Практика решения задачи анализа сетевого трафика на примере одного заказчика

Сергей Сурков
sergey.surkov@microolap.ru
+7 (929) 927 3642

Микроолап Текнолоджис

- Черноголовка, Московская область
- Анализ сетевого трафика и смежные задачи – с 1997 года

Задача: кто использует торренты?

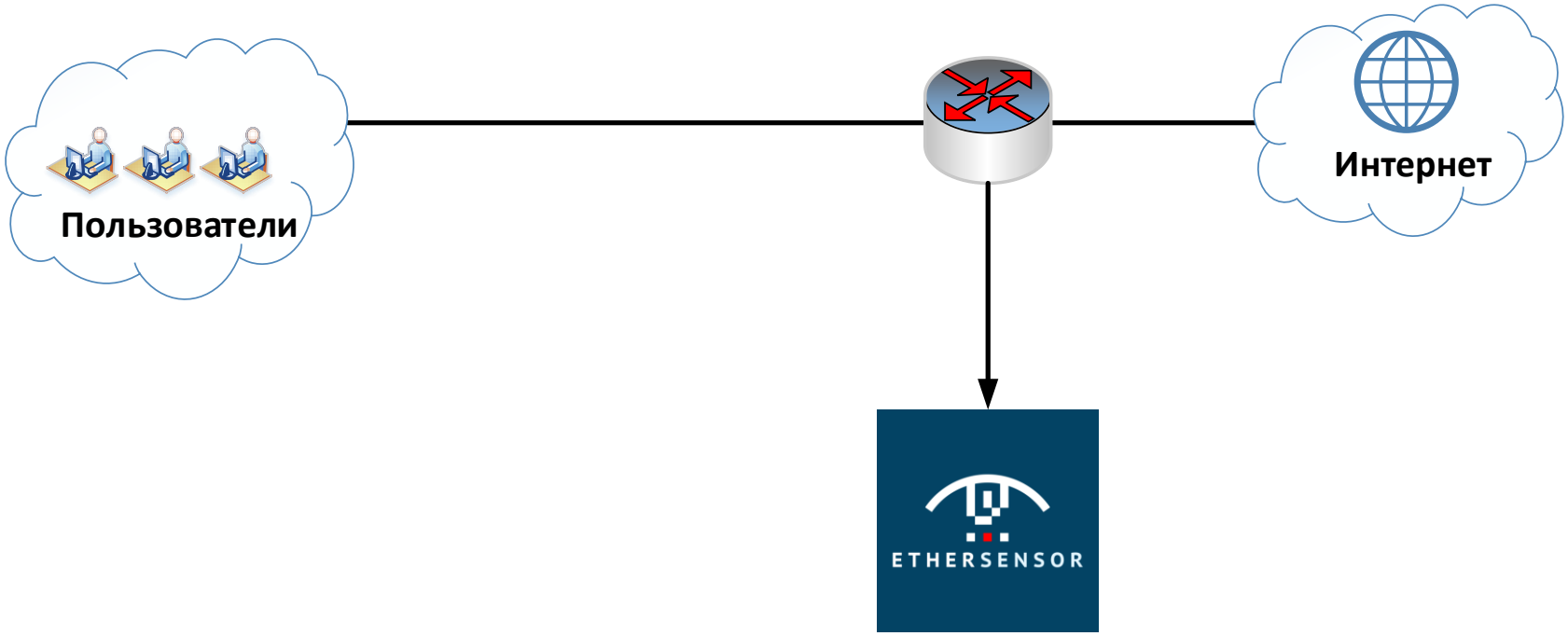
Директор по ИБ

EtherSensor – программная платформа анализа трафика

Принцип работы:

- **Получает** копию сетевого трафика (Mirror-порт, ICAP(S), интеграционные источники) в режиме реального времени
- **Извлекает** сообщения (электронная почта, веб-почта, соц. сети, мессенджеры, файлы), метаданные, сетевые события
- **Анализирует**:
  - Пользовательские сообщения (текст)
  - Файлы (имя, тип, размер, хеш)
  - События (аутентификация, различные сетевые действия)
  - Метаданные (адресаты, IP, хосты)
- **Отправляет** результаты системам-потребителям

