Контроль надежности и эффективности информационных потоков филиальной сети

Чеплиёв Максим
Специалист отдела аналитики
ООО Атом Безопасность
m.chepliev@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

STAFFCOP

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

учет рабочего времени

эффективность персонала

информационная безопасность

расследование инцидентов

удаленное администрирование

Особенности и сложности контроля филиальной сети

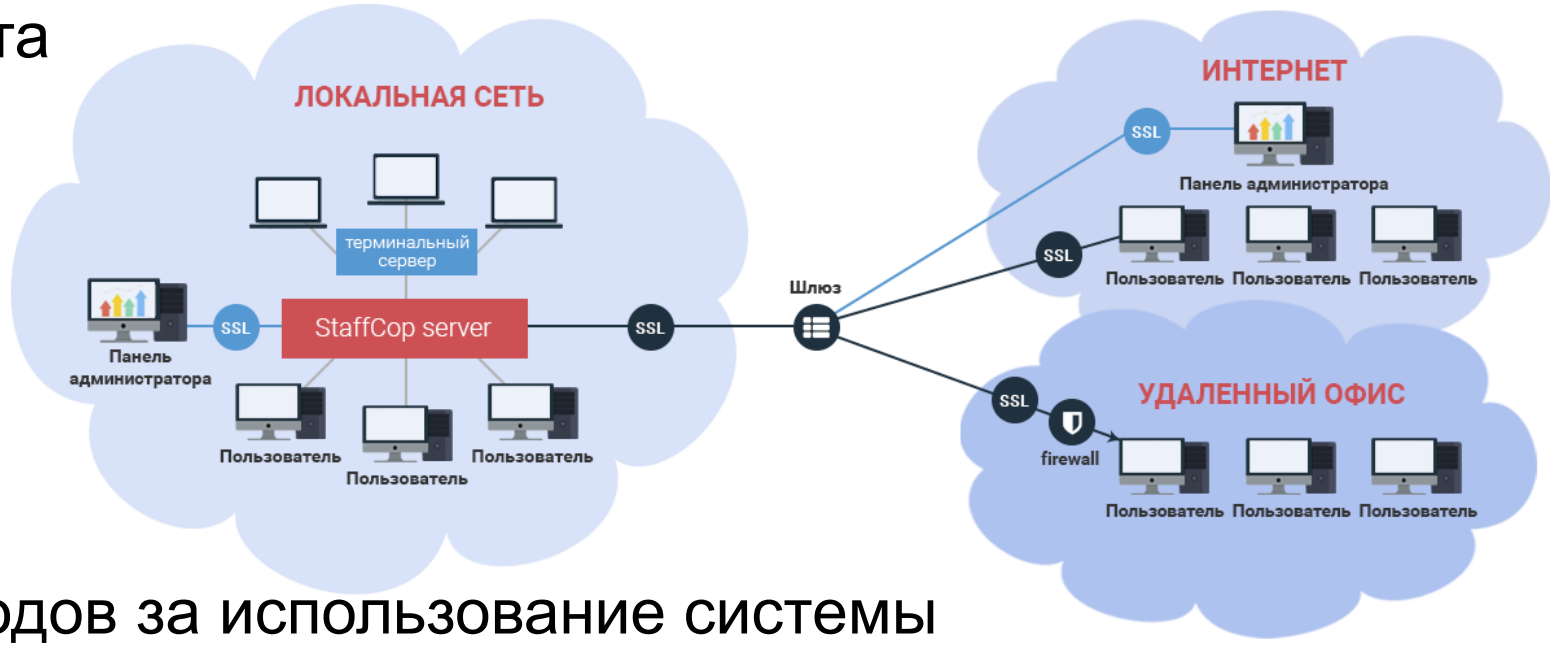
- Распределенность
- Сложность структуры
- Удаленность: время и расстояние
- Передача и контроль информации
- Организационные сложности
- Руководство, анализ и контроль

Особенности нашего решения

- Организация собранной информации
- Системы анализа и отчетов
- Интеграция с существующими системами контроля и организации
- Возможность распределенной структуры
- Возможность удаленного анализа

Наше решение

- 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

Полный контроль за объектом защиты

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

Местоположение среды контроля

- В одной сети с сервером
- В отличной от сервера подсети
- RDP до рабочей станции
- RDP до терминального сервера
- Среда контроля вне сети, но есть VPN
- Среда контроля имеет только доступ в интернет
- Только VPN
- Контроль среды без каналов передачи данных

Расследование инцидентов ИБ

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

Пользователи и администраторы, интеграция с AD

Пользователи

- Данные
- Группы
- Контроль
- Анализ
- Профиль пользователя

Администраторы

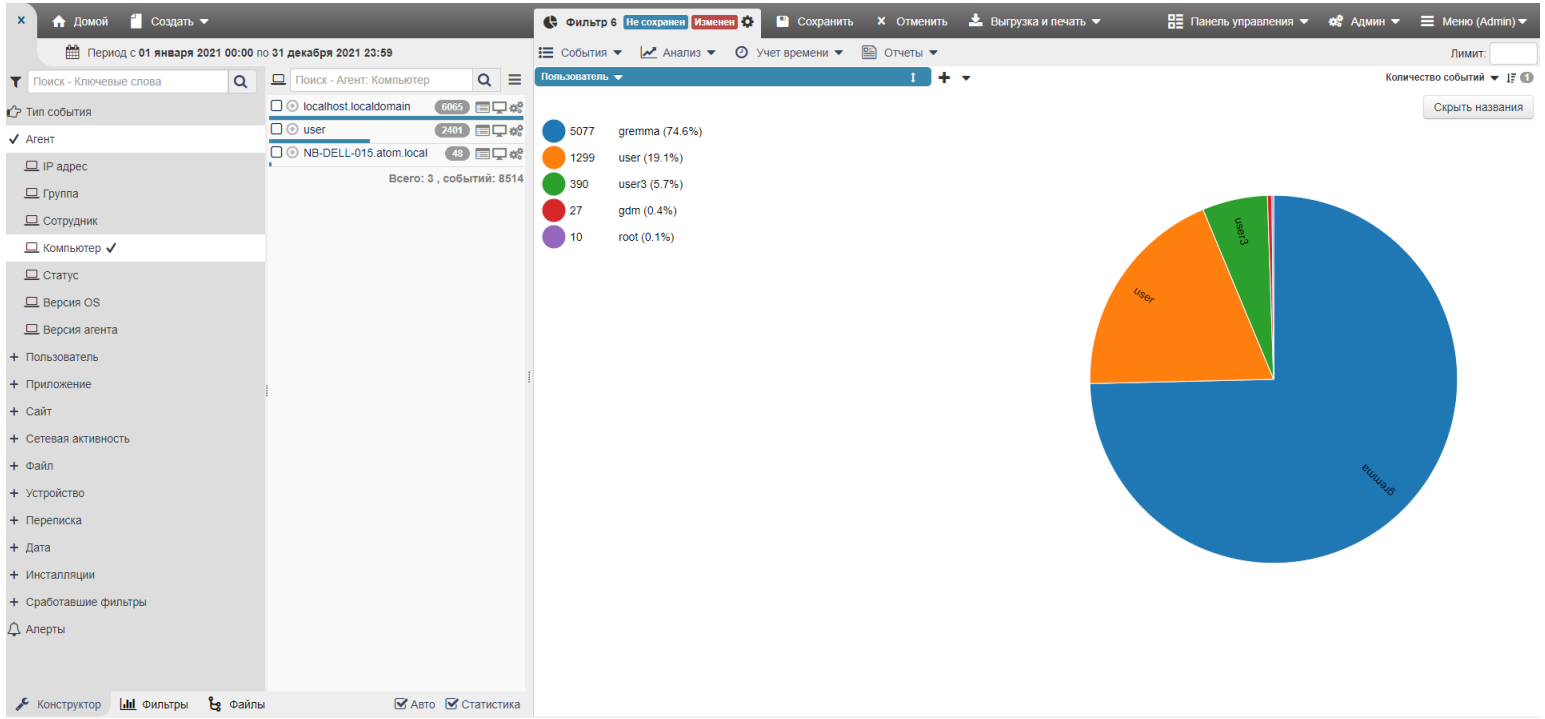
- Доступ к анализу и отчетам
- Контроль групп
- Уровень доступа
- Контроль администраторов

