Контроль над информационными потоками и действиями сотрудников.

Даниил Бориславский
Руководитель аналитического отдела
ООО Атом Безопасность
db@staffcop.ru

STAFFCOP

- Более 10 лет разработки приложений контроля сотрудников;
- Академгородок, Новосибирск, резиденты Технопарка и Сколково;
- Высокотехнологичная компания, ~50 сотрудников.
- Наша цель: «доступные решения задач информационной безопасности»
- Продано ~1300 серверных компонентов, ~ 66 000 АРМ за 2019-й год.
- Продано ~2200 серверных компонентов, ~ 171 000 АРМ за 2020-й год.

www.amtestlab.ru CERTIFIED AM TEST LAB REG # 00158 02/2016

PC MAGAZINE RUSSIAN EDITION BEST 2016 SOFT

Sk Сколково

академпарк Технопарк Новосибирского Академгородка

ФСТЭК России Федеральная служба по техническому и экспортному контролю

Минкомсвязь России

infosecurity RUSSIA

BIS SUMMIT 2018

Зачем нужен контроль над инф.потоками?

Тут могли быть слайды с числами, графиками, статистикой и даже картинками, но…

Зачем нужен контроль?

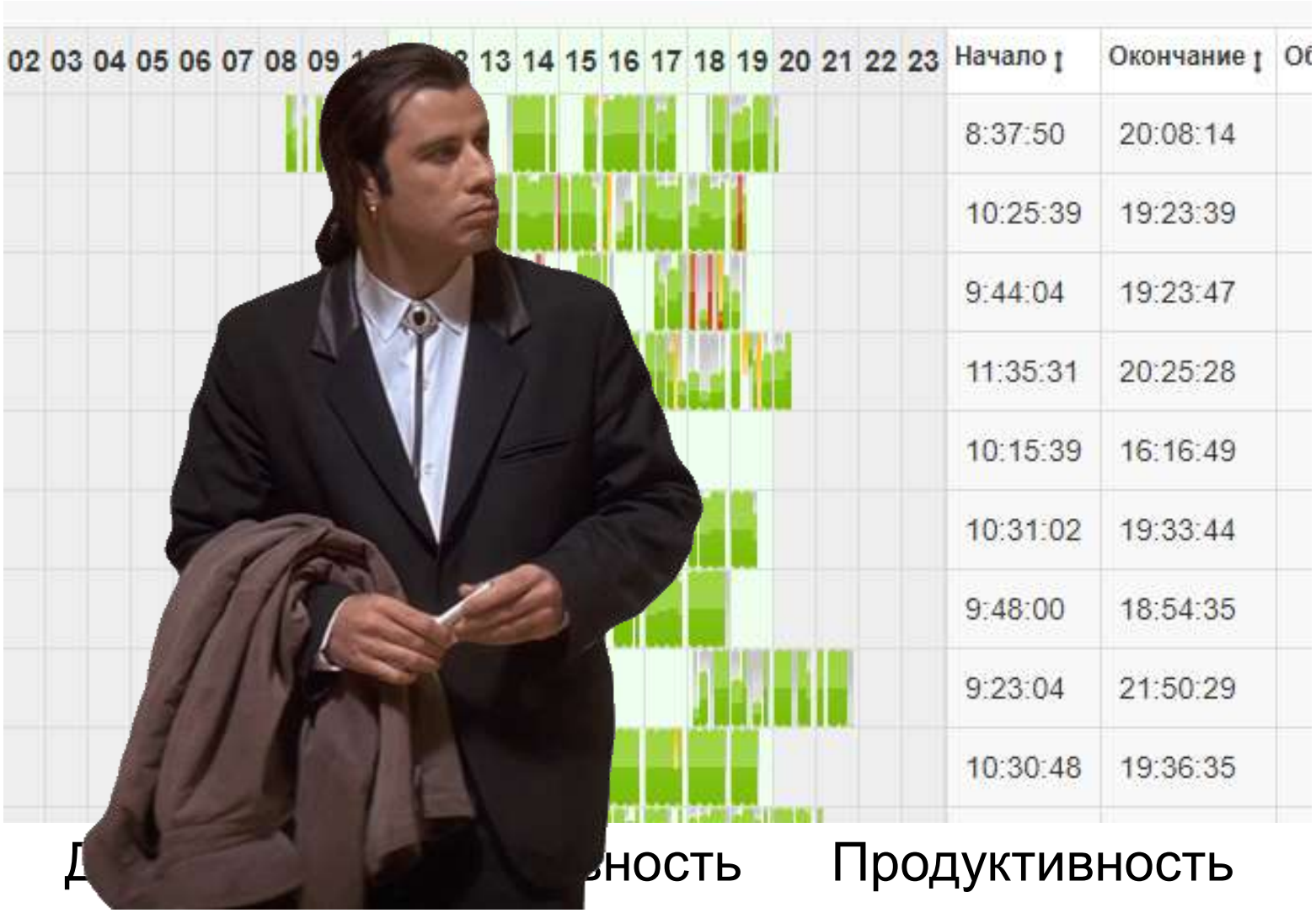
Лимит:

Учёт рабочего времени за период с 24 марта 2020 по 24 марта 2020

24 марта 2020 г. Вторник

Пользователь	00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23	Начало	Окончание	Общее время	Активное	Простой	Опоздание	Сверхурочные	Продуктивное	Непродуктивное	Нейтральное
		8:07:07	20:08:51	12ч 01м 44с	6ч 12м 31с	5ч 49м 13с	00с	1ч 09м 21с	00с	6ч 12м 31с	00с
Продуктивность											
Развлекательные ресурсы		6:12:53 (100.10%)									
Топ приложений											
chrome.exe		6:12:53 (100.10%)									
Топ сайтов											
youtube.com		5:40:29 (91.40%)									
twitch.tv		0:32:24 (8.70%)									

Зачем нужен контроль?



Д… …вность Продуктивность

Зачем нужен контроль?

