Профилирование активности пользователей в Splunk Enterprise

Построение профиля пользователя на примере данных веб-прокси

VolgaBlob

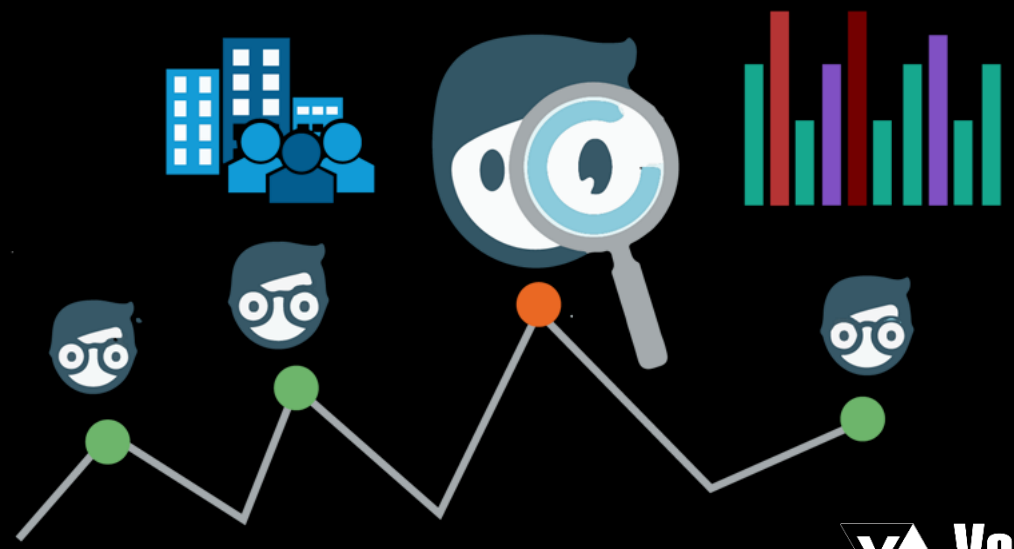
Об этом мастер-классе

- Принципы построения профилей в Splunk
- Реализация простого профиля пользователя
- Примеры использования профилей для анализа поведения
- Применяемые технологии:
  - чистый SPL

https://www.gotomeet.me/vbtrend-profiling

Профиль пользователя

- Набор параметров активности пользователя
- Содержит количественные и качественные характеристики
- Автоматически поддерживается системой в актуальном состоянии



Демонстрационный пример

- Используются данные от веб-прокси Cisco WSA
- Для каждого пользователя, строится профиль со следующими параметрами:
  1. Перечень посещенных сайтов
  2. Средний объем трафика за сутки
  3. Среднее кол-во запросов за сутки (с разбивкой по дням недели)

Профили пользователей в Splunk

1. Коллекция KV Store для хранения актуального профиля
2. Набор поисковых запросов для расчета параметров профиля
3. Поисковый запрос для сохранения истории профилирования