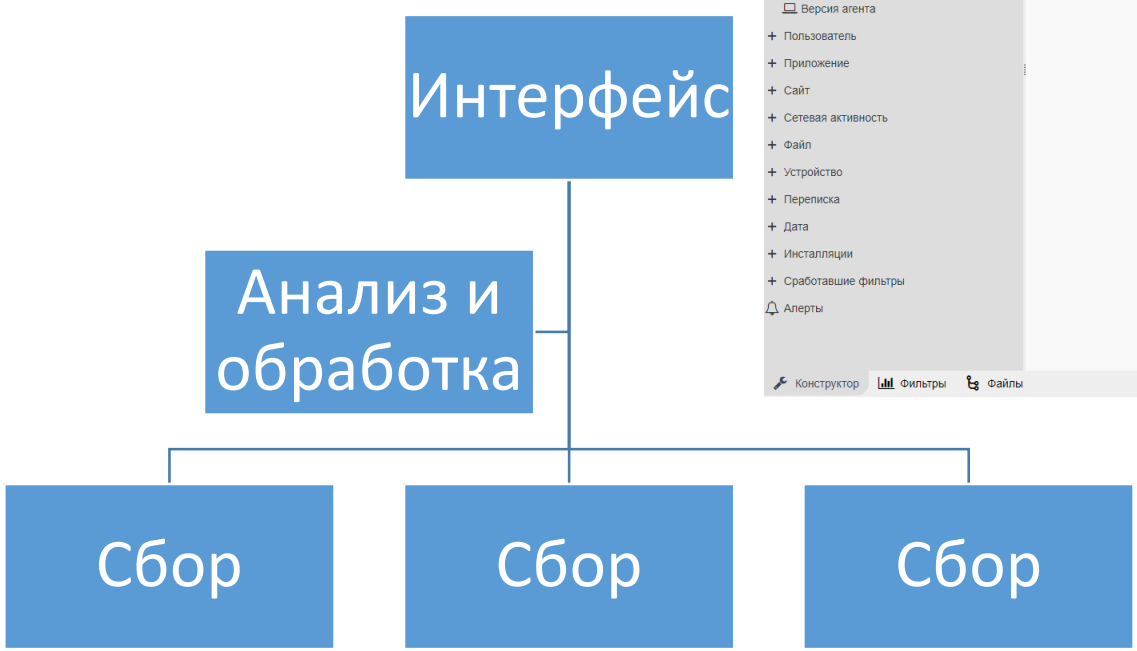
Анализ

- Групповой анализ
- Анализ деятельности
- Анализ взаимодействий

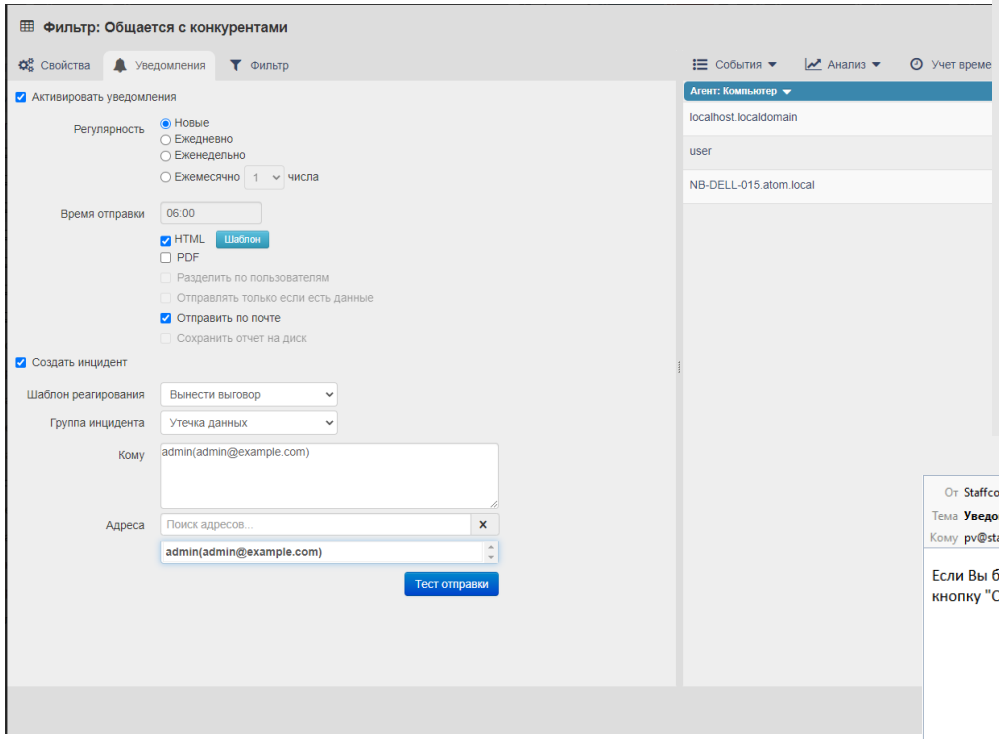
Slave-Master структура серверов

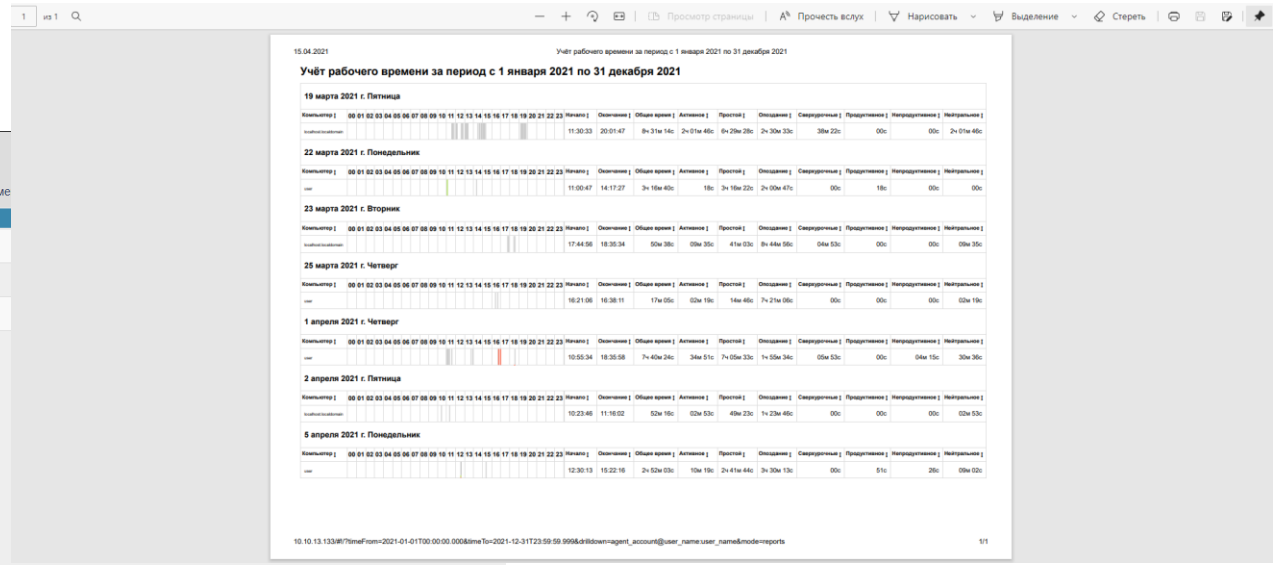
Удаленный доступ к серверу



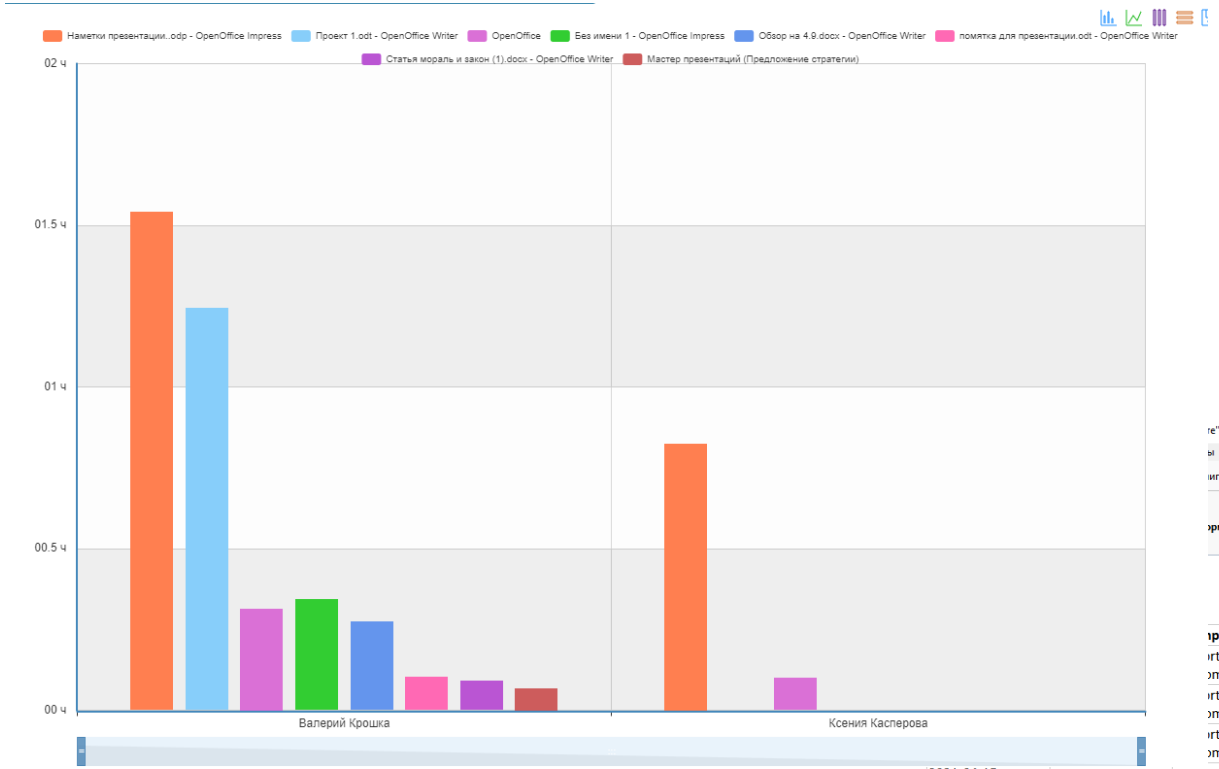


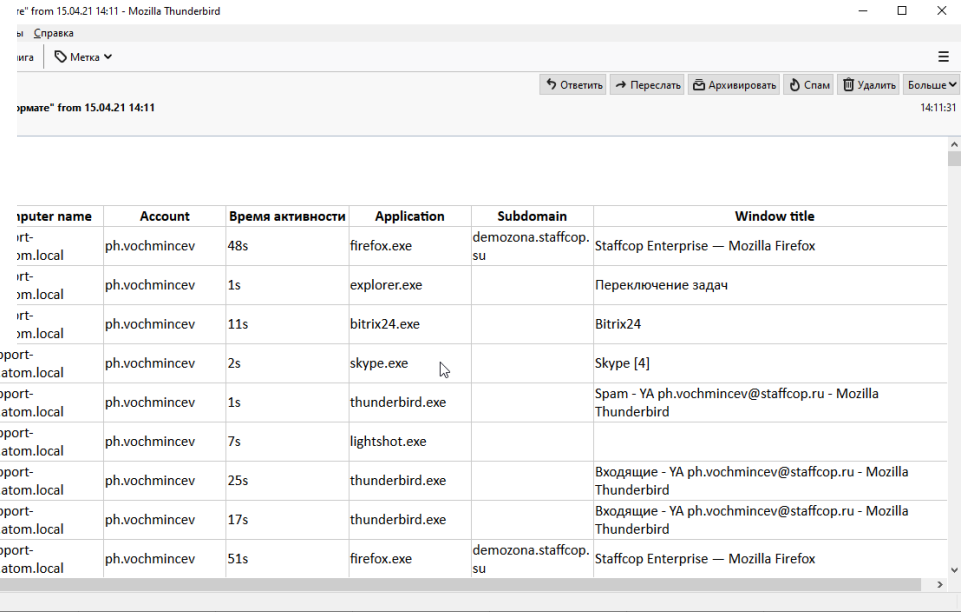
Система уведомлений





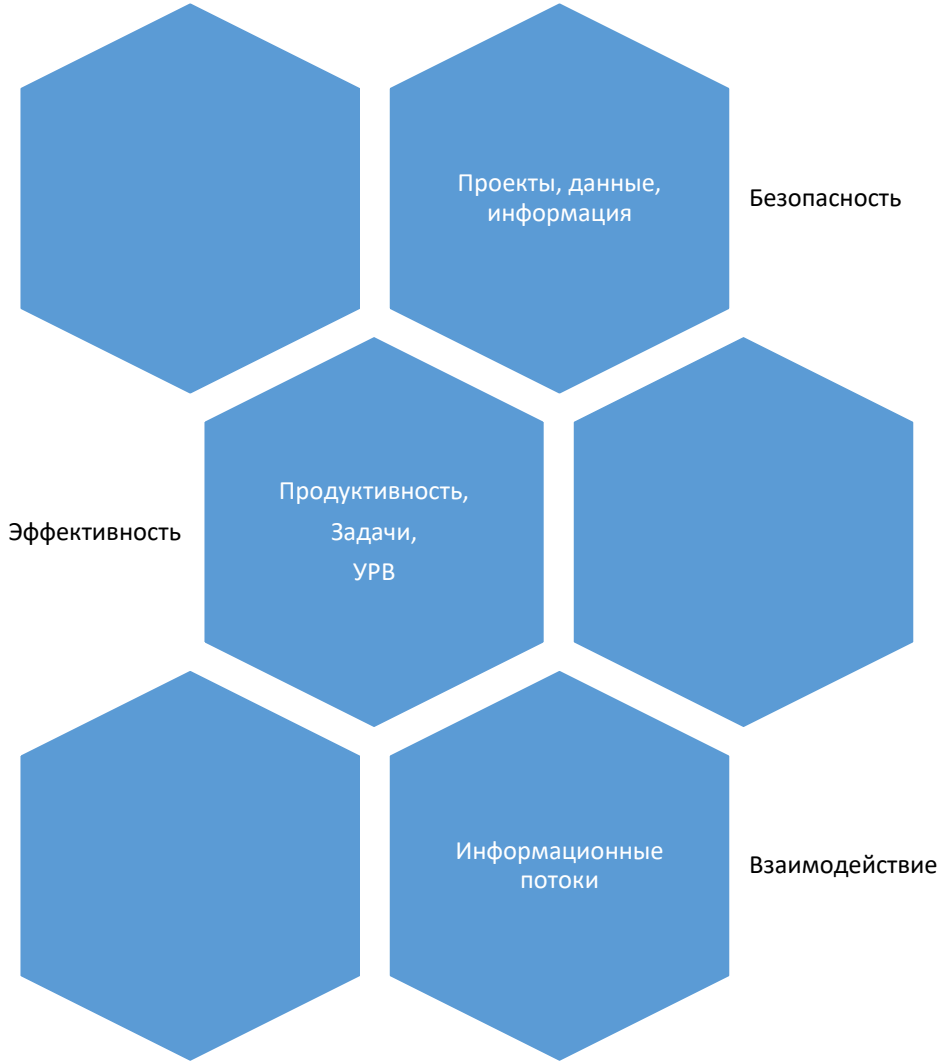
Контроль проектов



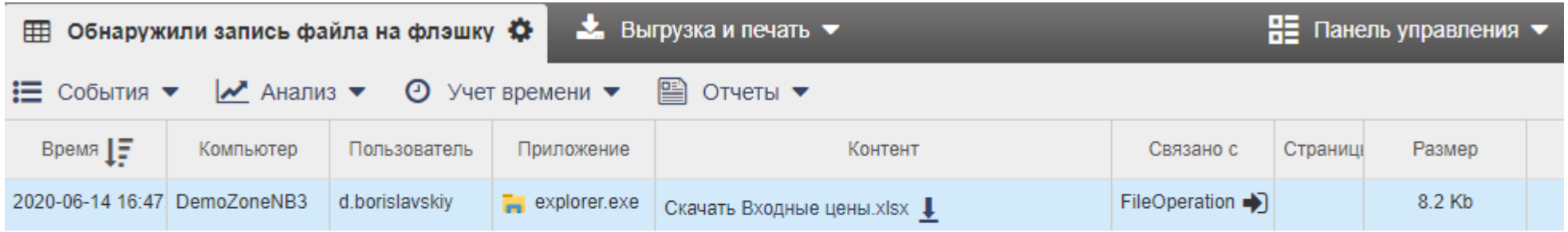


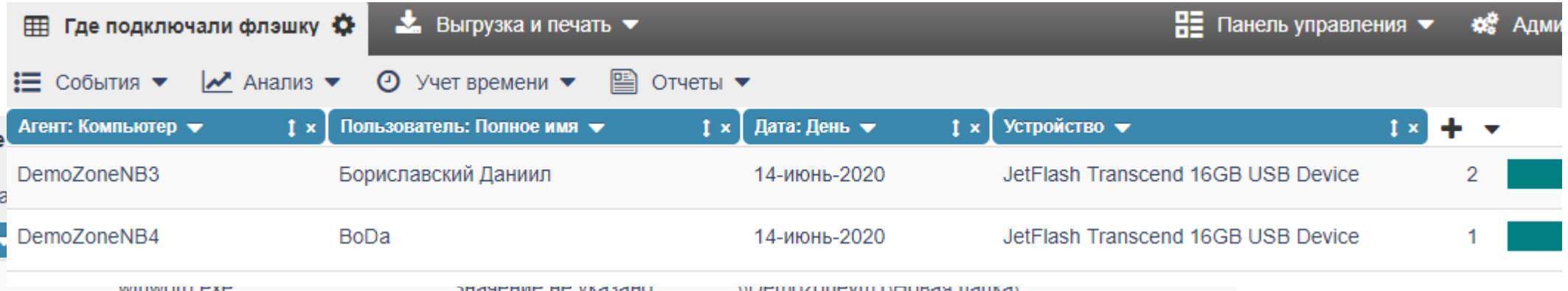