Пользователь: Полное имя	Сайт	Приложение: Заголовок окна	Количество событий
Арсений Есетовский	avito.ru	cisco asa - Авито — объявления в Новосибирске — Объявления на сайте Авито - Mozilla Firefox	6
Арсений Есетовский	avito.ru	Cisco 2821 ASA5510 Cisco 1760 Juniper srx100 купить в Кемерово с доставкой | Бытовая электро ника | Авито - Mozilla Firefox	2
Арсений Есетовский	avito.ru	Cisco asa5505 купить в Барнаул	
Арсений Есетовский	avito.ru	Cisco asa 5505 купить в Новоси х	
Арсений Есетовский	avito.ru	Cisco ASA 5505 купить в Новоси х	
Арсений Есетовский	avito.ru	Сетевой экран Cisco ASA5505 к - Mozilla Firefox	
Арсений Есетовский	avito.ru	Межсетевой экран Cisco ASA 5 вито - Mozilla Firefox	
Арсений Есетовский	avito.ru	Продам Cisco ASA5510-SEC-BL роника | Авито - Mozilla Firefox	
Арсений Есетовский	avito.ru	Авито — объявления в Новосиб	
Арсений Есетовский	avito.ru	Cisco asa5505 купить в Барнаул	
Арсений Есетовский	avito.ru	Cisco 2821 ASA5510 Cisco 1760 ника | Авито	

Cisco Маршрутизатор /свич /коммутатор / межсетевой 1 500 ₽

Добавить в избранное Добавить заметку Вчера в 11:25

Купить с доставкой

Доставка в пункт выдачи

Гарантия возврата денег, если товар не подойдет Как это работает

Показать телефон

Написать сообщение
Отвечает около 30 минут

5.0 ★★★★★ 8 отзывов

52 объявления пользователя

Отчеты

8.07.2020 **12:47:12**

08.07.2020 **12:47:04**

8.07.2020 **12:46:15**

08.07.2020 **12:46:06**

08.07.2020 **12:45:49**

08.07.2020 **12:45:22**

08.07.2020 **12:45:07**

Зачем нужен контроль?

Общение с конкурентами | Выгрузка и печать | Панель управления | Админ | Меню (Admin)

События | Анализ | Учет времени | Отчеты | Добавить | Лимит:

Посещение сайтов

Пользователь: Полное имя	Дата: День	Сайт	Время активности
Арсений Есетовский	18-июнь-2020	searchinform.ru	00 ч 02 м 55 с

Переписка - количество

Пользователь: Полное имя	Дата: День	Переписка: Домен
Арсений Есетовский	18-июнь-2020	searchinform.ru

Переписка - подробно

Время	Тип	Компьютер	Пользователь	Приложение
2020-06-18 10:47:23	Почта	DemoZoneVM1	Арсений	thunderbird.exe

Панель управления | Админ | Меню (Admin)

Лимит:

						Контент
2020-06-14 16:05:0	DemoZoneVM2	Ксения	Ксения Касперов	Арсений Есетовс	Re: Проверка связи	
2020-06-14 16:01:1	DemoZoneVM2	Ксения	Ксения Касперов	Бориславский Да	Данные	Скачать Входные цены.xlsx InterceptedFile
2020-06-14 15:45:3	DemoZoneVM2	Ксения	Ксения Касперов	Арсений Есетовс	Re: Проверка связи	Скачать Лист Microsoft Excel.xlsx InterceptedFile
2020-06-14 15:44:1	DemoZoneVM2	Ксения	Ксения Касперов	Арсений Есетовс	Проверка связи	

Зачем нужен контроль?

Банк России

ГОСТ Р 57580.1-2017

Безопасность финансовых (банковских) операций.

STAFFCOP

Комплексное решение по информационной безопасности,
учёту рабочего времени и контролю эффективности сотрудников

