

Комплекс программных продуктов Microolap для анализа сетевого трафика

Сергей Сурков

ss@microolap.ru

+7 (929) 927 3642

Распространенные задачи

- Анализ сетевого трафика в системах ИБ различных классов
- Повышение эффективности выявления утечек конфиденциальной информации
- Вскрытие SSL-трафика
- Визуализация сетевой статистики
- Анализ сетевых аномалий
- Построение аналитических отчетов

Где используется анализ сетевого трафика

SIEM

- HP ArcSight
- Splunk
- IBM QRadar
- McAfee ESM
- RSA ESM

DLP

- InfoWatch TM
- DeviceLock DLP
- Symantec DLP
- Solar Dozor
- SearchInform



Enterprise Archiving

- Symantec EV
- MailArchiva
- Enterprise Search

Anomaly Detection

- Prelert
- SQLStream
- Twitter Anomaly Detection

EtherSensor – программная платформа анализа трафика



Принцип работы:

- **Получает** копию сетевого трафика (Mirror-порт, ICAP(S), интеграционные источники) в режиме реального времени
- **Извлекает** сообщения, 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

Потребители

- **DLP – высокоуровневый анализ пользовательских событий, таких как сообщения, файлы, и другие события**
- **SIEM - низкоуровневый анализ и корреляция сетевых событий пользователей и систем**
- **eDiscovery – архивы для хранения различных данных, такие как электронная переписка, сетевые события и т.д.**
- **UEBA/UBA (User and Entity Behavior Analytics/User Behavior Analytics) – информация о сетевых соединениях и других событиях пользователей**
- **Anomaly Detection**

Извлекаемые данные

Веб-почта, социальные сети, форумы

- Gmail, Mail.ru, Yandex, Yahoo, Live.com, Facebook, VK, Odnoklassniki, Сервисы поиска работы – **СОТНИ сервисов**

Информация

- Аутентификация, регистрация
- Отправляемые сообщения и вложения
- Чтение входящих сообщений
- Списки контактов

Извлекаемые данные

Электронная почта

- Протоколы SMTP(S), POP3(S), IMAP4(S)
- Сообщения IBM Lotus Notes/Domino
- Microsoft OWA (Outlook Web Access)

Серверы электронной почты могут быть как корпоративными, так и внешними

Извлекаемые данные

Сервисы мгновенных сообщений - IM, SMS/MMS

- XMPP - Google Talk/Hangout, Yahoo ...
- Microsoft Skype for Business (Lync)
- MRA - Mail.Ru Агент
- OSCAR – ICQ ...
- Сервисы отправки SMS/MMS сообщений