puter name	Account	Время активности	Application	Subdomain	Window title
rt-om.local	ph.vochmincev	48s	firefox.exe	demozona.staffcop.su	Staffcop Enterprise — Mozilla Firefox
rt-om.local	ph.vochmincev	1s	explorer.exe		Переключение задач
rt-om.local	ph.vochmincev	11s	bitrix24.exe		Bitrix24
2021-04-15 14:08:39	Stat	support-01.atom.local	ph.vochmincev	2s	skype.exe		Skype [4]
2021-04-15 14:08:37	Stat	support-01.atom.local	ph.vochmincev	1s	thunderbird.exe		Spam - YA ph.vochmincev@staffcop.ru - Mozilla Thunderbird
2021-04-15 14:08:30	Stat	support-01.atom.local	ph.vochmincev	7s	lightshot.exe		
2021-04-15 14:08:05	Stat	support-01.atom.local	ph.vochmincev	25s	thunderbird.exe		Входящие - YA ph.vochmincev@staffcop.ru - Mozilla Thunderbird
2021-04-15 14:07:47	Stat	support-01.atom.local	ph.vochmincev	17s	thunderbird.exe		Входящие - YA ph.vochmincev@staffcop.ru - Mozilla Thunderbird
2021-04-15 14:06:54	Stat	support-01.atom.local	ph.vochmincev	51s	firefox.exe	demozona.staffcop.su	Staffcop Enterprise — Mozilla Firefox

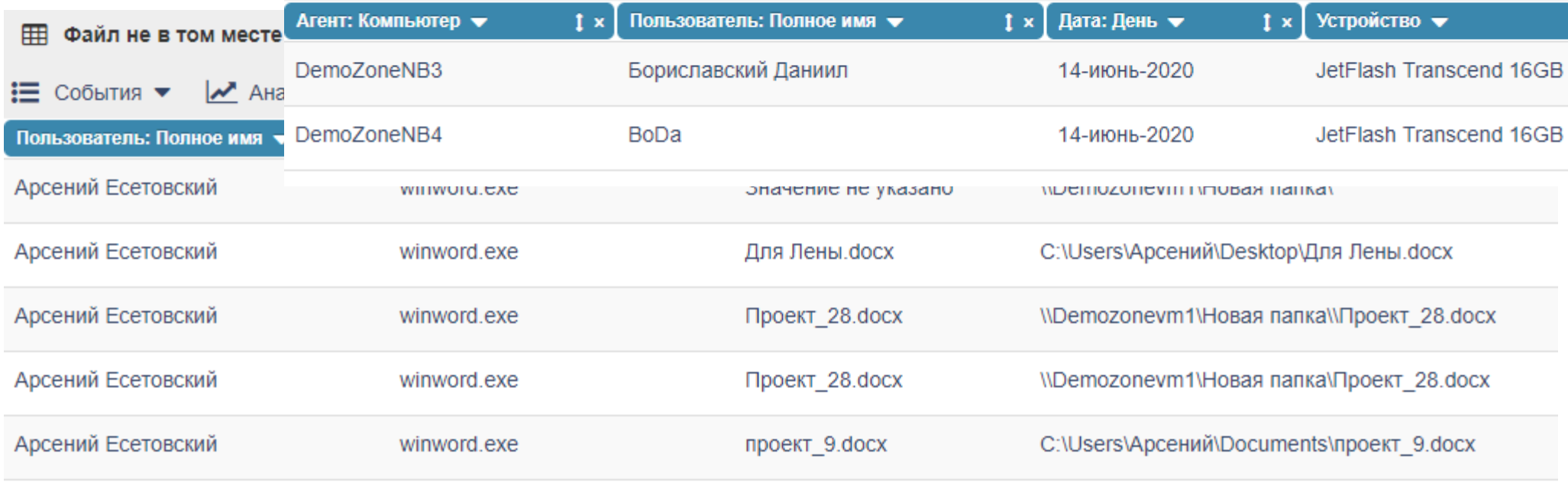
Чем мы в итоге можем помочь?