учет рабочего времени

эффективность персонала

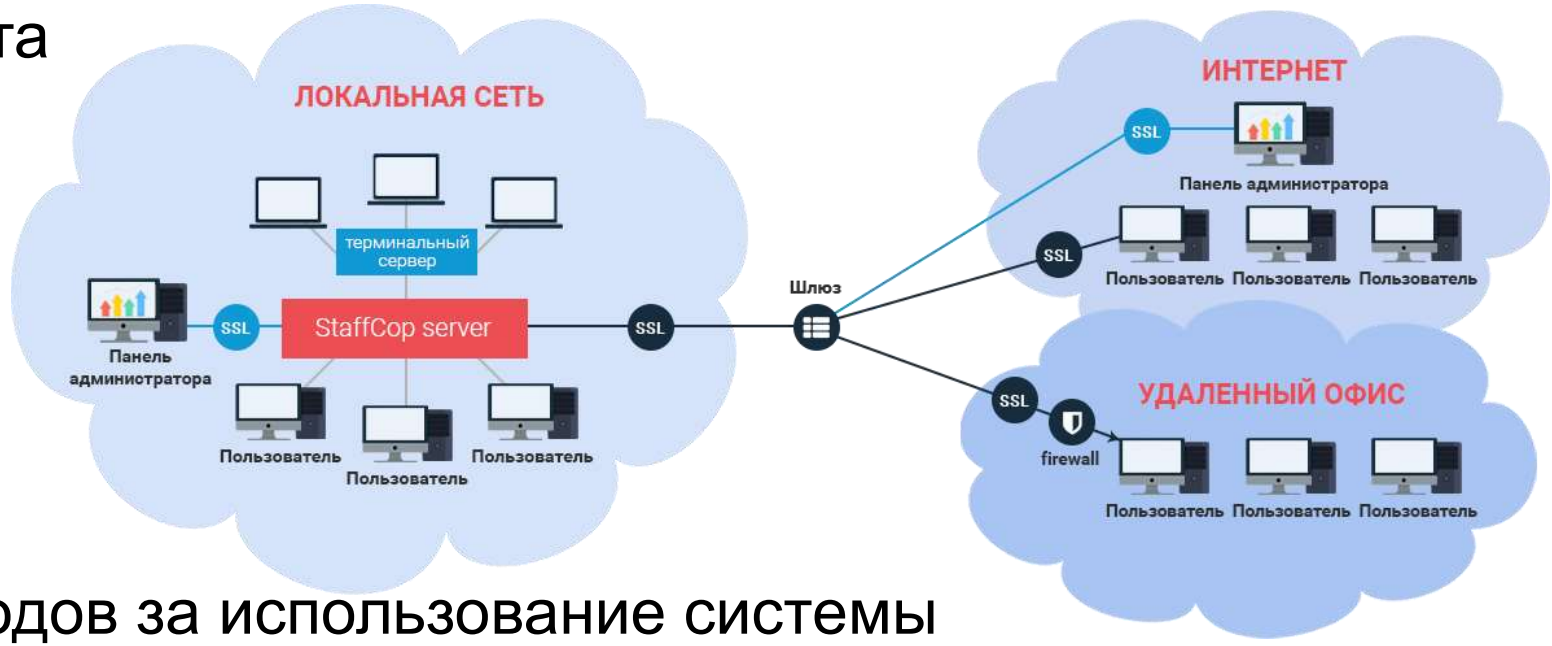
информационная безопасность

расследование инцидентов

удаленное администрирование

Современные архитектурные решения

- Для работы сервера уже достаточно всего одной виртуальной машины
- Контроль ПК под управлением OS Windows, Linux, MacOS
- Система готова к сбору данных сразу после установки
- Удалённая установка агента
- OS Linux, BD PostgreSQL



- Нет дополнительных расходов за использование системы

Тотальный контроль действий за ПК

Декодирование сервисов веб-почты и социальных сетей:

— mail.ru, yandex.ru, gmail.com…
— VK, FB, Одноклассники, LinkedIn…

Почтовые протоколы:
— SMTP / SMTPs
— IMAP
— POP3 / POP3s
— MS Exchange

Передача гипертекстовой информации и файлов:
— HTTP / HTTPs
— FTP / FTPs

Интернет-мессенджеры
— Skype
— ICQ, QIP, Jabber (XMPP)
— Mail.ru Agent
— Yahoo и другие

USB-порты
— контроль и блокировка

Теневое копирование файлов
— из электронной почты
— со съемных носителей
— переданных через интернет
— отправленных на печать

Расследование инцидентов ИБ

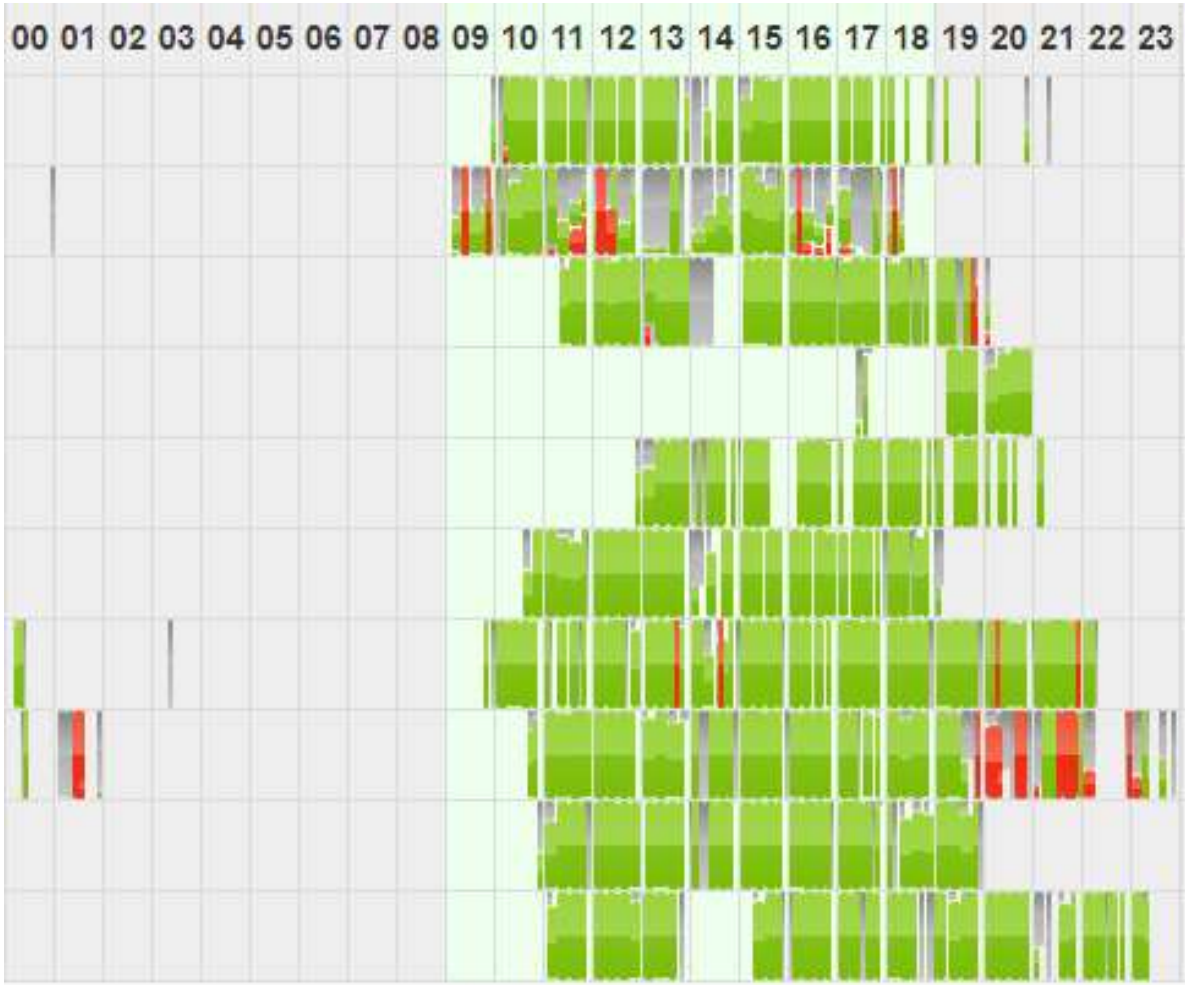
- Архив данных
- Конструктор многомерных отчетов
- Поиск по словам и регулярным выражениям
- Множество графов и диаграмм
- Система оповещений
- Гибкая система настройки фильтров

Управление и администрирование

- Мониторинг
- Блокировки
- Инвентаризация ПО и «железа»
- Интеграция с SIEM
- Разные доступы для разных пользователей системы


