Контроль над информационными потоками и действиями сотрудников

Кандыбович Дмитрий
Директор по развитию
ООО Атом Безопасность
dk@staffcop.ru

- Более 10 лет разработки приложений контроля сотрудников;
- Академгородок, Новосибирск, резиденты Технопарка и Сколково;
- Высокотехнологичная компания, ~70 сотрудников.
- Продано ~1300 серверных компонентов, ~ 66 000 АРМ за 2019-й год.
- Продано ~2200 серверных компонентов, ~ 171 000 АРМ за 2020-й год.
- Продано ~3100 серверных компонентов, ~ 230 000 АРМ за 2021-й год.

академпарк
Технопарк Новосибирского Академгородка
BIS SUMMIT 2018
infosecurity RUSSIA
Минкомсвязь России
Федеральная служба по техническому и экспортному контролю
Sk Сколково
CERTIFIED AM TEST LAB

STAFFCOP

Система мониторинга для расследования инцидентов
и контроля работы сотрудников

Учет рабочего времени

Эффективность персонала

Информационная безопасность

Расследование и 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

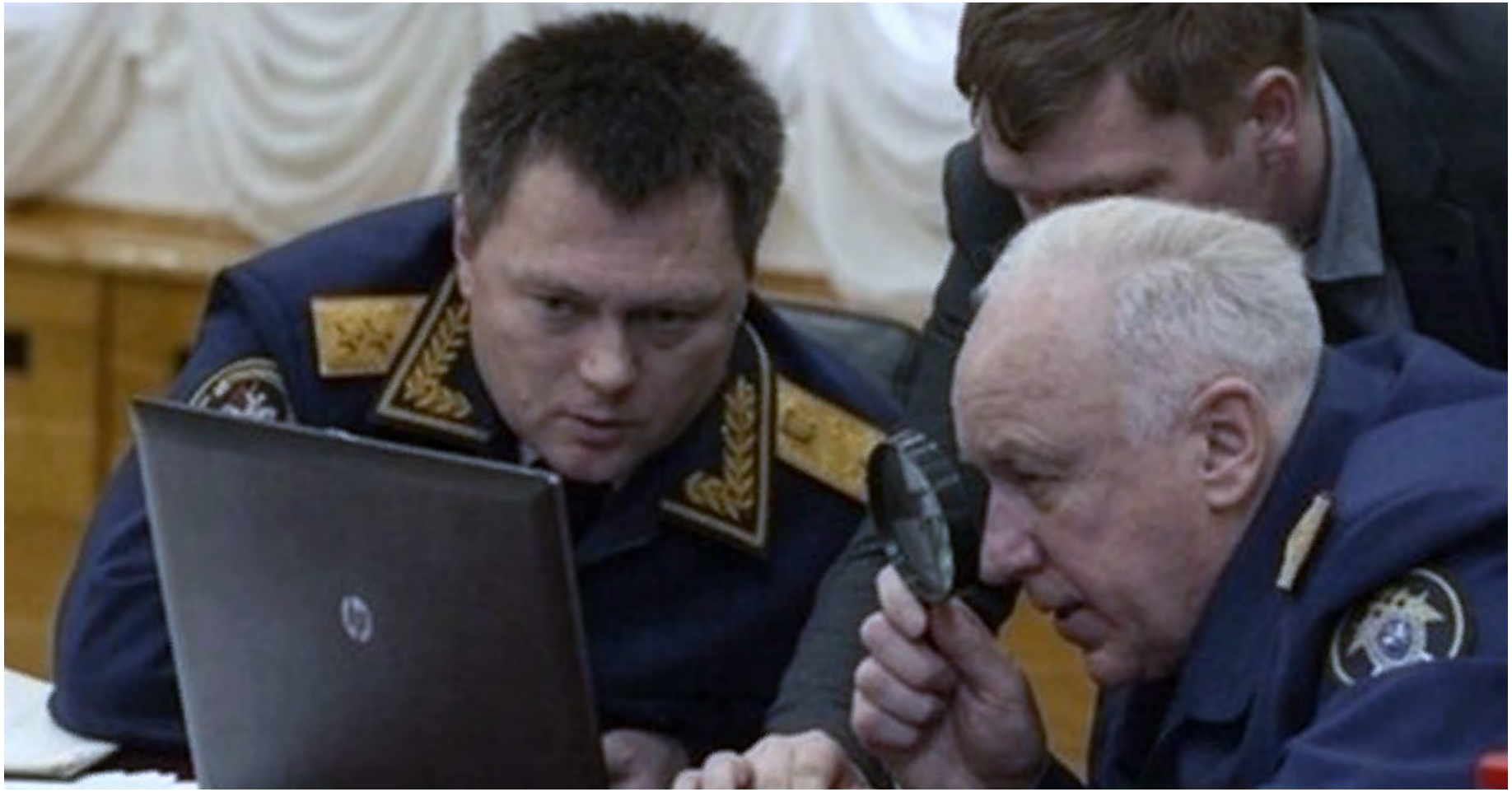
- Удалённая установка агента
- 100 сотрудников <> 6CPU, 16RAM
- Локальные блокировки

- Нет дополнительных расходов за использование системы

Что нужно бизнесу?

