Контроль действий сотрудников в информационной среде компании.

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»
- ~100 серверных компонентов в месяц; ~ 94 000 АРМ за 2019-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?

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

Зачем нужен контроль над инф.потоками?

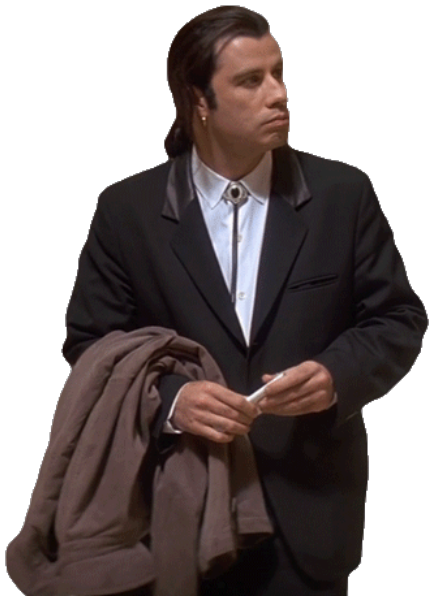
Лимит:

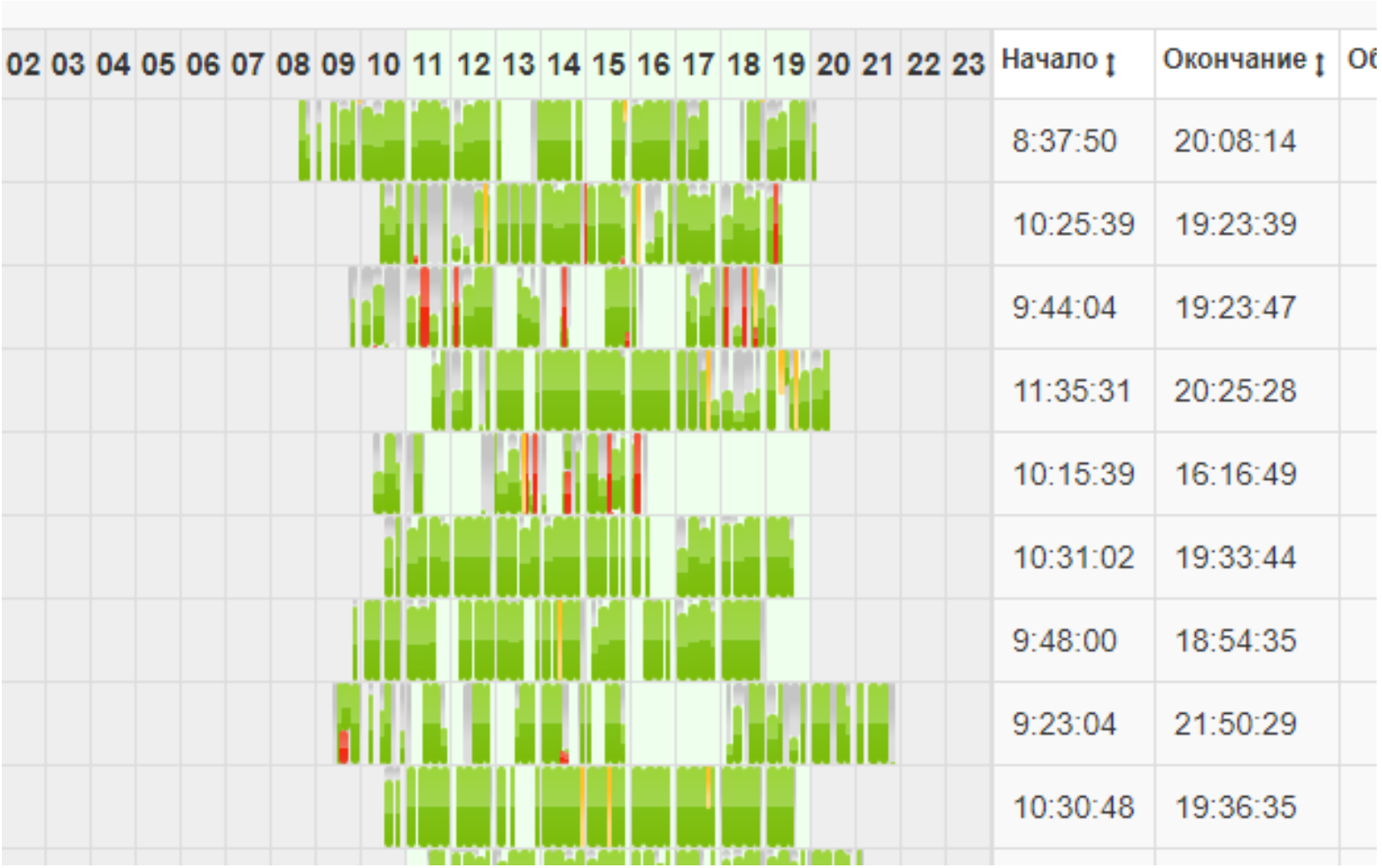
Учёт рабочего времени за период с 24 марта 2020 по 24 марта 2020

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 над инф.потоками?