EtherSensor



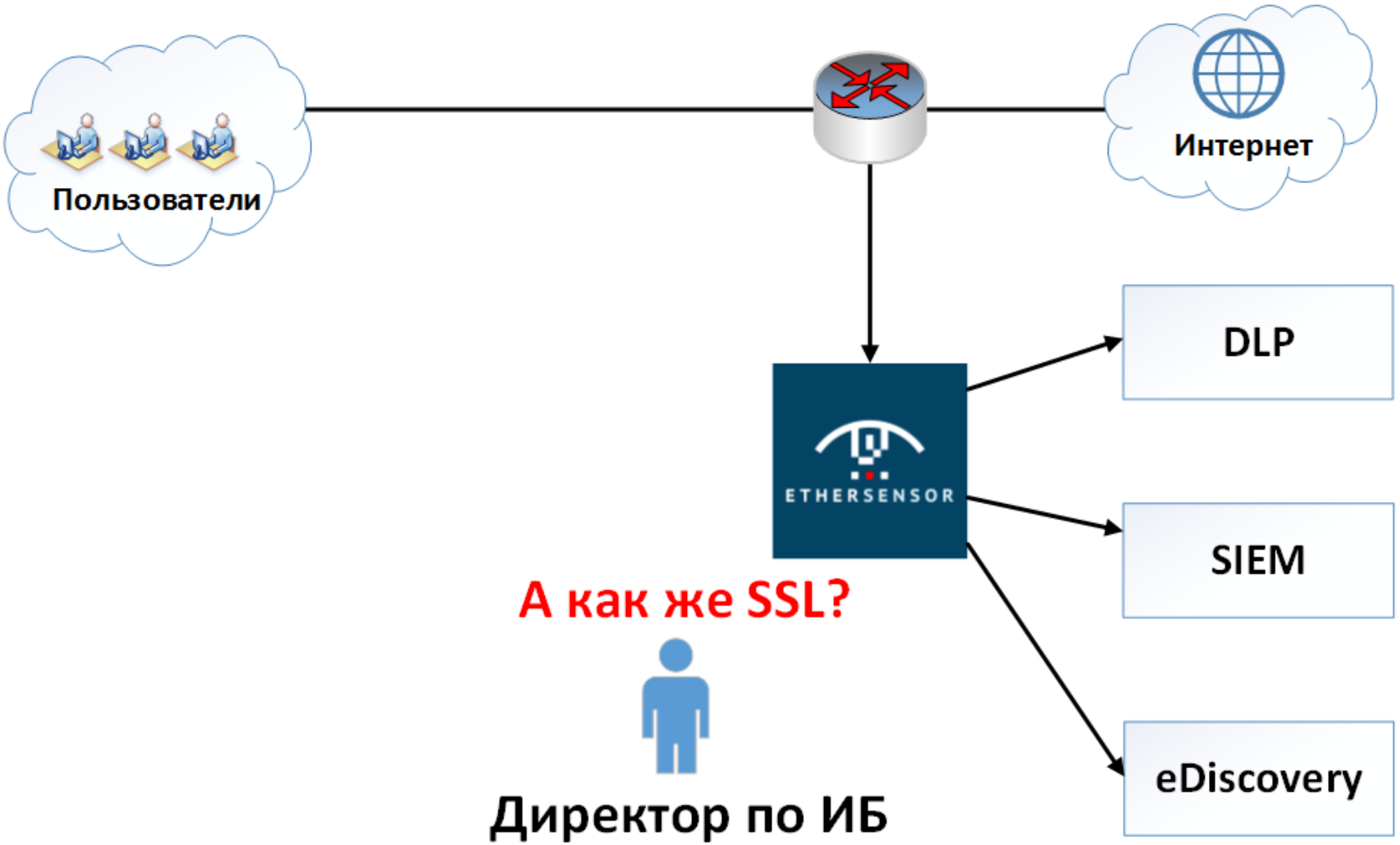
Интеграция..?