Картинки о том как всё будет работать
Скриншоты и примеры как работает

Учёт рабочего времени и его оценка



Начало	Окончание	Общее время	Активное	Простой
9:54:29	21:15:32	11:21:03	6:14:19	5:06:44
9:07:06	18:22:55	9:15:49	8:34:07	0:41:42
11:20:35	20:01:01	8:40:26	7:04:36	1:35:50
17:23:27	20:57:18	3:33:51	1:41:48	1:52:03
12:53:25	21:14:43	8:21:18	3:46:49	4:34:29
10:35:44	19:10:12	8:34:28	7:17:27	1:17:01
0:10:40	22:15:10	22:04:30	10:35:12	11:29:18
0:00:33	23:54:10	23:53:37	12:44:53	11:08:44
10:51:19	19:52:45	9:01:26	8:11:35	0:49:51
11:05:09	23:19:51	12:14:42	9:13:23	3:01:19

Дисциплина Активность Продуктивность

Учёт рабочего времени на удалёнке

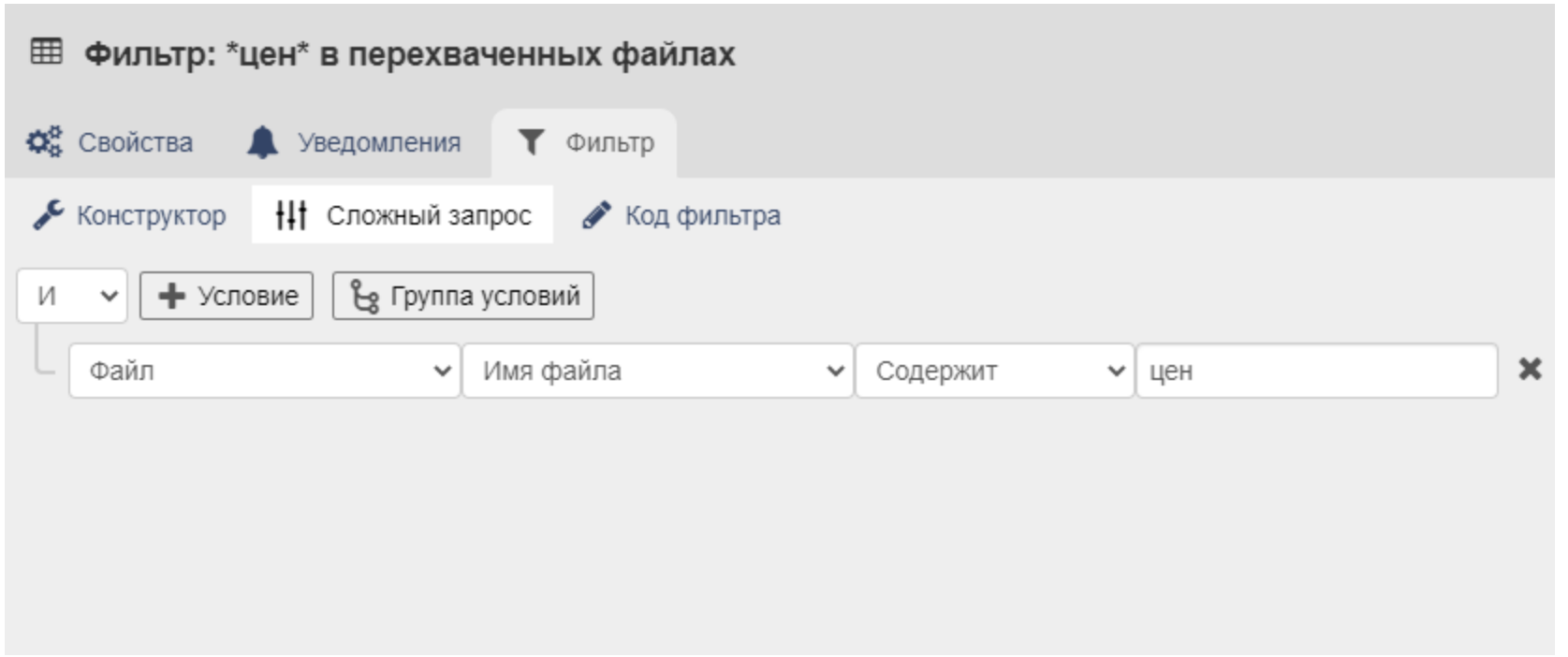
Отчет по активности пользователей за период с 1 июня 2020 по 30 июня 2020

Даниил Бориславский

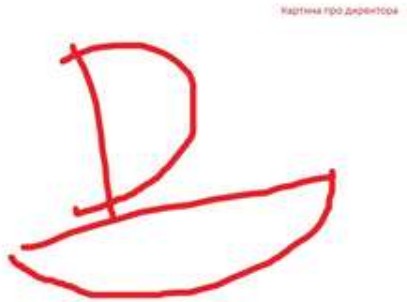
Пользователь	Общее время	Активное время	Время простоя	Опоздание	Сверхурочные	Продуктивн
Даниил Бориславский	245:46:59	106:55:53	138:51:06	27:50:19	6:01:37	
− **Продуктивность**						
Офисные приложения	23:54:58 (22.37%)					
Поисковые порталы	17:01:07 (15.92%)					
Приложения для удаленного доступа	14:40:02 (13.72%)					
Всё остальное	13:41:09 (12.80%)					
Корпоративные ресурсы	11:59:14 (11.21%)					
Интернет-мессенджеры	7:24:04 (6.92%)					
Корп. ресурсы	5:45:15 (5.38%)					
Почтовые приложения	4:34:14 (4.27%)					
Информационная безопасность	2:02:01 (1.90%)					
Интерфейс системы	1:22:53 (1.29%)					
+ **Топ приложений**						
+ **Топ сайтов**						