- Обычный **Skype**
 - Без агентов, на канале

Информация

- Сообщения
- Контакт-листы
- Файлы, документы

Извлекаемые данные

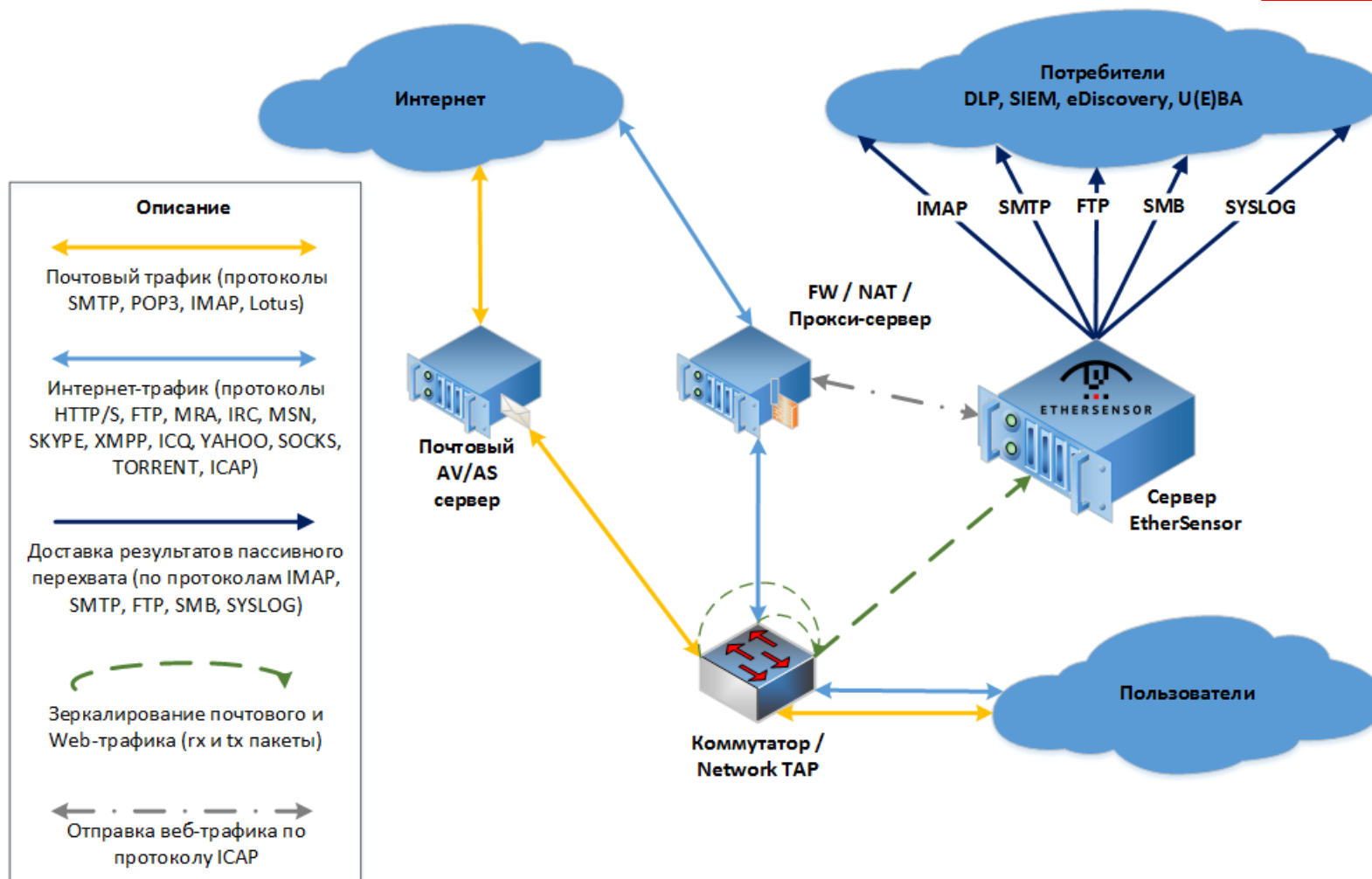
Отправка/загрузка файлов

- Через веб-браузер - HTTP(S)
- Сервис мгновенных сообщений
- Протоколов FTP(S), WebDAV(S)