Директор по ИБ

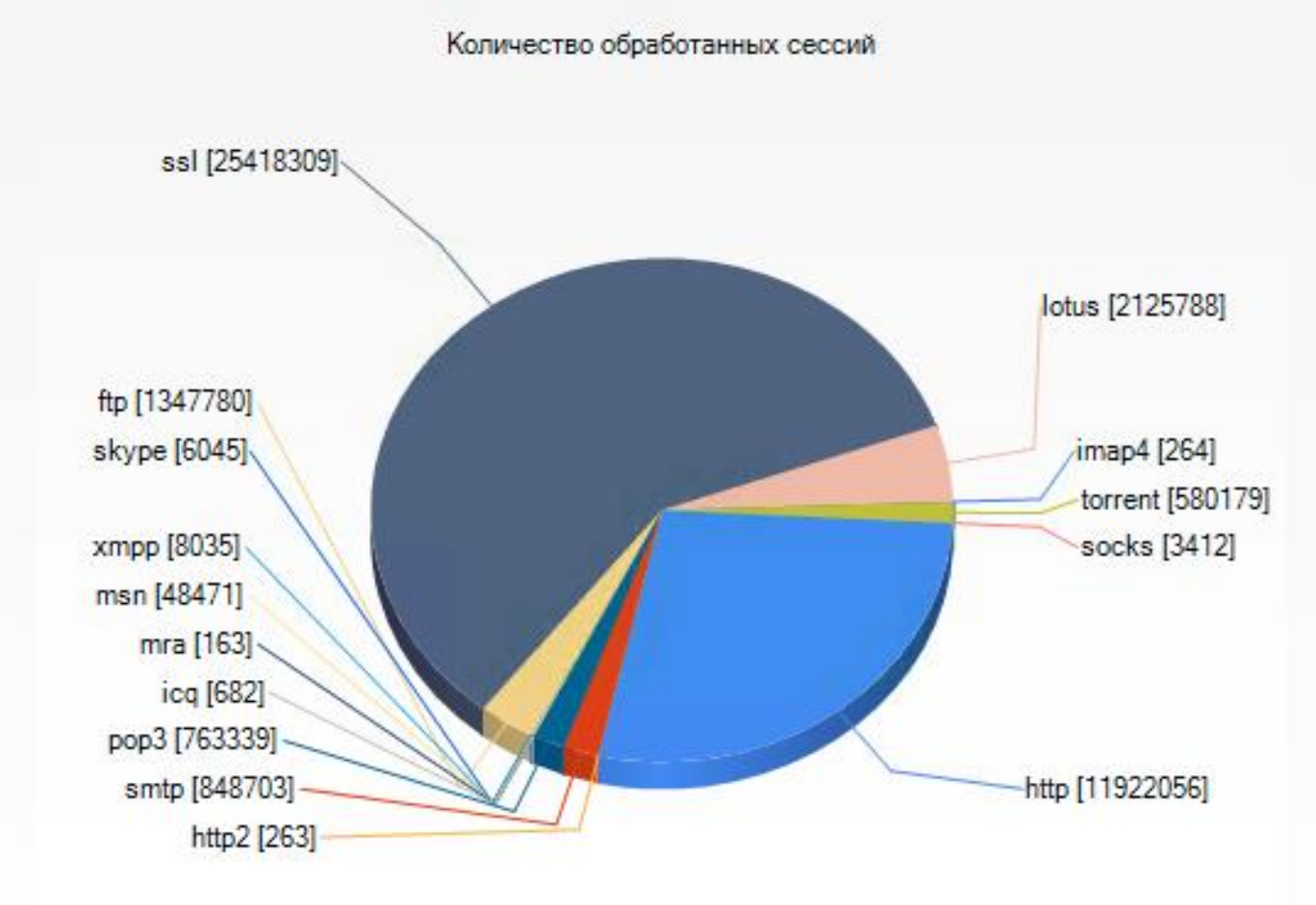
EtherSensor – потребители

- **DLP** – высокоуровневый анализ пользовательских событий, сообщений, файлов, метаданных
- **SIEM** – низкоуровневый анализ и корреляция сетевых событий пользователей и систем
- **eDiscovery** – архив корпоративных коммуникаций
- **U(E)BA** (User (and Entity) Behavior Analytics) – информация о сетевых соединениях и других событиях пользователей, данные для поведенческого анализа