Теневые копии файлов – поиск по атрибутам

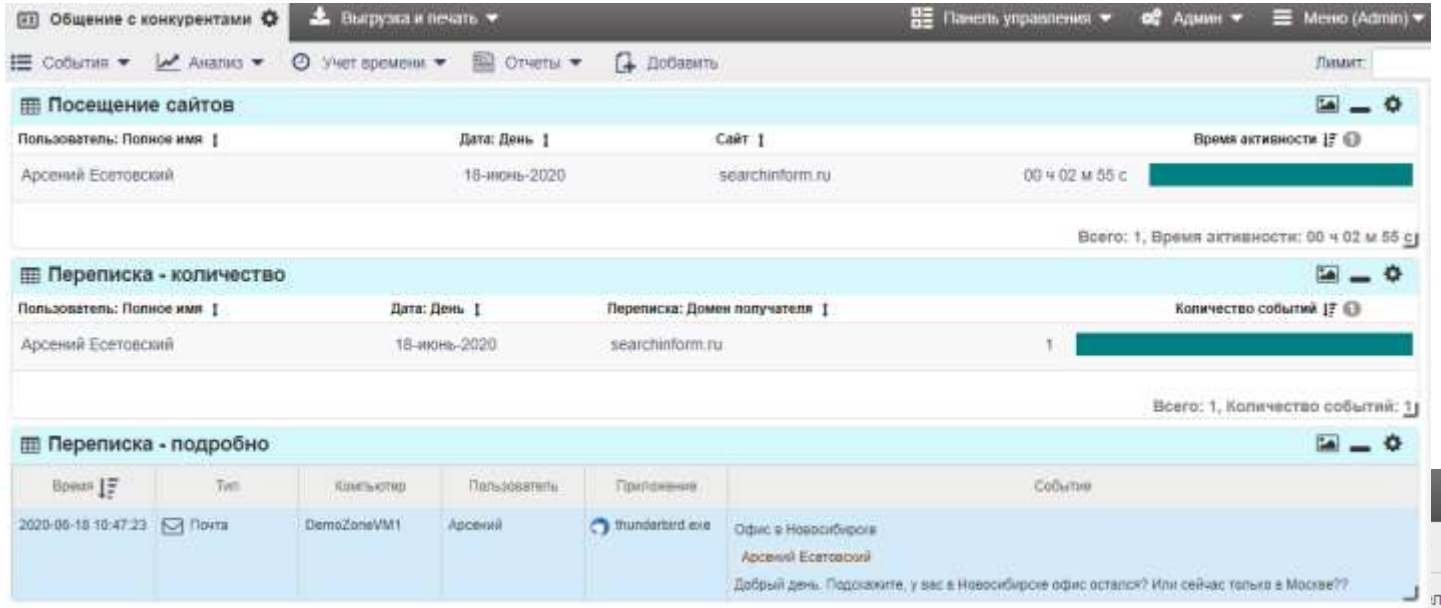
Время	Компьютер	Пользователь	Приложение	Контент	Связано с	Страниц	Размер	Получатели
2020-07-08 12:34	DemoZoneVM2	Ксения	explorer.exe	Скачать Входные цены.xlsx	FileOperation		8.2 Kb	
2020-06-14 17:25	DemoZoneNB4	BoDa		Скачать входные цены.xlsx	PrintDoc	1	8.2 Kb	
2020-06-14 16:47	DemoZoneNB3	d.borislavskiy	explorer.exe	Скачать Входные цены.xlsx	FileOperation		8.2 Kb	
2020-06-14 16:01	DemoZoneVM2	Ксения	chrome.exe	Скачать Входные цены.xlsx	Mail		8.2 Kb	Бориславский Даниил

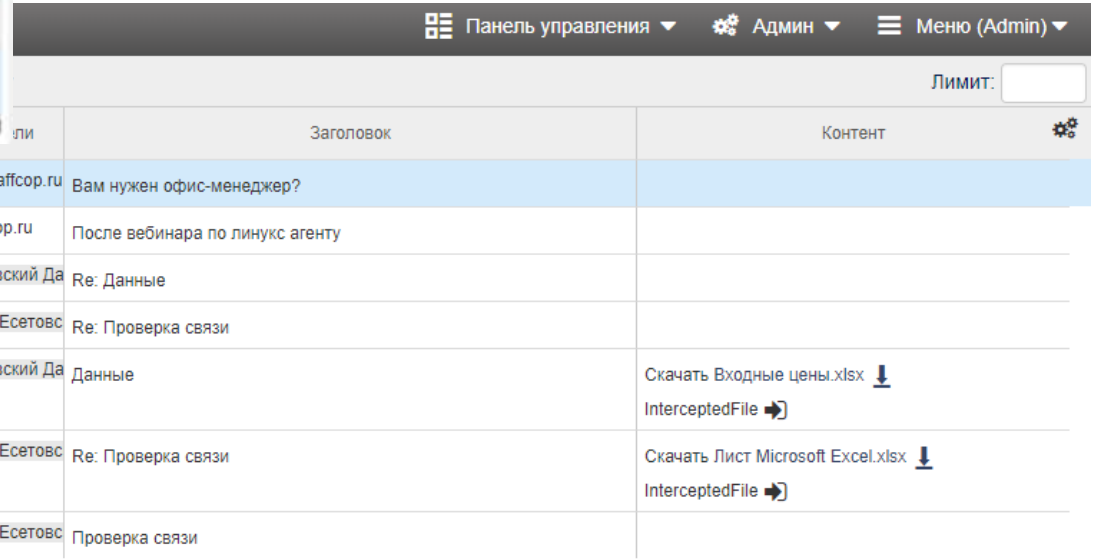


Теневые копии файлов – поиск по тексту

Перехваченный ф	DemoZoneVM2	Ксения	skype.exe	Ищем директора Отчёт 2 кв.docx Скачать Отчёт 2 кв.docx 8:live:.cid.2ba49cc565661352 Ежеквартальный отчёт для директора Тут какие-то очень важные данные Im
Перехваченный ф	DemoZoneVM1	Арсений	thunderbird.exe	Ищем директора Картиночка.jpg  Скачать Картиночка.jpg Ксения Касперова Картина продиректора Mail

Общение с конкурентами и личная почта





2020-06-18 10:37:1	DemoZoneVM2	Ксения	Ксения Касперов	r.frank@staffcop.ru	Вам нужен офис-менеджер?	
2020-06-14 16:36:1	DemoZoneVM2	Ксения	Ксения Касперов	pv@staffcop.ru	После вебинара по линукс агенту	
2020-06-14 16:08:1	DemoZoneVM2	Ксения	Ксения Касперов	Бориславский Да	Re: Данные	
2020-06-14 16:05:0	DemoZoneVM2	Ксения	Ксения Касперов	Арсений Есетовс	Re: Проверка связи	
2020-06-14 16:01:1	DemoZoneVM2	Ксения	Ксения Касперов	Бориславский Да	Данные	Скачать Входные цены.xlsx InterceptedFile
2020-06-14 15:45:3	DemoZoneVM2	Ксения	Ксения Касперов	Арсений Есетовс	Re: Проверка связи	Скачать Лист Microsoft Excel.xlsx InterceptedFile
2020-06-14 15:44:1	DemoZoneVM2	Ксения	Ксения Касперов	Арсений Есетовс	Проверка связи	

