениями
  - Гибкая система фильтрации сетевых потоков
- Интеграция с внешними СЗИ
  - Перенаправление расшифрованного трафика на внешние анализаторы
  - Интеграция с внешними системами обработки – SIEM

Технические характеристики

	Малый	Средний	Enterprise
Скорость канала	10 Мб/с	100 Мб/с	1 Гб/с
Количество сессий в сек	<5000	<20000	<100000
Количество пользователей	<30	<100	<10000
Форм-фактор	PC,1U	PC,1U-2U	2U-4U
Время хранения (дней)	100 (10ТБ)	50 (50ТБ)	30 (300ТБ)

Схема подключения



Экономическое обоснование Конкурентные преимущества

- Простая процедура развертывания/внедрения, не требующая дополнительного оборудования и свойств оборудования от клиента
- Управление на уровне простого пользователя
- Для каналов до 1 Гбит/с не требует дорогого серверного оборудования
- Уникальный функционал: алгоритмы выявления, плагинная система расширения возможностей по аналитике (плагины пользователей и собственной разработки, доступные на маркете собственной площадки).
- Сделано в России (Импортозамещение)
- Возможность внедрения в государственные органы (лицензирование, сертификация по требования нормативной базы РФ в области защиты информации)

Текущее состояние и планы

- Реализована однопользовательская версия Стетоскопа по записи и индексации сетевого трафика, включая расшифрованный трафик SSL/TLS;
- Тестируется шлюзовая версия Стетоскопа по записи и индексации сетевого трафика;
- В разработке DPI-модули анализа протоколов прикладного уровня: WEB, почта, сервисы сообщений;
- Планируется enterprise версия, позволяющая проводить DPI-анализ трафика в каналах связи на скорости до 1 Гбит/с.

SSECLINE

www.ssecline.com