EtherSensor



SSL-трафик – 50-75% от всего трафика



SSLSplitter

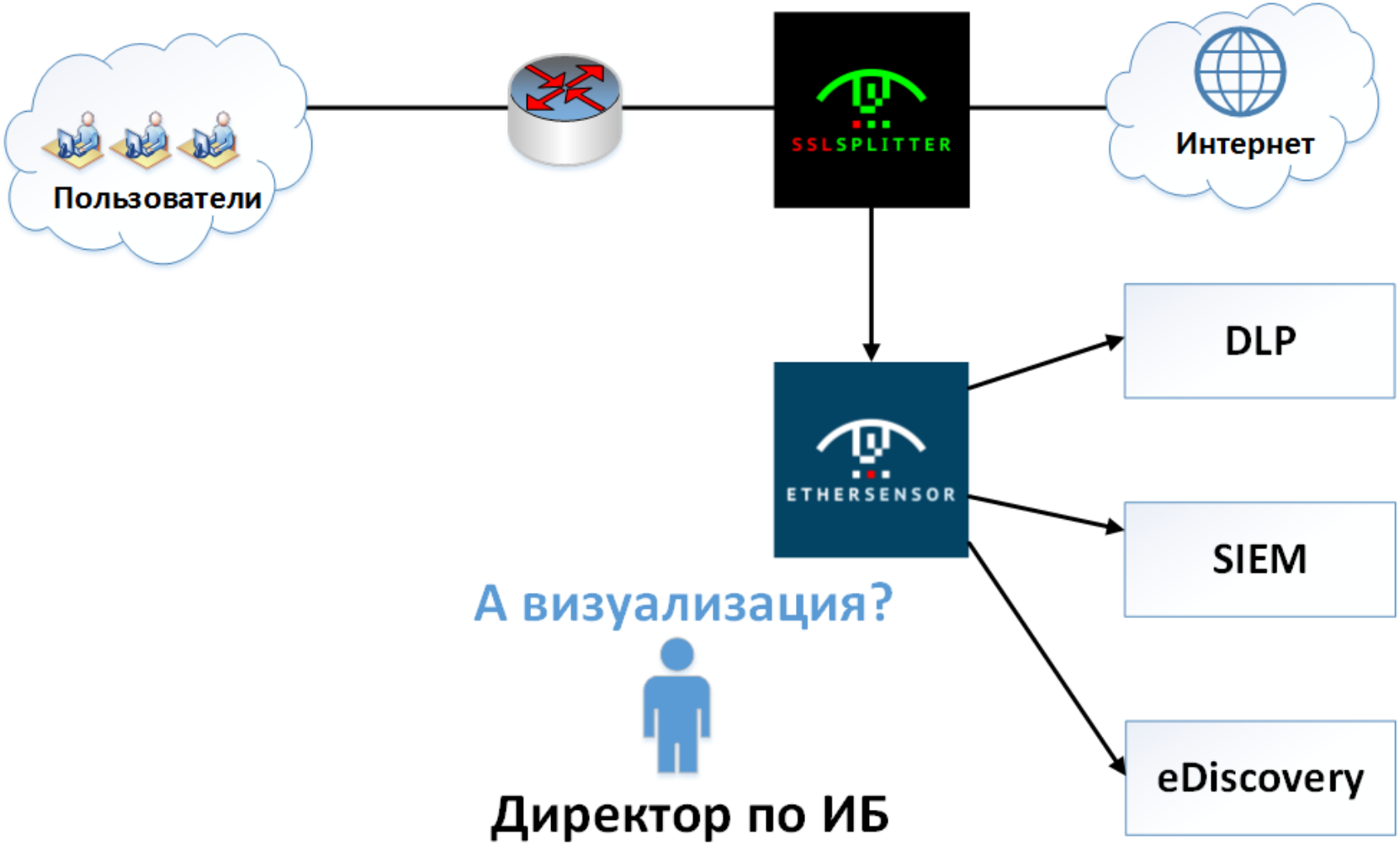
Описание:

Программное MITM-решение, расшифровывает SSL-соединения, отдает данные в Mirror-интерфейсы, подключенные к **EtherSensor**

Отличия от других решений:

- Не нужно платить за навязанный функционал (VPN, FW, DHCP, и т.д.)
- Не только HTTPS и FTPS, а все протоколы Over SSL
- Отечественный производитель
- Функционирует в режимах L2 (bridge) и L3 (router)
- Проще в обслуживании