Расследование инцидентов







Контроль деятельности сотрудников.

Продуктивное время за период с 8 февраля 2021 по 8 февраля 2021

Отчёт отражает суммарное продуктивное\непродуктивное и нейтральное время пользователей на рабочих местах за выбранный период времени от общей активности пользователя

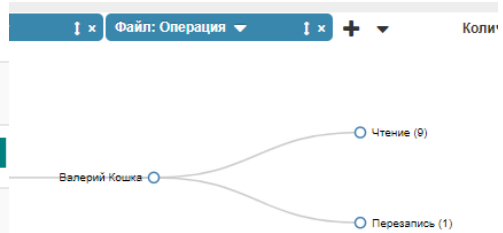
Продуктивное время | Непродуктивное время | Нейтральное время

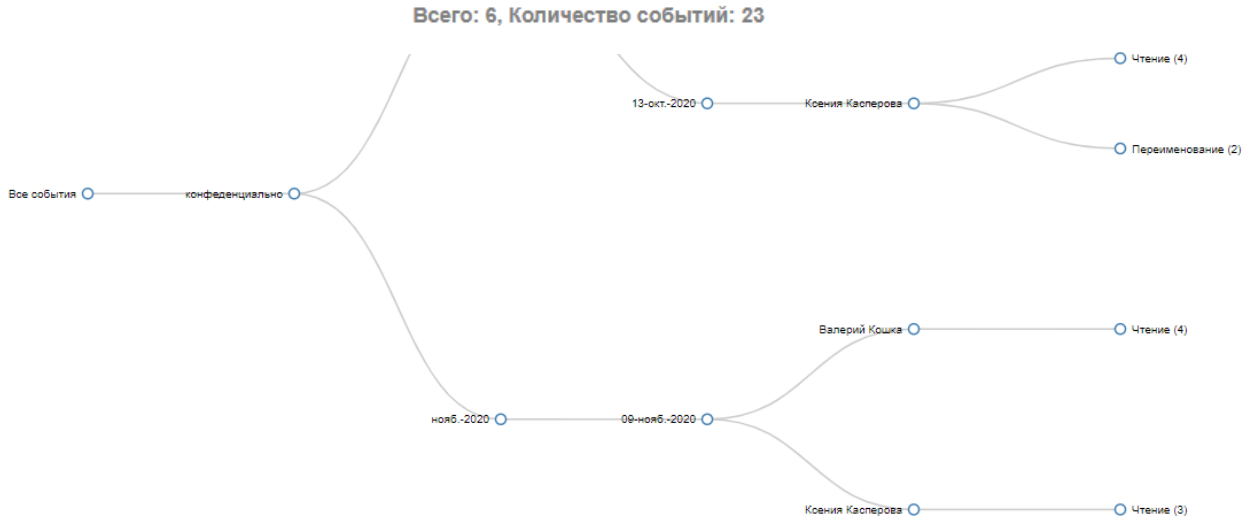
Сотрудник	Отработанное	Продуктивное	Непродуктивное	Нейтральное
По всем отделам (10)		28:45:10 (52,69 %)	1:56:43 (3,56 %)	23:52:35 (43,75 %)
▼ Техническая Поддержка (10)		28:45:10 (52,69 %)	1:56:43 (3,56 %)	23:52:35 (43,75 %)
Максим		5:15:41 (61,05 %)	0:01:45 (0,34 %)	3:19:37 (38,61 %)
Даниил		4:49:46 (66,08 %)	0:36:09 (8,24 %)	1:52:37 (25,68 %)
Владимир		4:40:12 (60,74 %)	0:00:00 (0,0 %)	3:01:07 (39,26 %)
Юрий		4:28:38 (78,15 %)	0:00:00 (0,0 %)	1:15:06 (21,85 %)
Сергей		3:16:07 (47,13 %)	0:00:00 (0,0 %)	3:40:00 (52,87 %)
Филипп		2:35:04 (48,51 %)	1:12:01 (22,53 %)	1:32:36 (28,97 %)
Александр		1:54:38 (25,55 %)	0:00:16 (0,06 %)	5:33:41 (74,39 %)
Дмитрий		1:29:52 (33,0 %)	0:00:00 (0,0 %)	3:02:27 (67,0 %)
Анатольевич		0:14:54 (36,56 %)	0:00:00 (0,0 %)	0:25:51 (63,44 %)

Начало	Окончание	Общее время	Активное	Простой	Опоздание	Сверхурочные	Продуктивное	Непродуктивное	Нейтральное
10:24:50	20:07:58	8:43	6:48	1:54	1:24	0:18	4:46	0:01	1:59
9:25:52	18:31:41	9:05	7:02	2:03	1:25	1:19	4:16	0:28	1:33

Метки на файлы

Файл: Метка	Дата: Месяц	Дата: День	Пользователь: Полное имя	Файл: Операция	Количество событий
конфеденциально	нояб.-2020	09-нояб.-2020	Валерий Кошка	Чтение	4
конфеденциально	нояб.-2020	09-нояб.-2020	Ксения Касперова	Чтение	3
конфеденциально	окт.-2020	12-окт.-2020	Валерий Кошка	Перезапись	1
конфеденциально	окт.-2020	12-окт.-2020	Валерий Кошка	Чтение	9
конфеденциально	окт.-2020	13-окт.-2020	Ксения Касперова	Переименование	2
конфеденциально	окт.-2020	13-окт.-2020	Ксения Касперова	Чтение	4





Сканы паспортов и номера кредитных карт – инцедент?