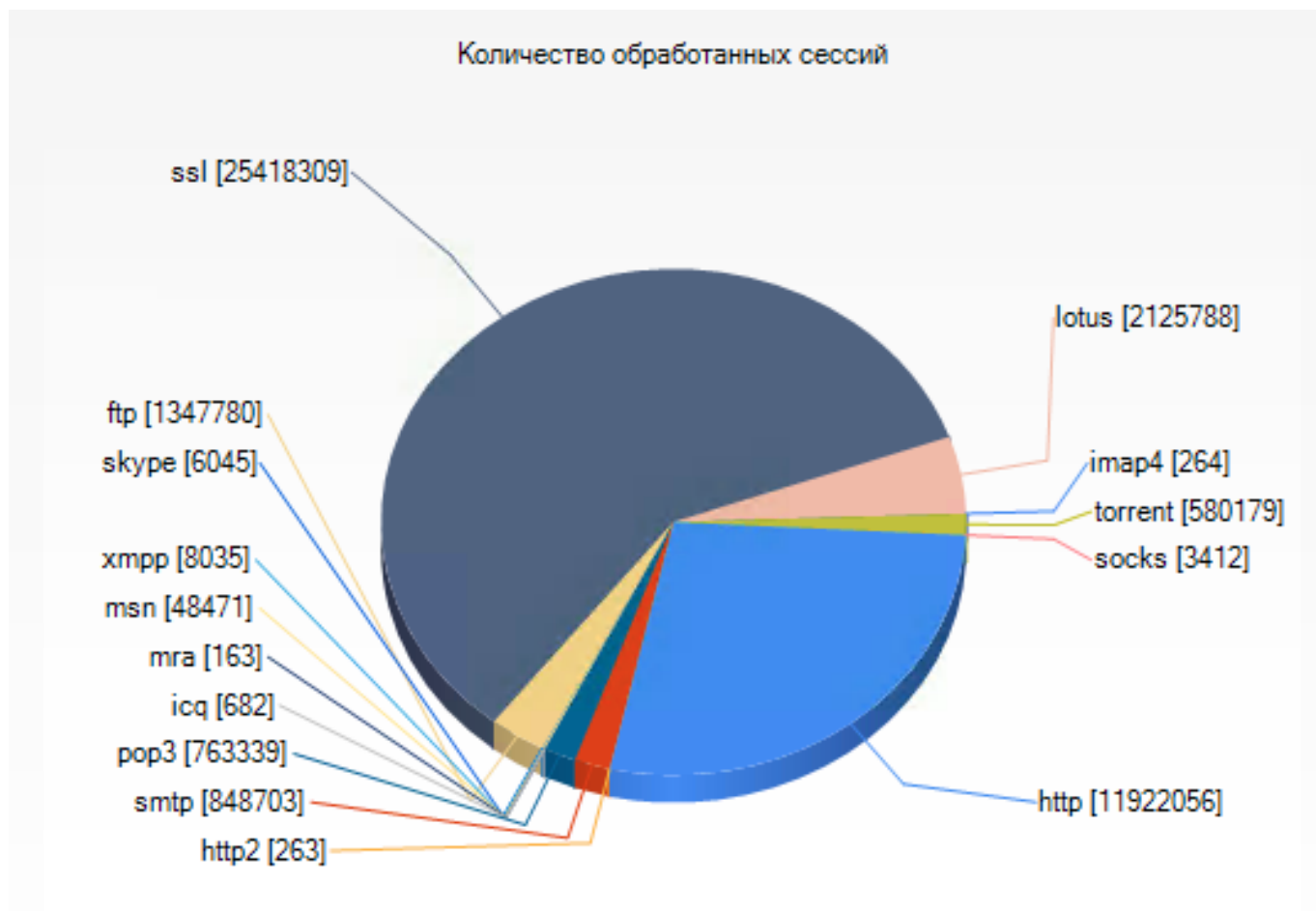
Поисковые запросы

- Google
- Yandex
- Yahoo
- Rambler
- Bing
- Wikipedia.org...

Схема интеграции



В среднем SSL-трафик составляет от 50% до 75%



SSLSplitter

Описание:

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

Отличия от других решений:

- Не нужно платить за неиспользуемый функционал (VPN, FW, DHCP, и т.д.)
- Не только HTTPS и FTPS, а все протоколы Over SSL
- Поддержка шифрования ГОСТ
- Поддержка TLS 1.3
- Функционирует в режимах L2 (bridge) и L3 (router)
- Проще в обслуживании

SSLSplitter

Возвращает ИБ контроль над ситуацией в организации:

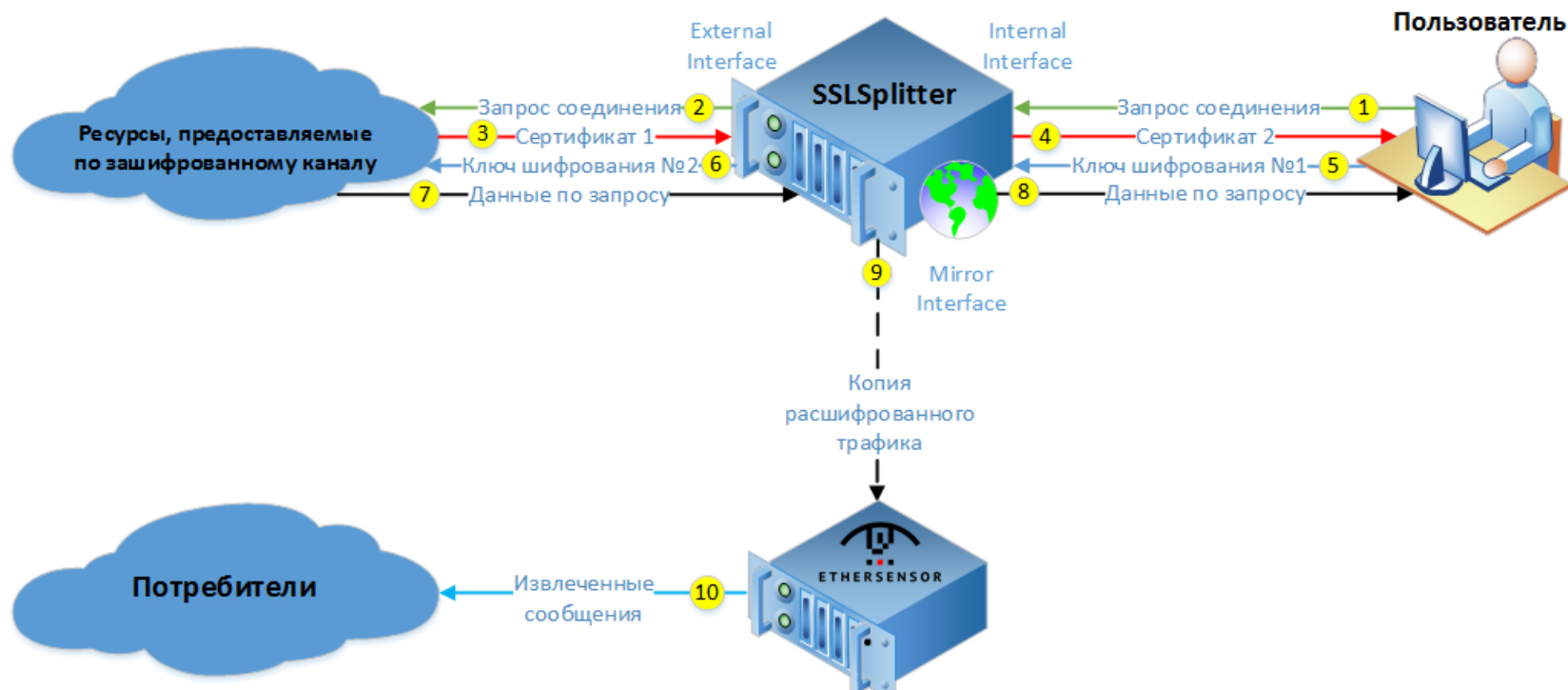
- Интернет-трафик, мессенджеры, веб-почта, соц. сети, передача файлов, сетевые события и т.д.