SSLSplitter



EtherStat – анализ сетевой статистики

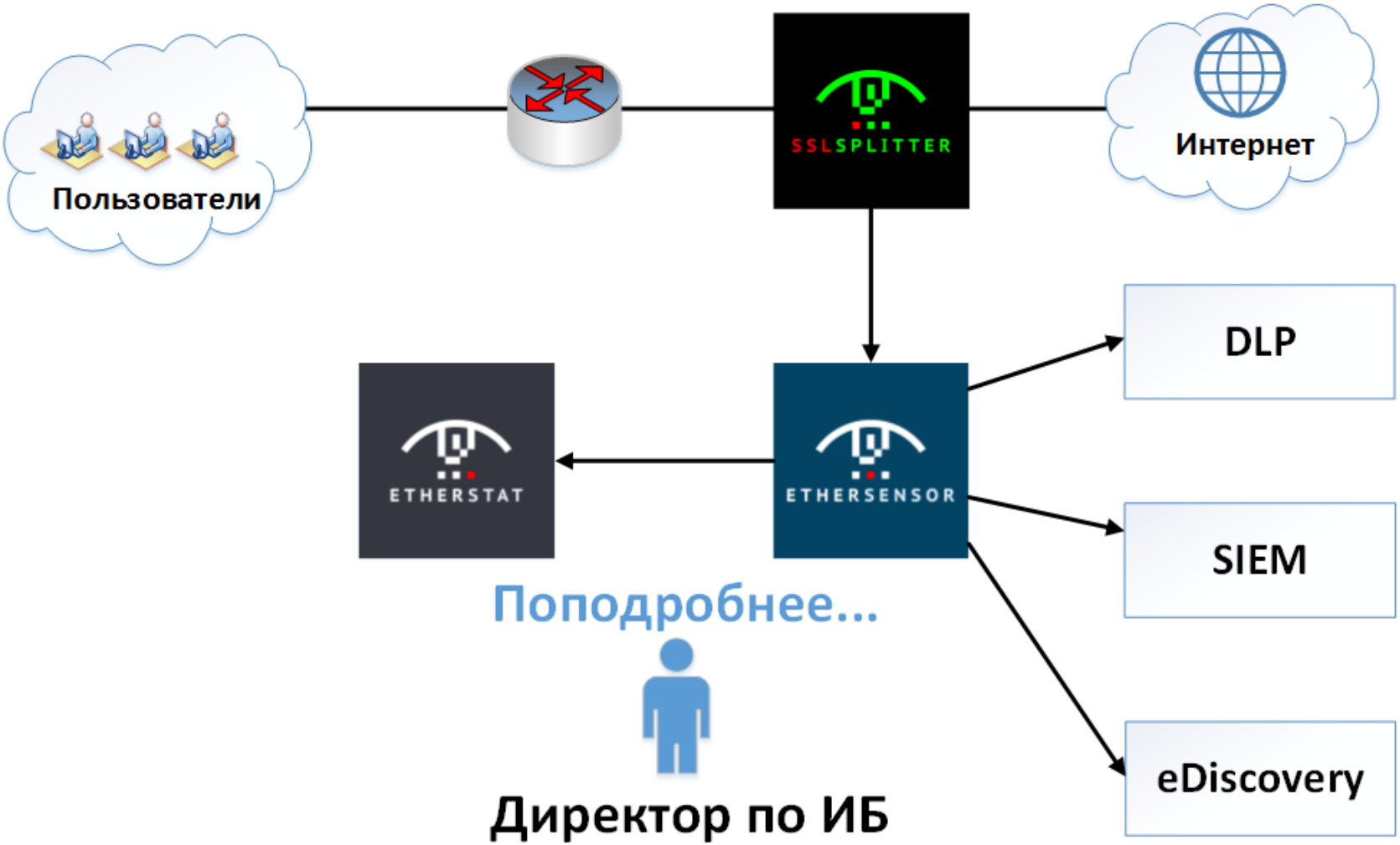
Описание:

Программная система хранения и анализа статистики, генерируемой платформой **EtherSensor**

Возможности:

- Мониторинг сетевой активности, в online и в ретроспективе
- Привязка сетевого трафика к конкретным пользователям и их устройствам
- Выявление нехороших действий в сети
- Предоставление дополнительной информации о событиях
- Формирование отчетов о сетевых событиях