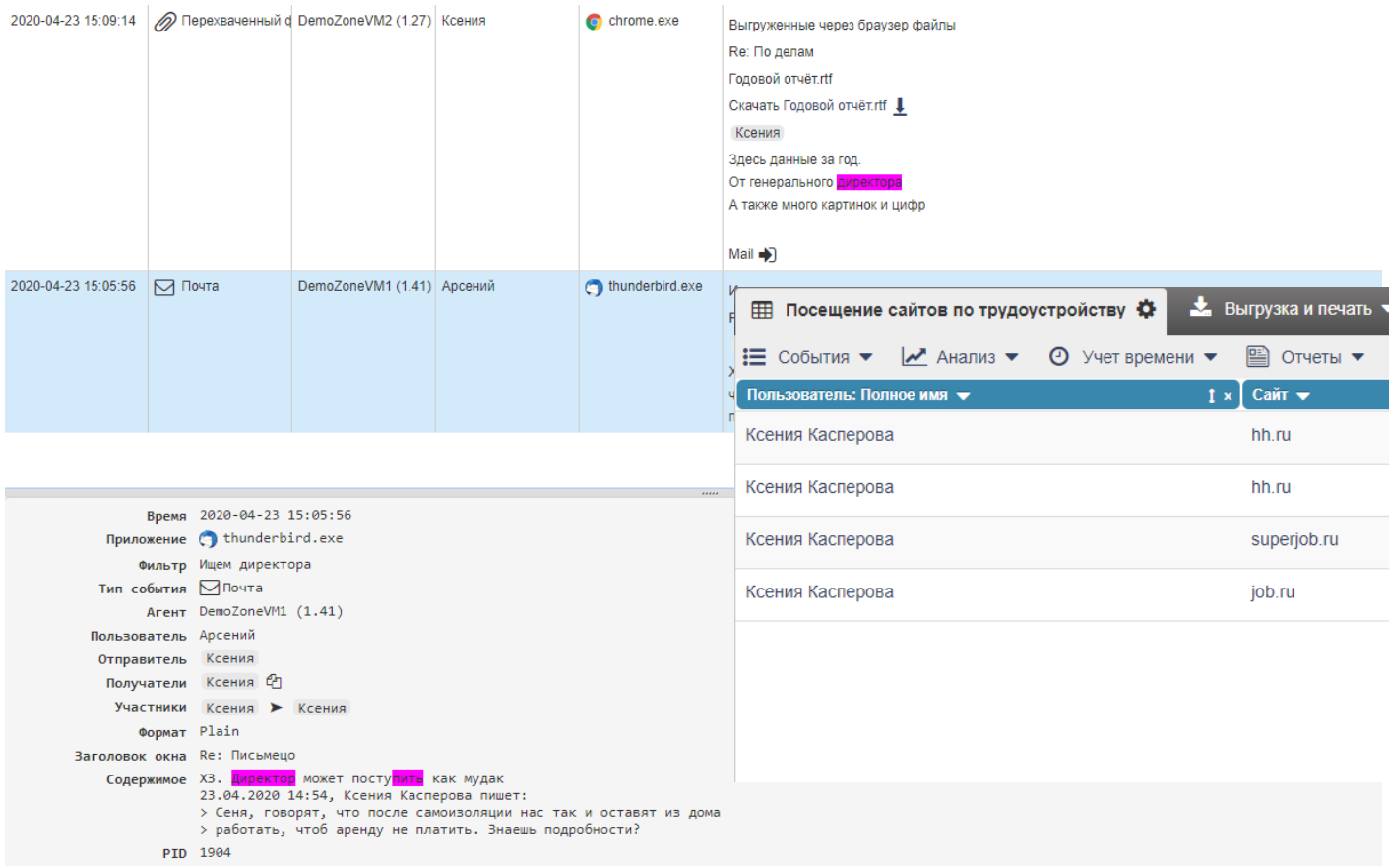
Время 2020-11-17 11:48:15

Фильтр Сервер распознаваний

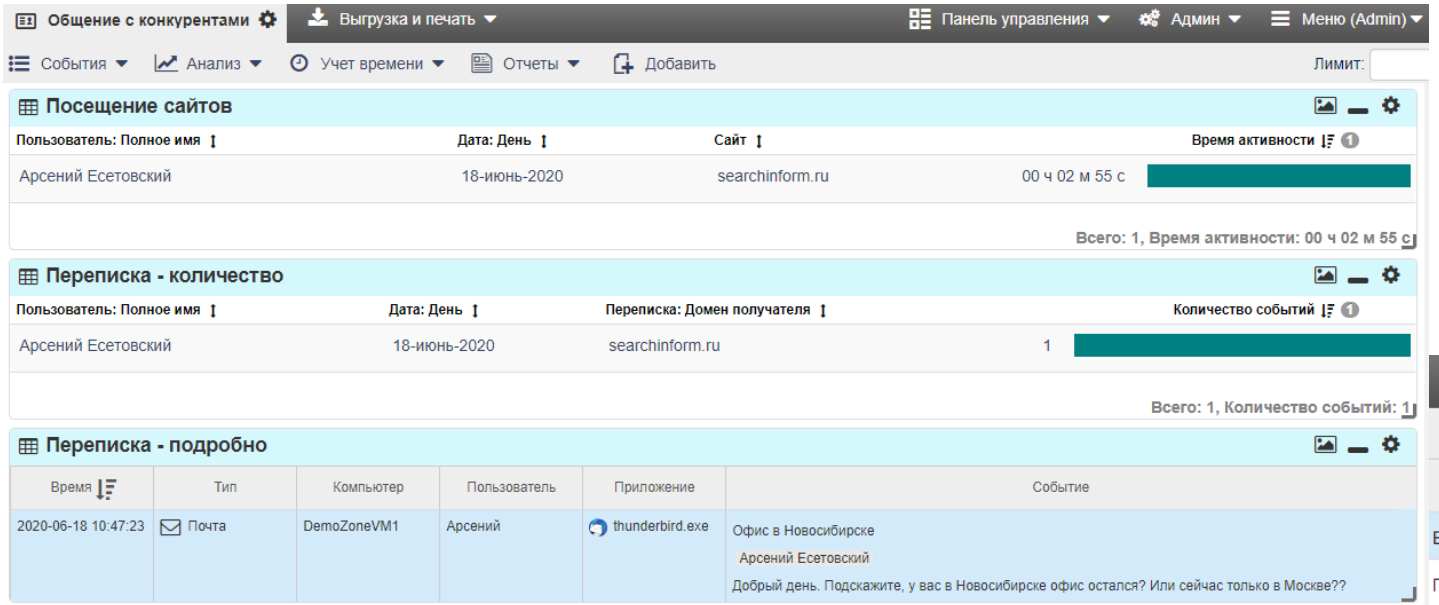
Контент

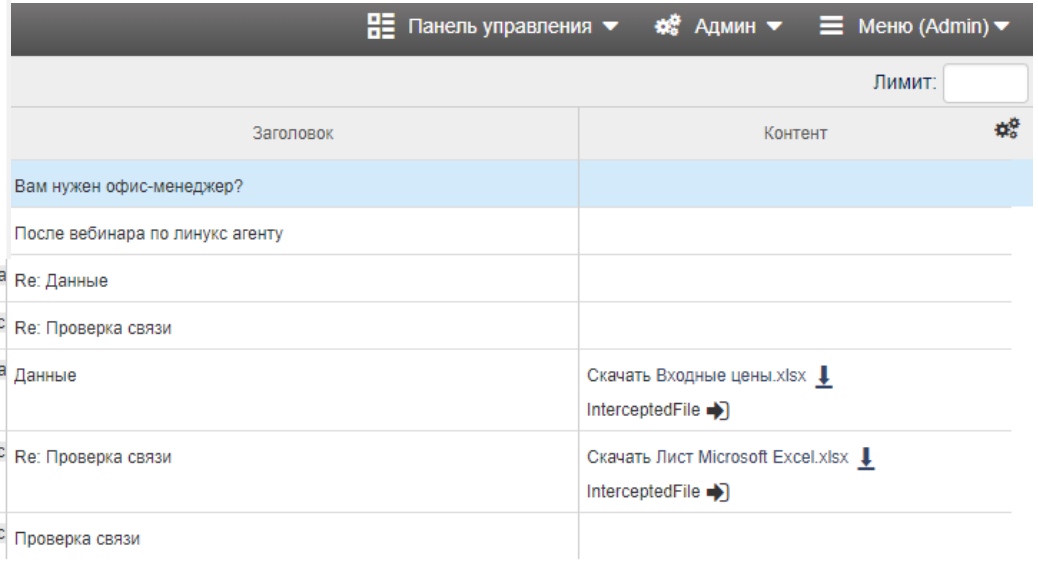
				Скачать Documents.7z
	DemoZoneVM2	Ксения	chrome.exe	Кредитные карты Ксения Касперова Сначала деньги, потом остальное 4276160971368577 сбер вс, 14 июн. 2020 г. в 16:06, Даниил Борославский <d.borislavskiy@staffcop.ru>: норм, давай ещё вс, 14 июн. 2020 г. в 16:01, Ксения Касперова <kkasperova522@gmail.com>: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

Отслеживание поиска работы и эмоциональная обстановка в офисе.