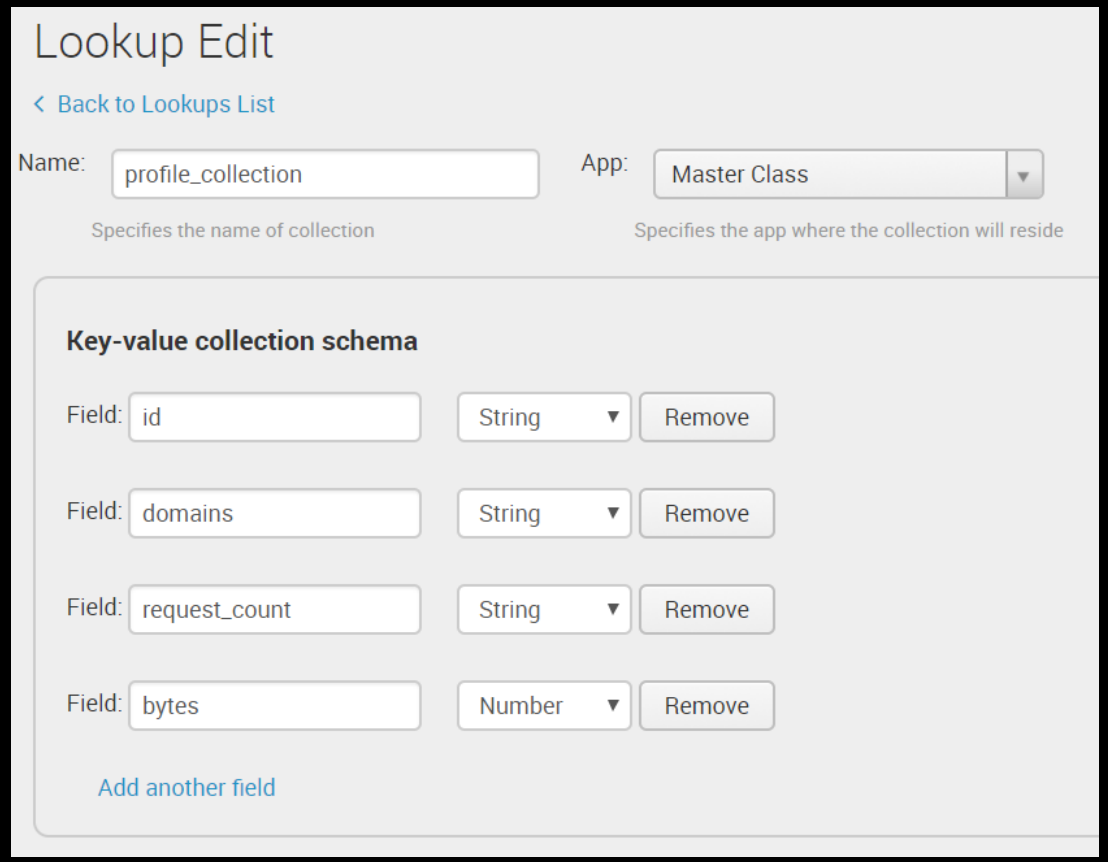
KV Store

Collections
контейнеры для объектов, существуют в контексте приложения

Records
конкретная запись, похожи на строки в реляционных БД

Fields
поля записи, похожи на столбцы в реляционных БД

Приложение Lookup Editor



Файл collections.conf

```
[profile_collection]
field.bytes = number
field.domains = string
field.id = string
field.request_count = string
replicate = true
```

Поисковые команды и KV Store

- inputlookup – получение данных из KV Store в качестве результата выполнения поиска
- outputlookup – запись результатов поискового запроса в коллекцию
- lookup – обогащение результатов поиска полями из KV Store

Примеры использования команд

- Записать данные в KV Store с обновлением

```
| outputlookup append=true profile_lookup
```

- Получить из KV Store записи с полем id="user@domain.com"

```
| inputlookup profile_lookup where id="user@domain.com"
```

- Загрузить из KV Store поле domains

```
| lookup profile_lookup id OUTPUT domains as domains_profile
```

Расчет параметров профиля

```
index=main sourcetype="cisco:wsa:squid" dest!="-"
| stats values(dest) as domains by user

| rename user as id
| lookup profile_lookup id OUTPUT domains as domains_profile
| eval domains = mvdedup(mvappend(domains, domains_profile))
| fields - domains_profile

| lookup profile_lookup id OUTPUTNEW
| outputlookup append=true profile_lookup
```

1. Расчет текущего значения параметра
2. Обновление сохраненного в профиле параметра
3. Обновление записи пользователя в профиле

История профилирования

```
| inputlookup profile_lookup
| table id, bytes, request_count, domains

| eval request_count = mvjoin(request_count, "| ")
| eval domains = mvjoin(domains, "| ")
| eval _time = now()

| collect testmode=true addtime=true index=profile_history
sourcetype=profile_history
```