EtherStat



EtherStat

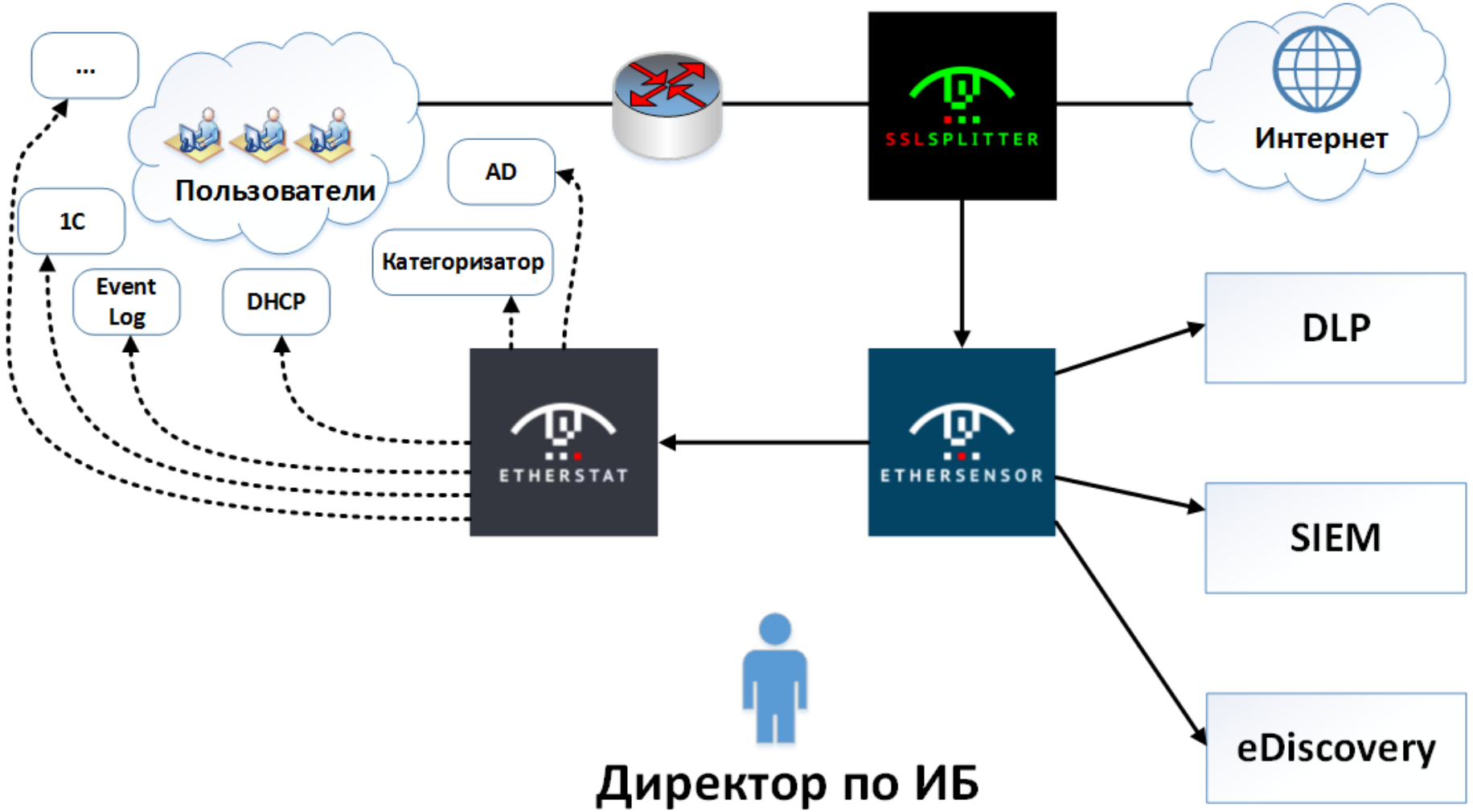
Принцип работы:

1. Получает статистику о TCP-соединениях, веб-запросах и поисковых запросах пользователей
2. Сохраняет данные в БД
3. Определяет устройство и пользователя, сгенерировавших трафик
4. На основании полученных данных строятся различные отчеты, позволяющие определить сетевую активность пользователей и их устройств
5. Интегрируется со сторонними системами для получения дополнительной информации о событиях

EtherStat

- Получение данных из смежных систем
  - AD
  - DHCP
  - Event Log
  - 1С – дополнение данных из AD
  - Категоризаторы интернет-трафика
  - Другие системы…
- Обогащение статистики
- Привязка к пользователю