Контроль переписки - общение с конкурентами.





2020-06-14 16:08:1	DemoZoneVM2	Ксения	Ксения Касперов	Бориславский Да	
2020-06-14 16:05:0	DemoZoneVM2	Ксения	Ксения Касперов	Арсений Есетовс	
2020-06-14 16:01:1	DemoZoneVM2	Ксения	Ксения Касперов	Бориславский Да	
2020-06-14 15:45:3	DemoZoneVM2	Ксения	Ксения Касперов	Арсений Есетовс	
2020-06-14 15:44:1	DemoZoneVM2	Ксения	Ксения Касперов	Арсений Есетовс	

Теневые копии файлов – Поиск по атрибутам и анализ содержимого.

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

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

Фильтр: *цен* в перехваченных файлах

Свойства | Уведомления | Фильтр

Конструктор | Сложный запрос | Код фильтра

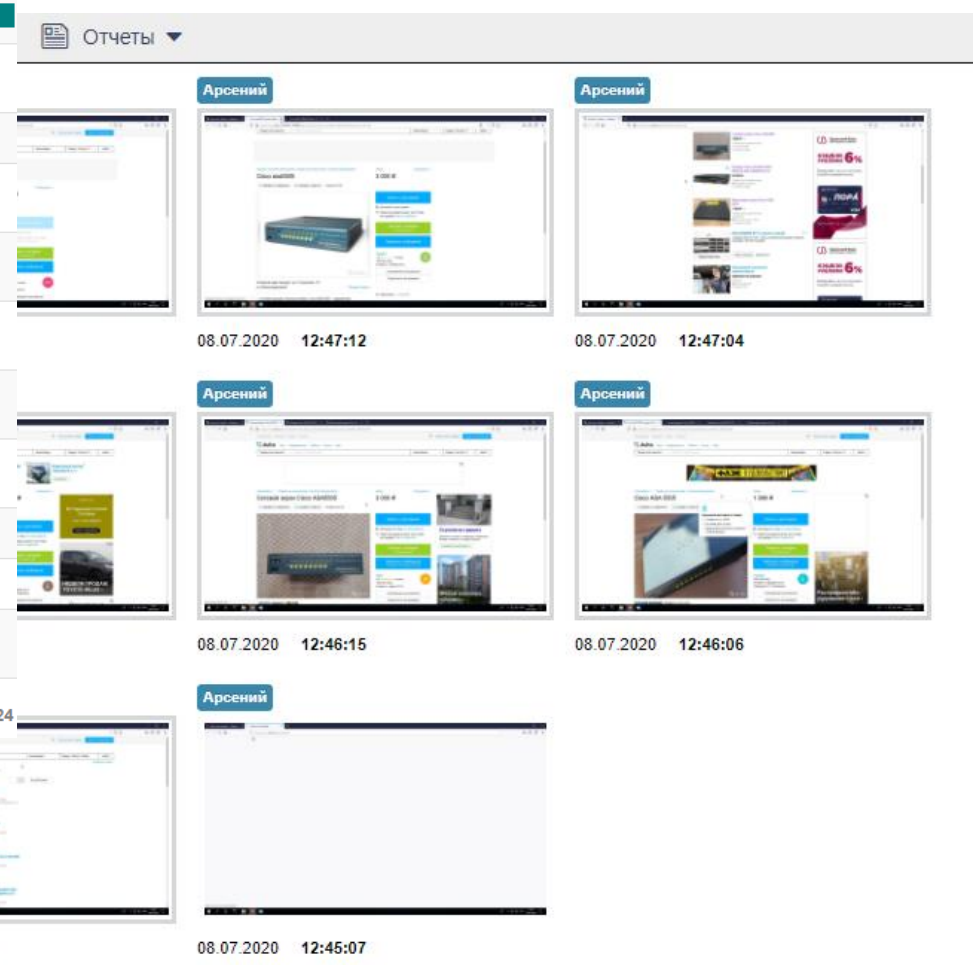
И | + Условие | Группа условий

Файл | Имя файла | Содержит | цен

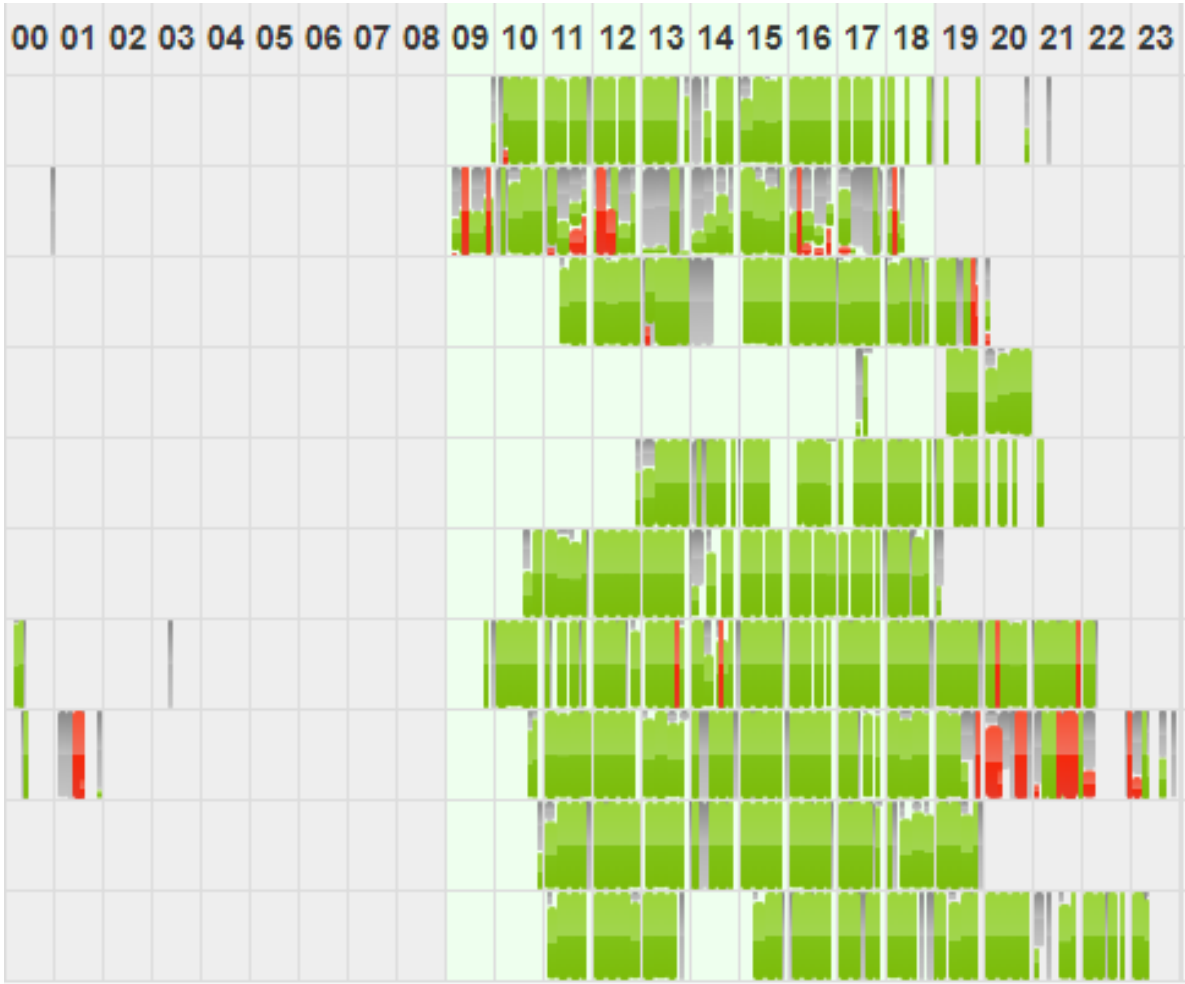
Доски объявлений – продажа оборудования.