Новые возможности анализа:

- детектирование VPN
- Skype на канале
- облачные хранилища
- SIP
- детекторы сервисов удаленного управления

Схема работы SSLSplitter

Расшифровка зашифрованного трафика
 (протоколы: HTTPS, MRAS, ICQS, SMTPS, POP3S, IMAP4S, XMPPS, FTPS, WebDAV/SSL,
 HTTP/2, RTMP и т.д.)



EtherStat



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

Основное назначение системы – хранение, обработка, анализ и построение отчетности о деятельности пользователей в корпоративной сети.

EtherStat



Возможности:

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

Позволяет строить отчеты следующих типов:

- топ самых активных пользователей
- топ посещаемых веб-доменов с возможностью углубления до конкретных веб-сервисов
- разбивка сетевого трафика по категориям (при интеграции с категоризатором)
- новые устройства в сети за период
- хосты, с которых работает множество пользователей (помогает находить в сети несанкционированно установленные коммутаторы и Wi-Fi точки доступа)
- история изменений в Active Directory
- проблемы в структуре Active Directory
- поиск по тексту поисковых запросов
- поиск по посещаемым URL (помогает осуществить отслеживание прохождения документов в сети Интернет при поиске инсайдеров)

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

Обогащение данных:

- Active Directory
- DHCP-журналы
- Windows Logs (Security)
- Категоризаторы (Entensys, SimilarWeb, ...)

В будущей версии (июнь 2017):

- Внешние источники (IBM X-Force Exchange)
- NMAP-сканирование сети
- Агенты Microolap

Скриншоты

EtherSensor:

Источники данных

 **Сетевые адаптеры**
Настройка перехвата трафика с сетевых адаптеров.

Параметры сетевых адаптеров

- Сетевые адаптеры
 - Bluetooth Device (Personal Area Network)
 - Intel(R) 82579LM Gigabit Network Connection
 - Intel(R) Centrino(R) Ultimate-N 6300 AGN
 - Microsoft Wi-Fi Direct Virtual Adapter
 - Microsoft Hosted Network Virtual Adapter
 - VMware Virtual Ethernet Adapter for VMnet1
 - MAC адрес
 - Описание
 - Комментарий
 - Прослушивать ☒
 - Считать контрольные суммы IP пакетов ☒
 - Считать контрольные суммы TCP пакетов ☒
 - Размер очереди ожидаемых пакетов 64
 - Фильтр
 - default: Не используется
 - Протоколы
 - [DC; FTP; HTTP; ICAP; ICQ; IMAP4; IRC; LOTUS; MRA; MSN; POP3;
 - VMware Virtual Ethernet Adapter for VMnet8
 - Не прослушивается
 - PCAP files processing adapter
 - Прослушивается

Источники данных

- Сетевые адаптеры
- Фильтры пакетов
- ICAP сервер
- Lotus Notes Transaction Log

Прослушивать
Разрешить/Запретить прослушивание трафика на данном сетевом адаптере.

Сохранить

EtherSensor: BPF-фильтрация



Фильтры пакетов

Управление фильтрами пакетов: создание, удаление, клонирование и изменение. Фильтры пакетов используются для отклонения (игнорирования) трафика, не подлежащего дальнейшей обработке.

Фильтр

Имя	Адрес источника	Порт ист...	Адрес получателя	Порт получ...	Протокол
Фильтр ненужного трафика					
Отклонить пакеты	any	any	2001:0db8:0a0b:...	any	ip6
Принять пакеты	any	any	10.100.100.100	514	udp
Отклонить пакеты	any	any	any	any	gre
Отклонить пакеты	192.168.1.2	any	any	any	tcp
Принять пакеты	any	any	any	any	tcp

Действия

Новый объект

- Фильтр
- Группа
- Правило

Общие

- Вырезать
- Копировать
- Копировать текст
- Вставить
- Удалить
- Свойства

Настройка

↑ ↓

Принять пакеты

- Адрес источника [any : any]
- Адрес получателя [any : any]
- Протокол [TCP]

Фильтр: default

Сохранить

EtherSensor: HTTP-фильтрация



Настройка фильтров HTTP запросов

Управление файлами фильтров HTTP запросов. Создание, удаление, клонирование и изменение.