Сканы паспортов и номера кредитных карт

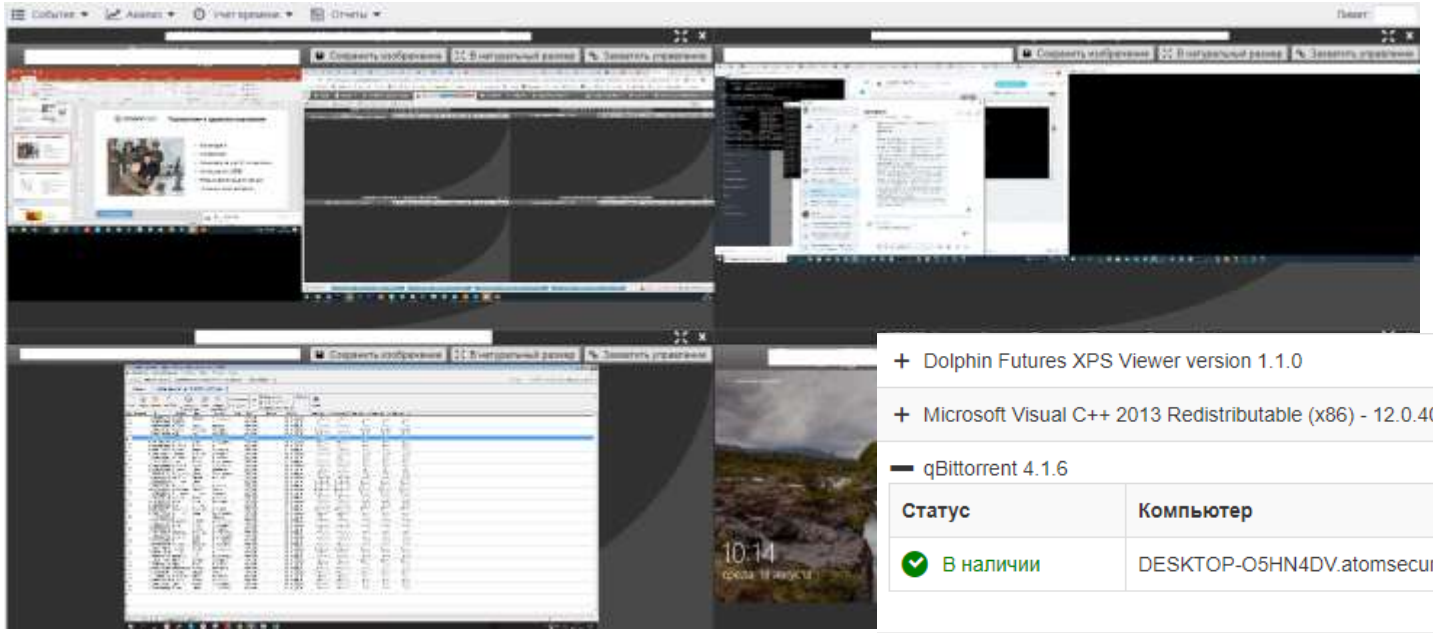
Время 2020-11-17 11:48:15

Фильтр Сервер распознаваний

Контент

				Скачать Documents.7z
	DemoZoneVM2	Ксения	chrome.exe	Кредитные карты Ксения Касперова Сначала деньги, потом остальное 4276160971368577 сбер вс, 14 июн. 2020 г. в 16:06, Даниил Бориславский <d.borislavskiy@staffcop.ru>: норм, давай ещё вс, 14 июн. 2020 г. в 16:01, Ксения Касперова <kkasperova522@gmail.com>: Как договаривались.

Управление и администрирование



+ Dolphin Futures XPS Viewer version 1.1.0
+ Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.40649
− qBittorrent 4.1.6

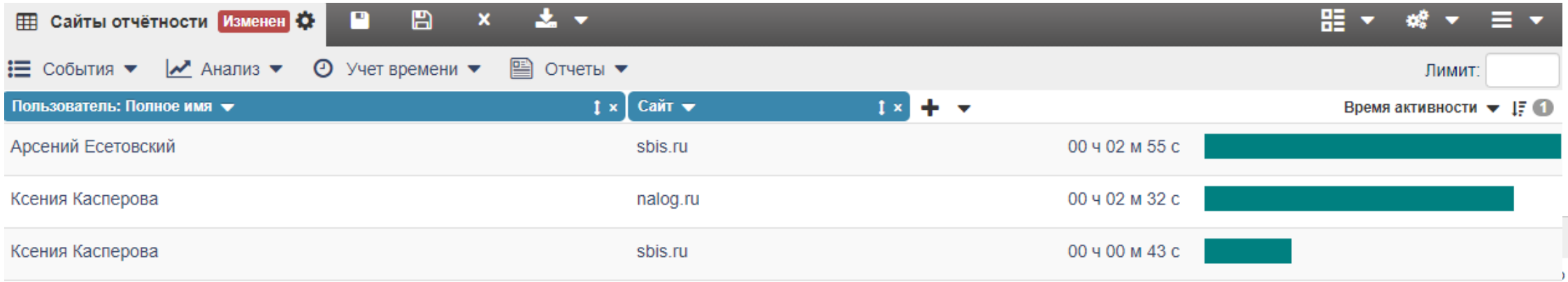
Статус	Компьютер	Поставщик	Версия	Дата наличия
В наличии	DESKTOP-O5HN4DV.atomsecurity.com	The qBittorrent project	4.1.6	17:06:25 04.06.2020