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 электроника | Авито - Mozilla Firefox	2
Арсений Есетовский	avito.ru	Cisco asa5505 купить в Барнауле с доставкой | Бытовая электроника | Авито - Mozilla Firefox	2
Арсений Есетовский	avito.ru	Cisco asa 5505 купить в Новосибирске с доставкой | Бытовая электроника | Авито - Mozilla Firefox	2
Арсений Есетовский	avito.ru	Cisco ASA 5505 купить в Новосибирске с доставкой | Бытовая электроника | Авито - Mozilla Firefox	2
Арсений Есетовский	avito.ru	Сетевой экран Cisco ASA5505 купить в Новосибирске с доставкой | Бытовая электроника | Авито - Mozilla Firefox	2
Арсений Есетовский	avito.ru	Межсетевой экран Cisco ASA 5510 купить в Новосибирске с доставкой | Бытовая электроника | Авито - Mozilla Firefox	2
Арсений Есетовский	avito.ru	Продам Cisco ASA5510-SEC-BUN-K9, WS-C2960PD-8TT-I купить в Новосибирске | Бытовая электроника | Авито - Mozilla Firefox	2
Арсений Есетовский	avito.ru	Авито — объявления в Новосибирске — Объявления на сайте Авито - Mozilla Firefox	2
Арсений Есетовский	avito.ru	Cisco asa5505 купить в Барнауле с доставкой | Бытовая электроника | Авито	1
Арсений Есетовский	avito.ru	Cisco 2821 ASA5510 Cisco 1760 Juniper srx100 купить в Кемерово с доставкой | Бытовая электроника | Авито	1

Всего: 11, Количество событий: 24



Учёт рабочего времени и его анализ



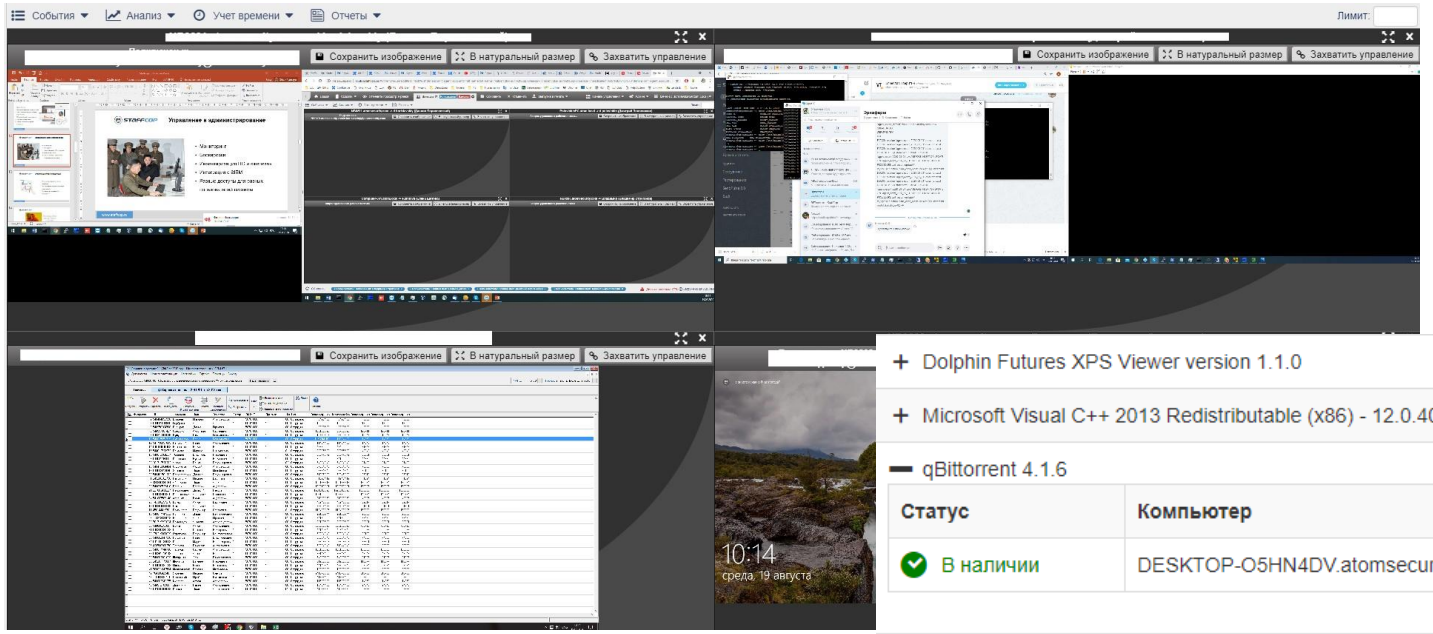
Начало	Окончание	Общее время	Активное	Простой
9:54:29	21:15:32	11:21:03	6:14:19	5:06:44
9:07:06	18:22:55	9:15:49	8:34:07	0:41:42
11:20:35	20:01:01	8:40:26	7:04:36	1:35:50
17:23:27	20:57:18	3:33:51	1:41:48	1:52:03
12:53:25	21:14:43	8:21:18	3:46:49	4:34:29
10:35:44	19:10:12	8:34:28	7:17:27	1:17:01
0:10:40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

Управление и администрирование

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

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)

Почему мы?

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.

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

STAFFCOP

Тестируйте бесплатно до 3-х месяцев на парке машин любого размера.

Полнофункциональная версия. Техническое сопровождение проекта на всем протяжении.

Быстро

Развертывание пилотного проекта обычно занимает не более одного дня

Легко

Требуется минимум усилий и ресурсов для запуска StaffCop Enterprise

Комплексно

Вы сможете оценить сразу весь комплекс решаемых задач и принять правильное решение

Благодарю за внимание!

Чеплиёв Максим
Специалист отдела аналитики
ООО Атом Безопасность

+7(499)6382809 доб. 238
m.chepliev@staffcop.ru