Фильтр

Имя	Состояние	Действие
Фильтр HTTP объектов		
Основная таблица		
Не обрабатывать потоковое видео	☒	Забудь
Условия		
Заголовок HTTP ответа [Content-Type] [=] [video]		
Действия		
Забудь HTTP объект		
Не обрабатывать слишком большие объекты	☒	Забудь
Условия		
Размер HTTP запроса или HTTP ответа [>=] [1G]		
Действия		
Сохранить информацию об объекте в канал [HTTPOver1G]		
Забудь HTTP объект		
Продолжить обработку	☒	Принять
Условия		
Любой запрос		
Действия		
Принять HTTP объект		

Действия

Новый объект

Фильтр

Таблица

Правило

Условие

Действие

Общие

Вырезать

Копировать

Копировать текст

Вставить

Удалить

Свойства

Настройка

↑ ↓ ⇐ ⇒ (…)

Не обрабатывать потоковое видео

Условия:

- Заголовок HTTP ответа [Content-Type] [=] [video]

Действия:

- Забудь HTTP объект

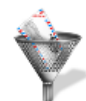
Фильтр

2015-08-28-rgs.HTTP.xml

Использовать

Сохранить

EtherSensor: Фильтры сообщений



Настройка фильтров сообщений

Управление файлами фильтров сообщений: создание, удаление, клонирование и изменение.

Фильтр

Имя	Состояние	Действие
Фильтр сообщений		
Основная таблица		
Удалять большие вложения	☒	Продолж...
Условия		
Наличие вложений		
Действия		
Удалить аттачменты, проверяя их размер [>] [37M]	☒	Забывать
Удалять большие сообщения	☒	Забывать
Условия		
Размер сообщения [>=] [37M]		
Действия		
Забывать сообщение	☒	Продолж...
dns resolve	☒	Продолж...
Условия		
Любое сообщение		
Действия		
Провести разрешение имён DNS в IP адреса [Оба адреса]	☒	Принять
Завершить обработку	☒	Принять
Условия		
Любое сообщение		
Действия		
Принять сообщение	☒	

Действия

Новый объект

Фильтр

Таблица

Правило

Условие

Действие

Общие

Вырезать

Копировать

Копировать текст

Вставить

Удалить

Свойства

Настройка

↑ ↓ ↔ (…)

Размер сообщения **[>=] [37M]**
Условие учитывает сумму размеров извлечённых текстов и аттачментов.

Фильтр

EtherSensor:

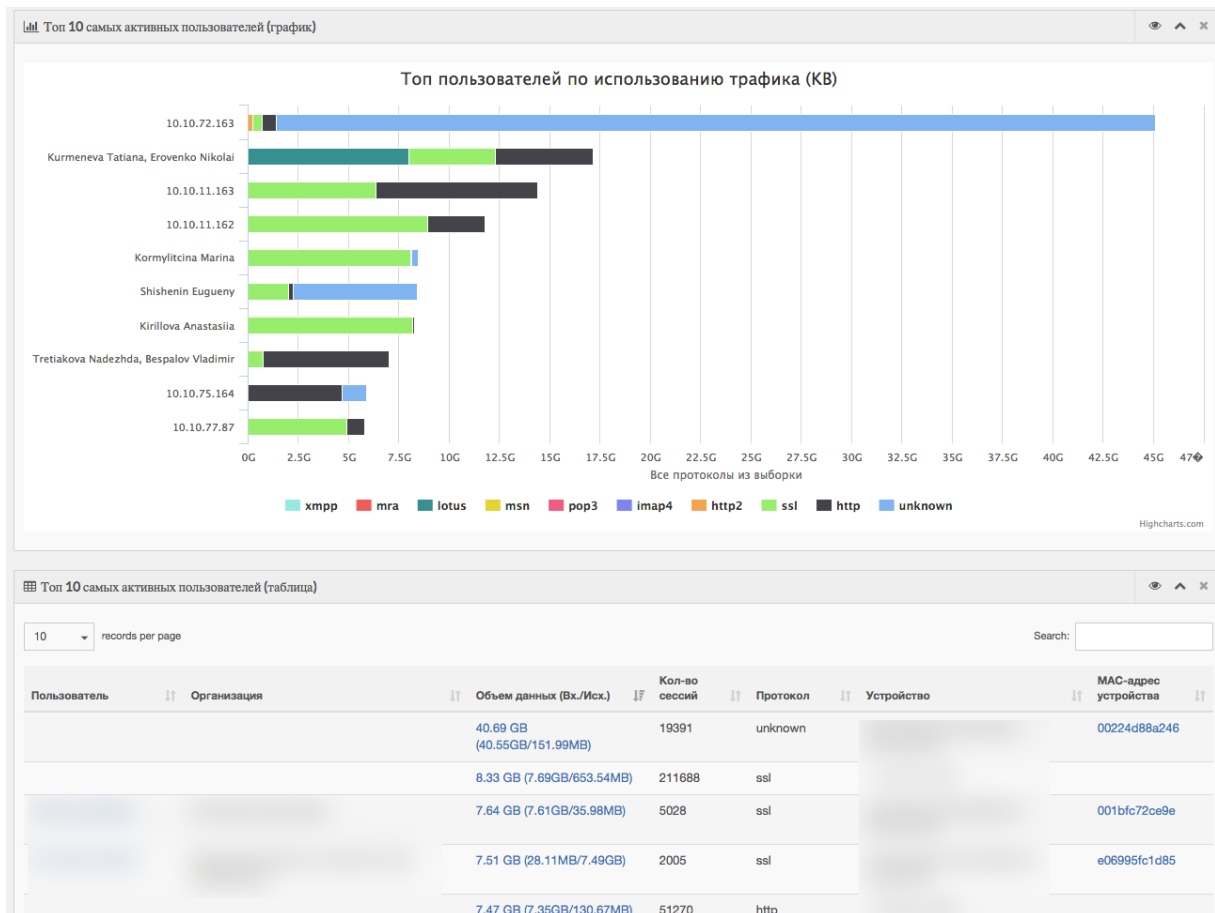
Транспорт результатов

Список профилей	Свойства профиля
☒ DLP	
☒ MailArchiva	
☒ SecureMailArchiva	
☒ Solar Dozor	
	1. Название и статус
	Название профиля MailArchiva
	Профиль используется по умолчанию Да
	2. Настройки SMTP
	Адрес сервера 10.10.1.242
	Порт 10025
	SSL Нет
	Таймаут сервера 10
	Держать соединение Да
	3. Идентификация
	Логин
	Пароль
	Адрес отправителя kpps@ethersensor.net
	Адрес получателя mail@archiva.com
	4. Формат сообщения
	Дублировать заголовки
	5. Обработка ошибок
	Ожидание после отказа 10
	6. Настройки групп профилей
	Вес 1
	Резервный профиль Да
	Название профиля
	Название профиля целиком на усмотрение пользователя. Рекомендуется использовать полные и заглавные буквы в именах профилей.