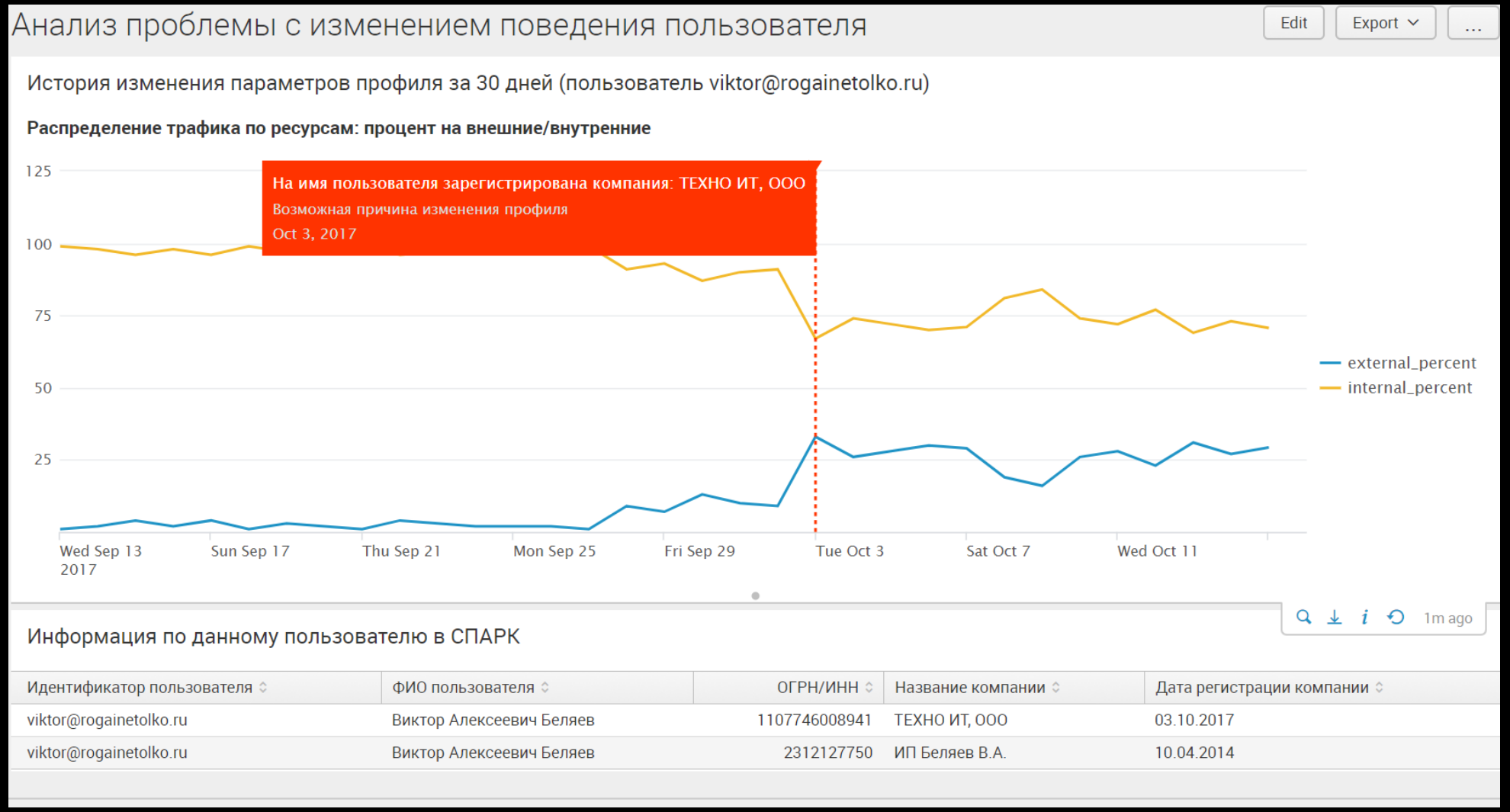
Загрузить из KV Store текущий профиль

Преобразовать данные в подходящий для записи формат

Сохранить в индекс с историей профилирования

Пример использования профиля

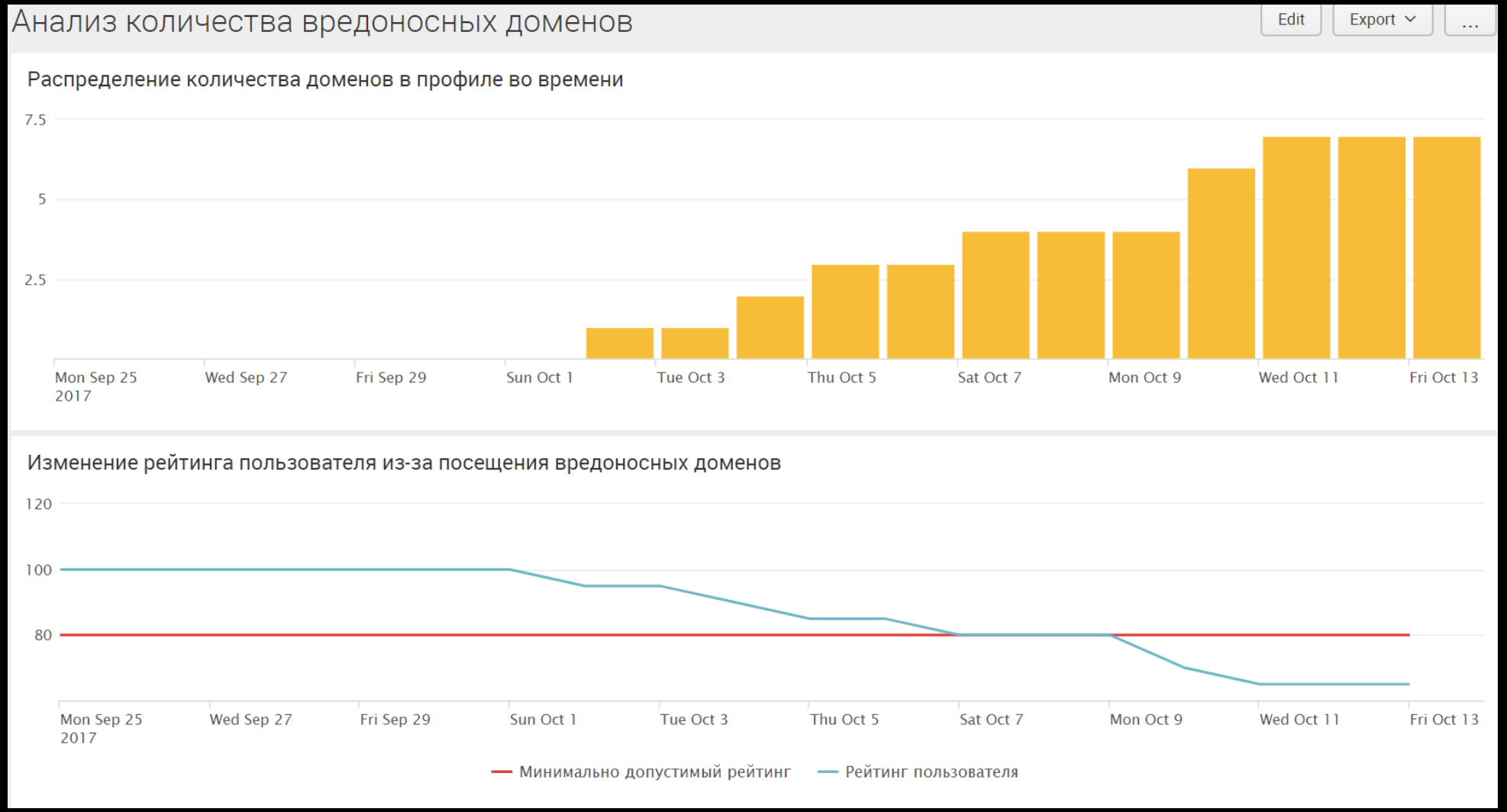
Комплексная аналитика: профилирование + внешние источники



Идентификатор пользователя	ФИО пользователя	ОГРН/ИНН	Название компании	Дата регистрации компании
viktor@rogainetolko.ru	Виктор Алексеевич Беляев	1107746008941	ТЕХНО ИТ, ООО	03.10.2017
viktor@rogainetolko.ru	Виктор Алексеевич Беляев	2312127750	ИП Беляев В.А.	10.04.2014

Пример использования профиля

Влияние параметра профиля на рейтинг пользователя



Спасибо за внимание!

VolgaBlob