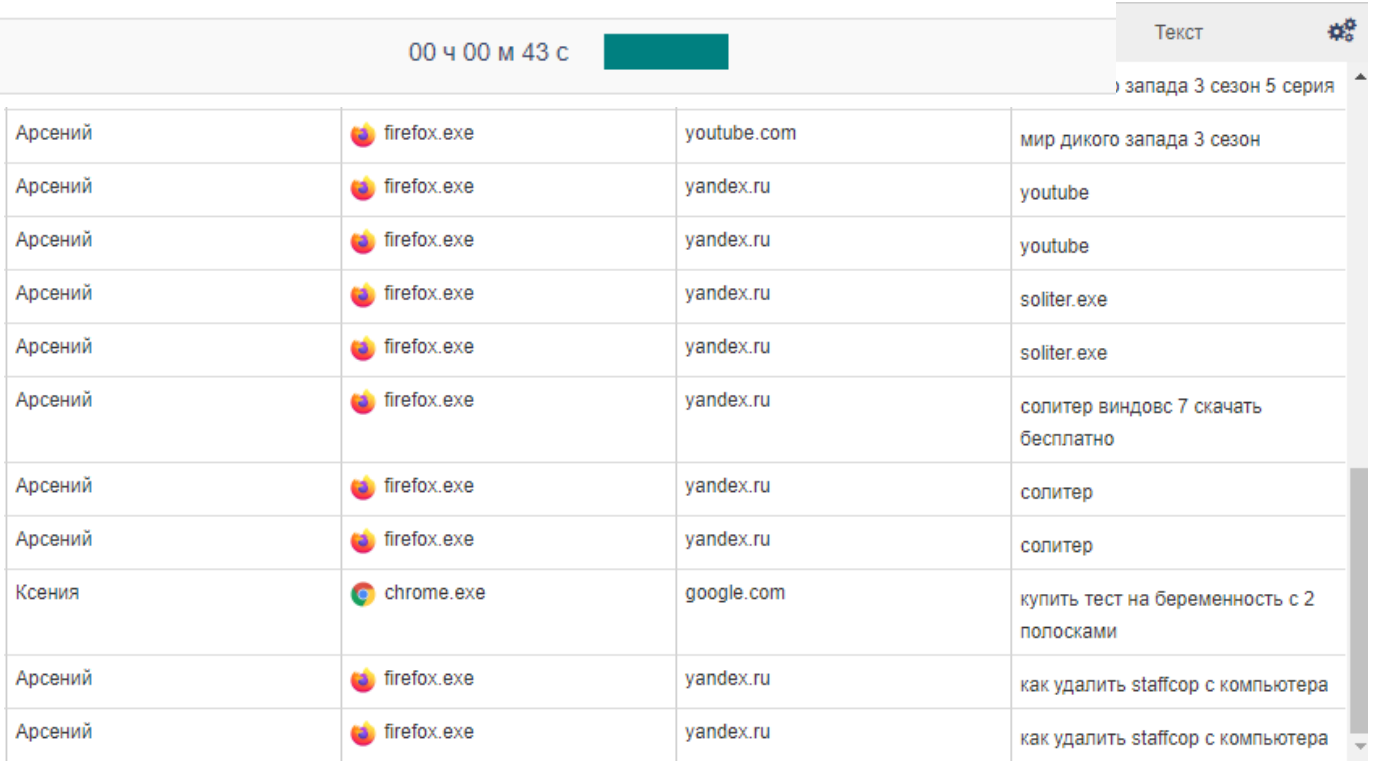
+ Update for Microsoft Office 2013 (KB3039756) 32-Bit Edition
+ Update for Microsoft Office 2010 (KB4092436) 32-Bit Edition
+ K-Lite Codec Pack 14.1.5 Full
− Git version 2.22.0.windows.1

Статус	Компьютер	Поставщик	Версия	Дата наличия
В наличии	NB0001.atomsecurity.com	The Git Development Community	2.22.0.windows.1	18:29:13 21.01.2020

+ Обновление безопасности для Windows XP (KB2820917)
+ Обновление безопасности для Windows XP (KB976323)