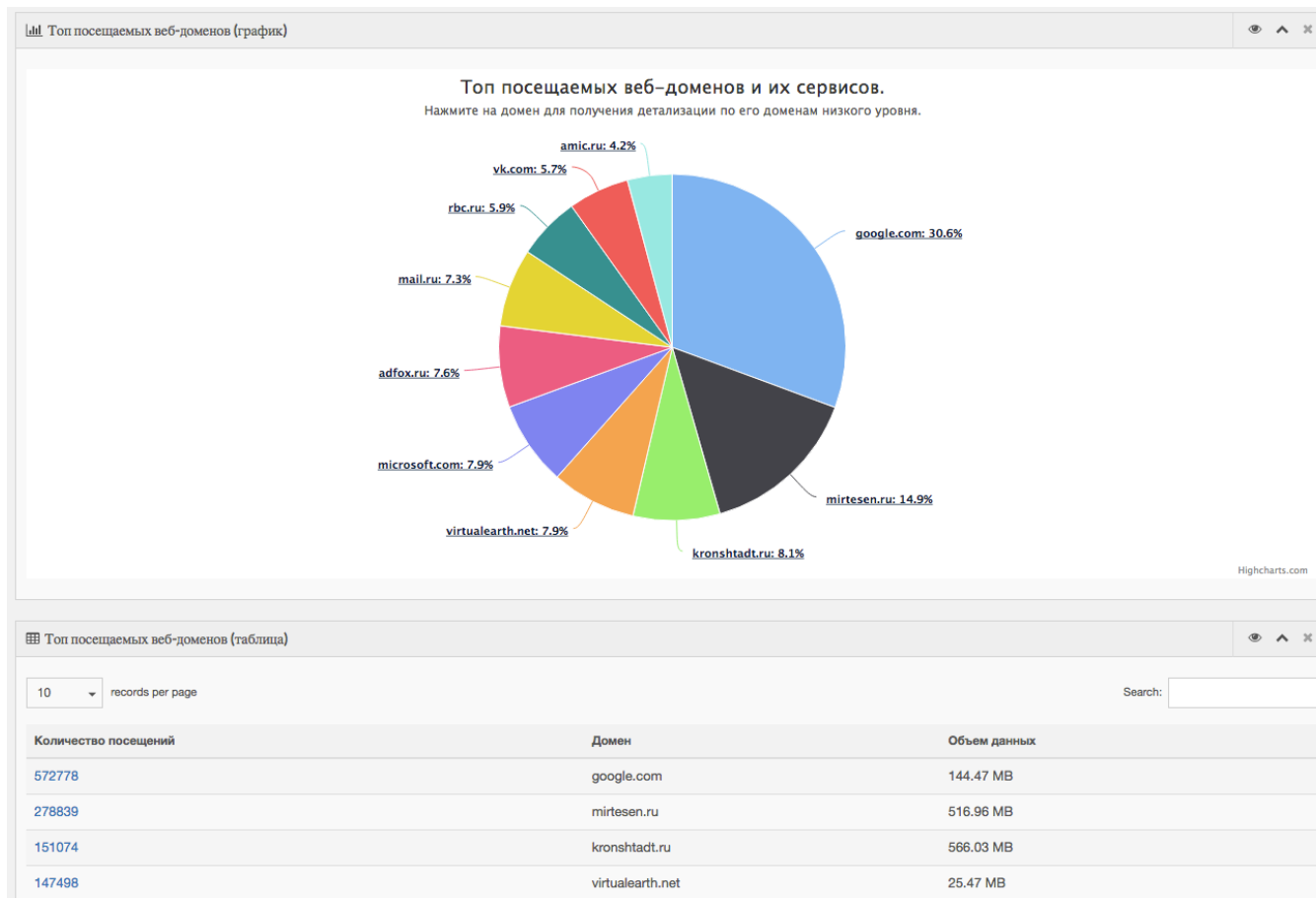
 **Транспортировка сообщений**

-  DEVICE LOCK профили
-  SMTP профили
-  FTP профили
-  SFTP профили
-  FILEDROP профили
-  IMAP профили
-  INFOWATCH профили
-  SMB профили
-  GROUP профили
-  Дополнительно

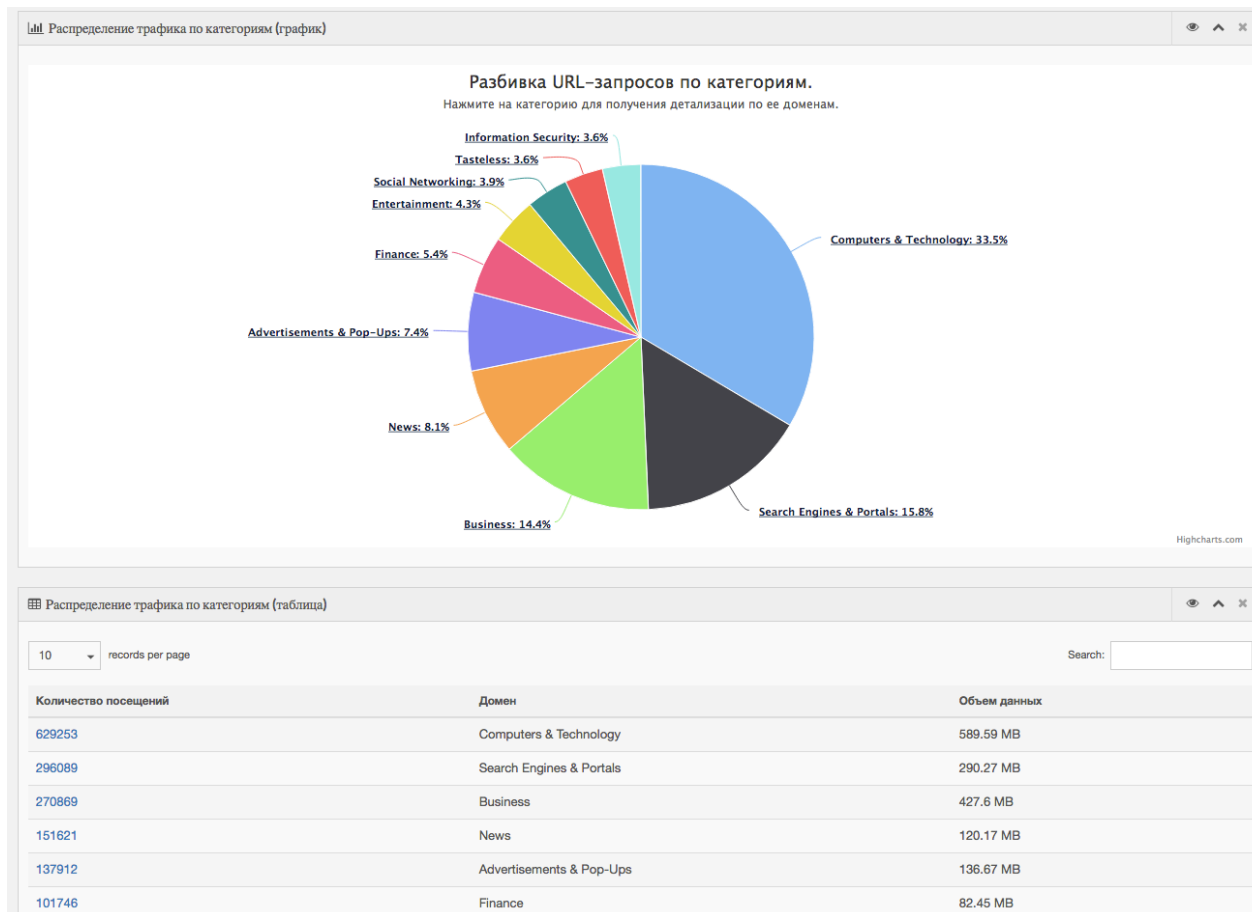
EtherStat: Отчет об использовании трафика