Дисциплина Активность Продуктивность

Зачем нужен контроль над инф.потоками?

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 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 Firefo x	2
Арсений Есетовский	avito.ru	Cisco ASA 5505 купить в Новосибирске с доставкой | Бытовая электроника | Авито - Mozilla Firefo x	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 | А вито - Mozilla Firefox	2
Арсений Есетовский	avito.ru	Продам Cisco ASA5510-SEC-BUN-K9, WS-C2960PD-8TT-I купить в Новосибирске | Бытовая элект роника | Авито - Mozilla Firefox	2
Арсений Есетовский	avito.ru	Авито — объявления в Новосибирске — Объявления на сайте Авито - Mozilla Firefox	2
Арсе		вкой | Бытовая электроника | Авито	1
Арсе		rx100 купить в Кемерово с доставкой | Бытовая электро	1

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 подойдёт. Как это работает

Показать телефон

Написать сообщение
Отвечает около 30 минут

5,0 ★★★★★ 8 отзывов

52 объявления пользователя

Отчеты

Всего: 11, Количество событий: 24

Арсений

08.07.2020 12:47:12

Арсений

08.07.2020 12:47:04

Арсений

08.07.2020 12:46:15

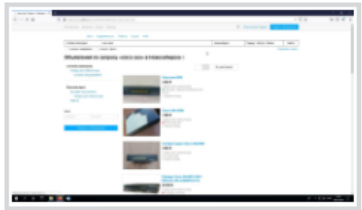
Арсений

08.07.2020 12:46:06

Арсений

08.07.2020 12:45:49

Арсений



08.07.2020 12:45:22

Арсений

08.07.2020 12:45:07

Зачем нужен контроль над инф.потоками?

Общение с конкурентами | Выгрузка и печать | Панель управления | Admin | 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

Всего: 1, Время активности: 00 ч 02 м 55 с

Переписка - количество

Пользователь: Полное имя	Дата: День	Переписка: Домен получателя	Количество событий
Арсений Есетовский	18-июнь-2020	searchinform.ru	1

Всего: 1, Количество событий: 1

Переписка - подробно

Время	Тип	Компьютер	Пользователь	Приложение	Событие
2020-06-18 10:47:23	Почта	DemoZoneVM1	Арсений	thunderbird.exe	Офис в Новосибирске Арсений Есетовский Добрый день. Подскажите, у вас в Новосибирске офис остался? Или сейчас только в Москве??

Панель управления | Admin | Меню (Admin)

Лимит:

					Заголовок	Контент
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	

Зачем нужен контроль над инф.потоками?