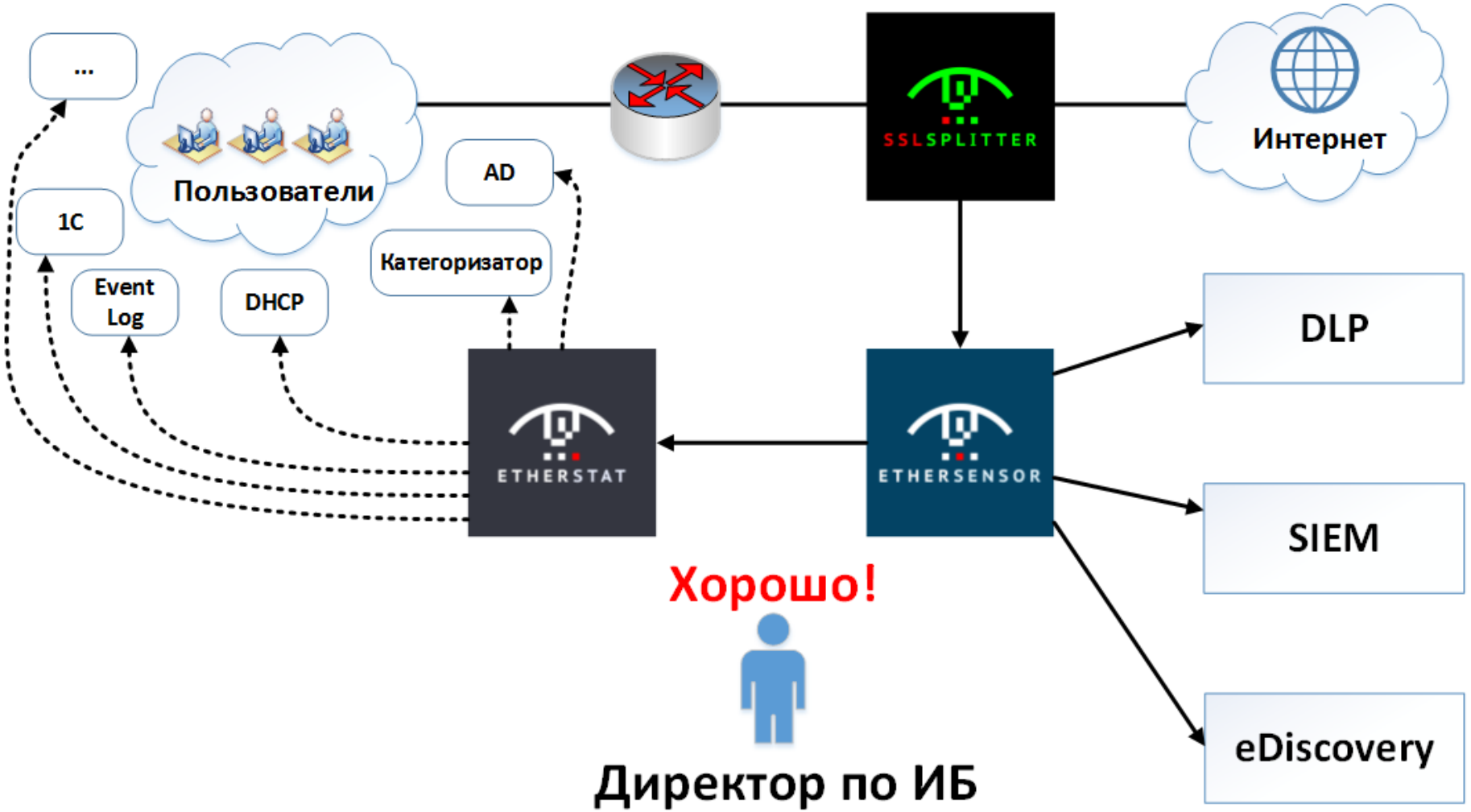
EtherStat



EtherStat – отчеты

- По сетевым соединениям
- По URL-запросам, категориям интернет-сервисов
- Новые устройства в сети
- Хосты, с которых работает множество пользователей
- По изменениям в Active Directory
- Анализ поисковых запросов пользователей

EtherStat



Решенные задачи

- Анализ сетевого трафика
- Выявления утечек
- Вскрытие SSL
- Визуализация сетевой активности
- Анализ аномалий
- Отчёты: оперативные и для руководства

Спасибо!

Будем рады Вашим вопросам!

info@microolap.ru

+7 (495) 748 8105

Сергей Сурков

sergey.surkov@microolap.ru

+7 (929) 927 3642