EtherStat: Топ посещаемых веб-доменов



EtherStat: Топ посещаемых категорий веб-доменов



EtherStat: Мониторинг веб-запросов



Последние HTTP-запросы

Кол-во записей

100

Частота обновления

5

сек.

10

records per page

Search:

Дата	Пользователь	Устройство (Имя/IP/MAC)	Домен	URL	Объем	Статус
2017-04-04 13:50:09	-	10.10.73.125	comagic.ru	http://tracker.comagic.ru/t/v/?sk=Gnr5R_6AlEv4qqzX ... b=jsonp1491303416908	1151.0 B	200
2017-04-04 13:50:09	-		revzona.ru	http://revzona.ru/mail/webapi/entry.cgi ... ail/webapi/entry.cgi	1429.0 B	200
2017-04-04 13:50:09	-	172.16.72.67	vk.com	http://vk.com/feed2.php ... p://vk.com/feed2.php	480.0 B	302
2017-04-04 13:50:09	-	/ 172.16.254.109 / 5cf9dd74fe35	mirtesen.ru	http://mtmsa.mirtesen.ru/pm/online?id=51528189 ... m/online?id=51528189	1340.0 B	200
2017-04-04 13:50:09	-	10.10.78.72	microsoft.com	http://officecdn.microsoft.com/pr/492350f6-3a01-4f ... tream.x64.x-none.dat	227.0 B	301
2017-04-04 13:50:09	-	10.10.78.72	microsoft.com	http://officecdn.microsoft.com/pr/492350f6-3a01-4f ... tream.x64.x-none.dat	227.0 B	301
2017-04-04 13:50:09		/ 10.10.76.171 / 7427ea11e6f4	guns.ru	http://forum.guns.ru/forums/icons/forum_pictures/0 ... 035/thm/18035957.jpg	941.0 B	301
2017-04-04 13:50:09		/ 10.10.76.171 / 7427ea11e6f4	guns.ru	http://forum.guns.ru/forums/icons/forum_pictures/0 ... 035/thm/18035969.jpg	951.0 B	301
2017-04-04 13:50:09	-	android-85b1d24b153ac850.int.kronshtadt.ru / 172.16.64.24 / 000822a7dcc5	apple.com	http://gsa21.ls.apple.com/stylesheet/default-8056 ... ea3dc03b63e8c22a0bbd	367.0 B	403
2017-04-04 13:50:09		/ 10.10.76.171 / 7427ea11e6f4	guns.ru	http://i2.guns.ru/forums/icons/forum_pictures/0180 ... 035/thm/18035961.jpg	540.0 B	200

Showing 1 to 10 of 100 entries

Previous

1

2

3

4

5

...

10

Next

EtherStat: Мониторинг поисковых запросов



Q Последние поисковые запросы

Частота обновления (сек.) Количество записей

Дата	Пользователь	Устройство (Имя/IP/MAC)	Поисковая машина	Поисковый запрос
2015-11-25 20:20:13			mail.ru	почему кошка топчет вас лапками
			mail.ru	yandex.ru
			yandex.ru	ао таргин
			yandex.ru	бэск инжиниринг
			yandex.ru	бэст инжиниринг
			google.com	австралопитек люси
			google.com	переводчик
			mail.ru	vk.com
			google.com	липецкий хладокомбинат логотип
			google.com	белгородский хладокомбинат логотип
			yandex.ru	очень сухая кожа лица с одной стороны
			yandex.ru	mail
			google.com	запись на прием в 29 жк

1

Начните вводить IP...

MAC-адрес:

Начните вводить MAC...

Имя устройства:

Начните вводить Hostname...

Компания:

Подразделение:

Начните вводить название подразделения...

Группа в AD:

Начните вводить название группы в AD...

№ комнаты:

Начните вводить № комнаты...

Пользователь:

Начните вводить ФИО, login

Поисковый запрос:

Поисковая машина	Поисковый запрос
yandex.ru	конец операции ре
yandex.ru	смотреть фильмы
yandex.ru	смотреть фильм с
yandex.ru	смотреть спектр 0
yandex.ru	как посмотреть за
yandex.ru	телеканал бобер т

Спасибо!



Сергей Сурков

ss@microolap.ru

Будем рады Вашим вопросам!

+7 (929) 927 36 42