ФСТЭК России

Федеральная служба по техническому и экспортному контролю

приказ ведомства №35 от 20.02.2020

об обеспечении безопасности КИИ

STAFFCOP

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

учет рабочего времени

эффективность персонала

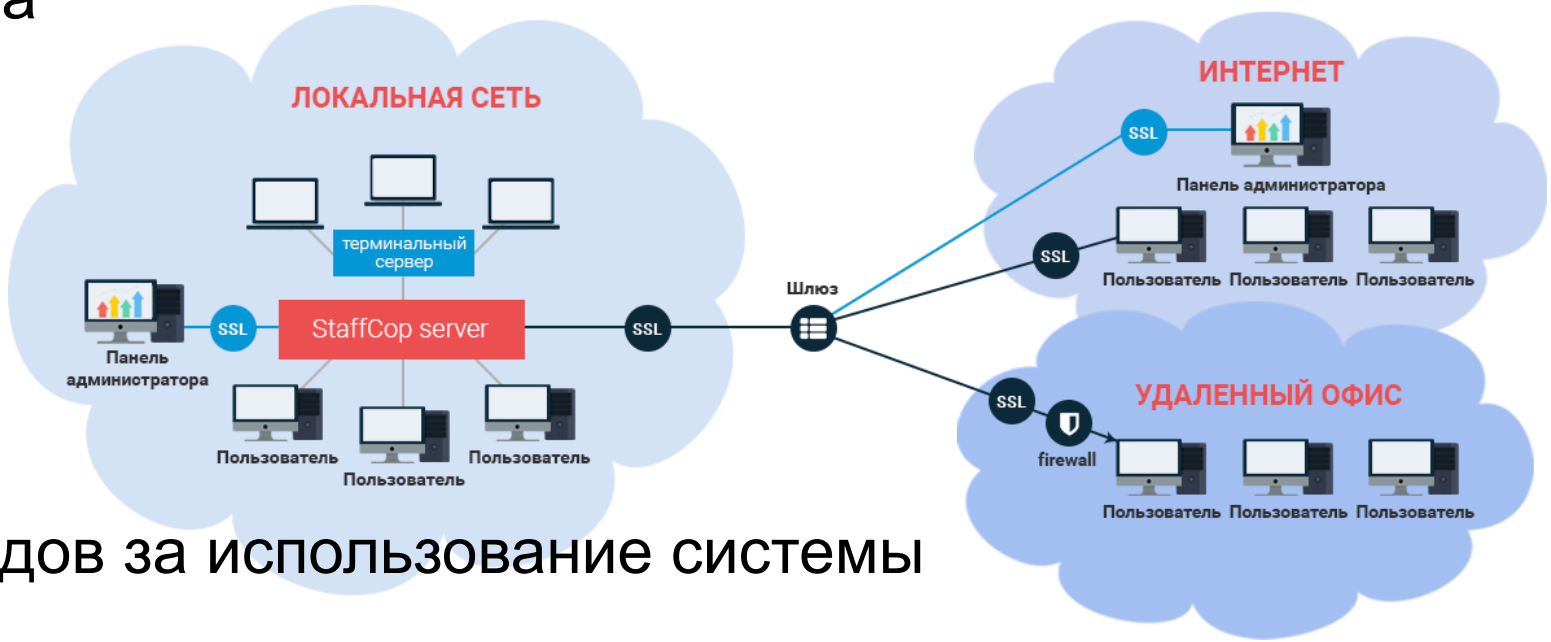
информационная безопасность

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

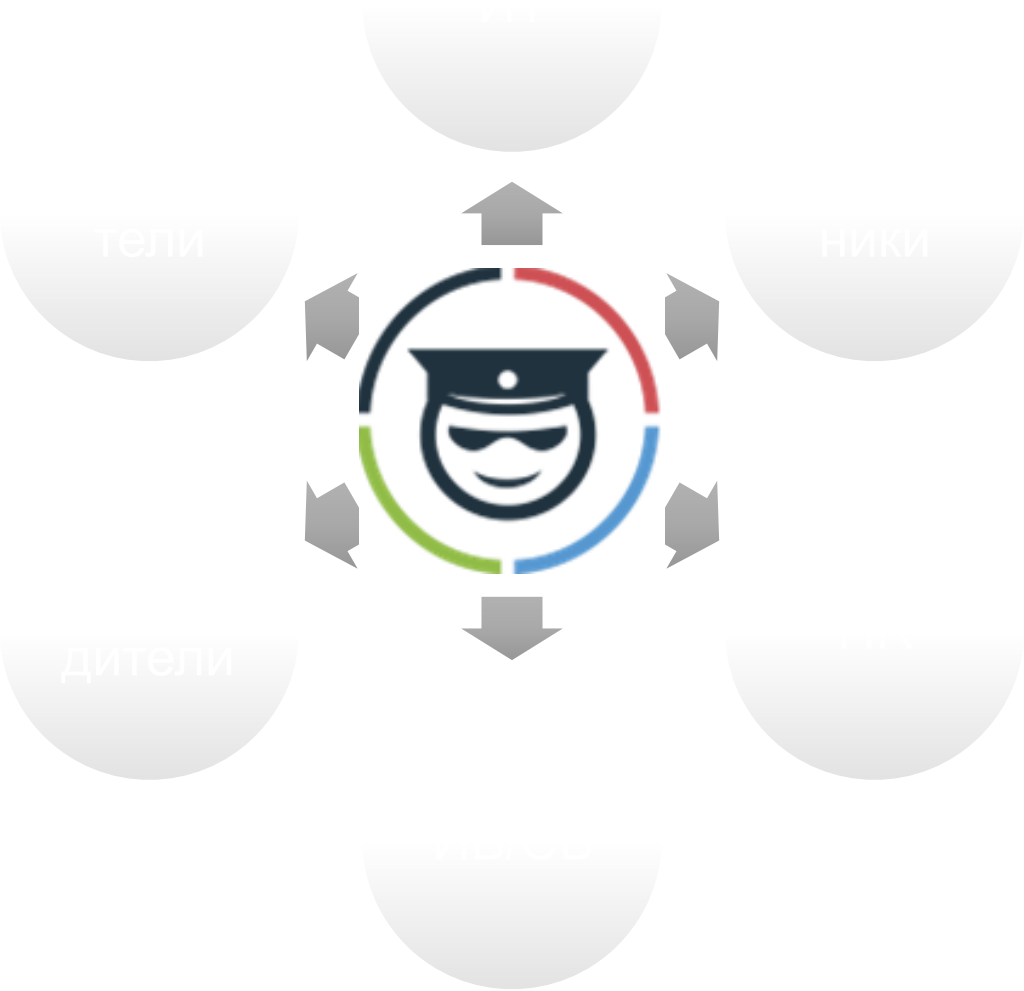
Расследование инцидентов ИБ

- 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

Потребители



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

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

Аспекты внедрения: правовые

- **№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: технические

- 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.

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!

Даниил Бориславский
Руководитель аналитического отдела
ООО Атом Безопасность

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