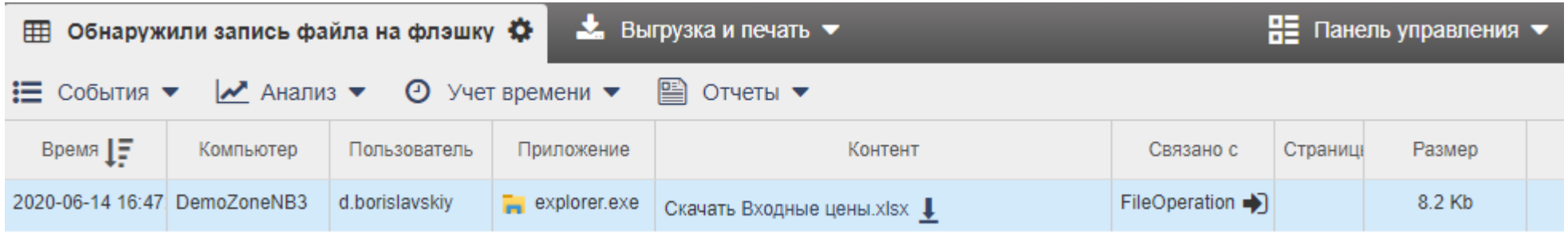
Поисковые запросы и посещение сайтов

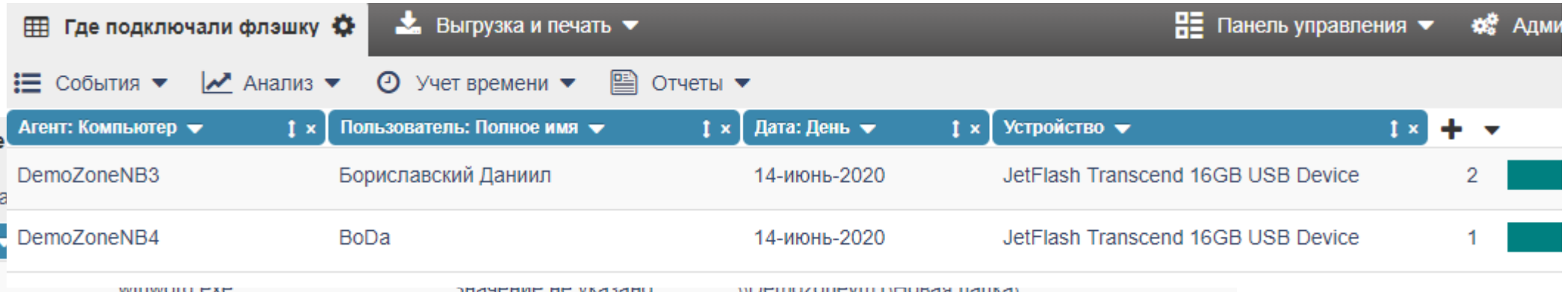


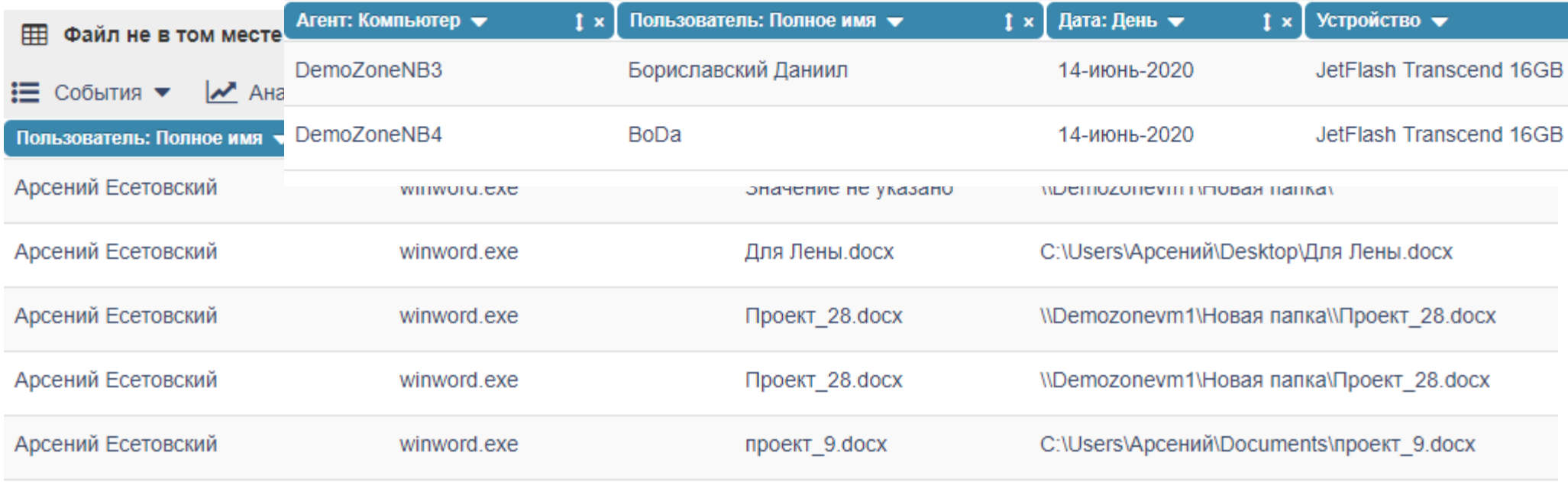


Арсений	firefox.exe	youtube.com	мир дикого запада 3 сезон
Арсений	firefox.exe	yandex.ru	youtube
Арсений	firefox.exe	yandex.ru	youtube
Арсений	firefox.exe	yandex.ru	soliter.exe
Арсений	firefox.exe	yandex.ru	soliter.exe
Арсений	firefox.exe	yandex.ru	солитер виндовс 7 скачать бесплатно
Арсений	firefox.exe	yandex.ru	солитер
Арсений	firefox.exe	yandex.ru	солитер
Ксения	chrome.exe	google.com	купить тест на беременность с 2 полосками
Арсений	firefox.exe	yandex.ru	как удалить staffcop с компьютера
Арсений	firefox.exe	yandex.ru	как удалить staffcop с компьютера

Расследование инцидентов







Потребители

Преимущества

На open source решениях и не требует дополнительного платного программного обеспечения.

Бессрочные лицензии и гибкая политика лицензирования.

OLAP-куб снижает требования к «железу» сервера.

97% внедрений StaffCop окупились менее чем за 2 месяца.

Полноценное техническое сопровождение с начального этапа тестирования.

Многомерные аналитические отчёты и схемы с возможностью перехода от общего к частному и наоборот.

Аспекты внедрения

Правовые

Технические

Административные

Аспекты внедрения

- **№149 ФЗ «Об информации, информационных технологиях и о защите информации».**
- **№98 ФЗ «О коммерческой тайне».**
- **№152 ФЗ «О защите персональных данных».**
- Определить и довести до работников правила использования средств хранения, обработки и передачи информации .
- Разработать и довести до работников регламент проведения мониторинга.
- Получить согласие работников на проведение мониторинга использования им средств хранения, обработки и передачи информации.
- Включить положения об обязательстве работника соблюдать правила использования средств коммуникации и согласие на мониторинг в трудовой договор (дополнительное соглашение к трудовому договору).

Аспекты внедрения

- В дополнение к лицензиям на ПО могут потребоваться лицензии на OS и DataBase.
- Развёртывание и настройка системы.
- Система не должна мешать бизнесу работать и зарабатывать.
- Не платите за то, что вам не нужно.
- Возможно, потребуется сертифицированная ФСТЭК версия.
- Система должна иметь возможность быть полезной всем подразделениям.
- Система должна решать задачи поставленные бизнесом.

Политика лицензирования и стоимость

Количество компьютеров	Лицензия на 12 месяцев	Лицензия на 3 месяца
5–25	3 350 ₽ / 1 ПК	1 117 ₽ / 1 ПК
26–50	3 050 ₽ / 1 ПК	1 017 ₽ / 1 ПК
51–150	2 990 ₽ / 1 ПК	997 ₽ / 1 ПК
151–250	2 890 ₽ / 1 ПК	963 ₽ / 1 ПК
251–500	2 790 ₽ / 1 ПК	930 ₽ / 1 ПК
501–1000	2 690 ₽ / 1 ПК	897 ₽ / 1 ПК
1000+	2 590 ₽ / 1 ПК	863 ₽ / 1 ПК

Бессрочная лицензия – по запросу

Благодарю за внимание!

Даниил Бориславский
Руководитель аналитического отдела
ООО Атом Безопасность

+7(499)6382809 доб. 235
db@staffcop.ru
d.borislavskiy