- Расследовать инциденты
- Понимание что делает сотрудник за ПК (или не делает)
- Знать что происходит на удалёнке (и в офисе)
- Знать к чему готовиться
- Помощь IT
- Чтоб не дорого и честно
- Польза всем подразделениям
- **Выполнить требования регуляторов**
- **Снизить ущерб от санкций; использовать отечественное ПО**

Хочу расследовать инциденты

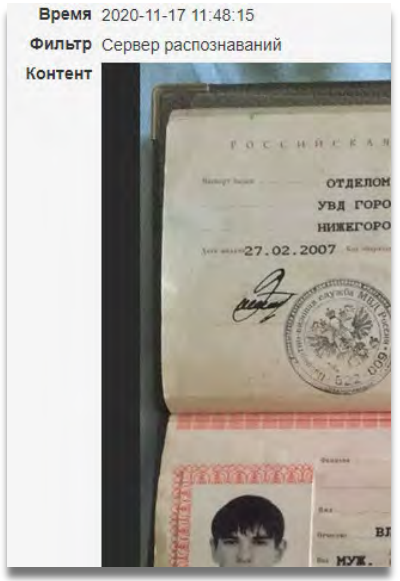


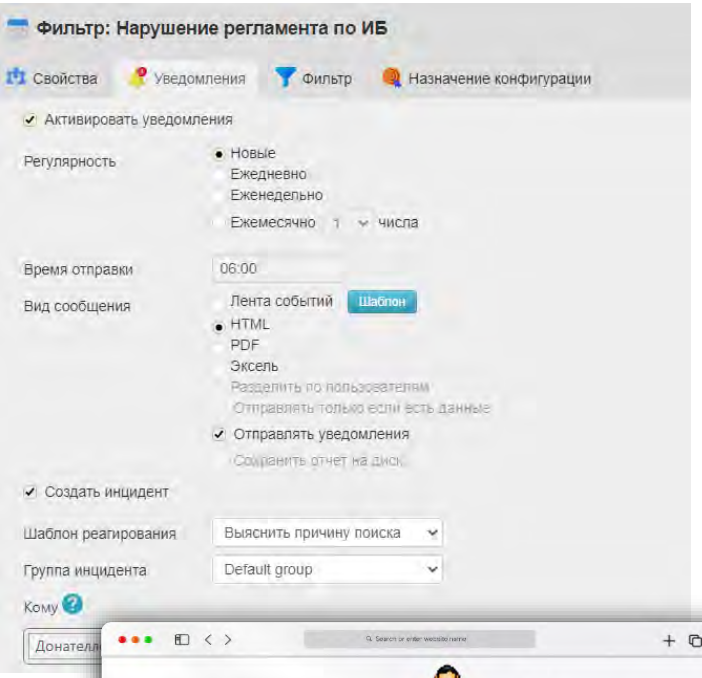
Хочу расследовать инциденты

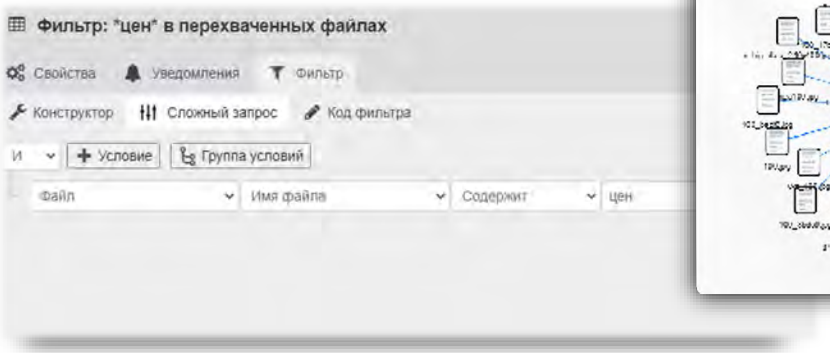
- Цифровой след
- Поиск по атрибутам\теневые копии файлов
- Поиск по содержимому
- OCR
- Словари и регулярные выражения
- Нейросети

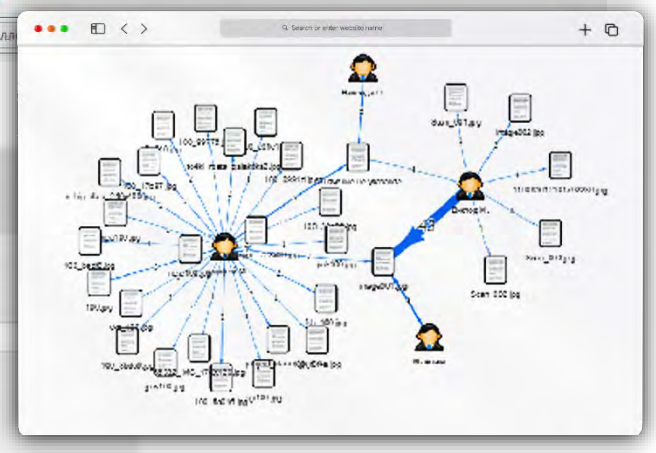
Расследование инцидентов ИБ

- Система оповещений
- Гибкая система настройки фильтров
- Графы взаимосвязей
- Метки для файлов
- Изменение конфигурации контроля при наступлении определённого события
- Защита от массового копирования
- Нейронная сеть распознавания изображений









Хочу понимать что делает сотрудник за ПК (или не делает)

Хочу понимать что делает сотрудник за ПК (или не делает)

- Метаданные
- Информация
- События системы
- Работа с данными

Тотальный контроль действий за ПК

Инвентаризация «железа» и ПО

Снимки с веб-камер

Мониторинг посещенных сайтов и поисковых запросов

Мониторинг действий в социальных сетях

Контроль email-переписки

Контроль USB и CD

Мониторинг доступа к файлам

Сканирование хранящихся файлов

Скриншоты и запись видео рабочего стола

Подключение к рабочему столу

Контроль печати

Перехват сообщений в мессенджерах

Кейлоггер

Запись аудио с микрофона и колонок

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

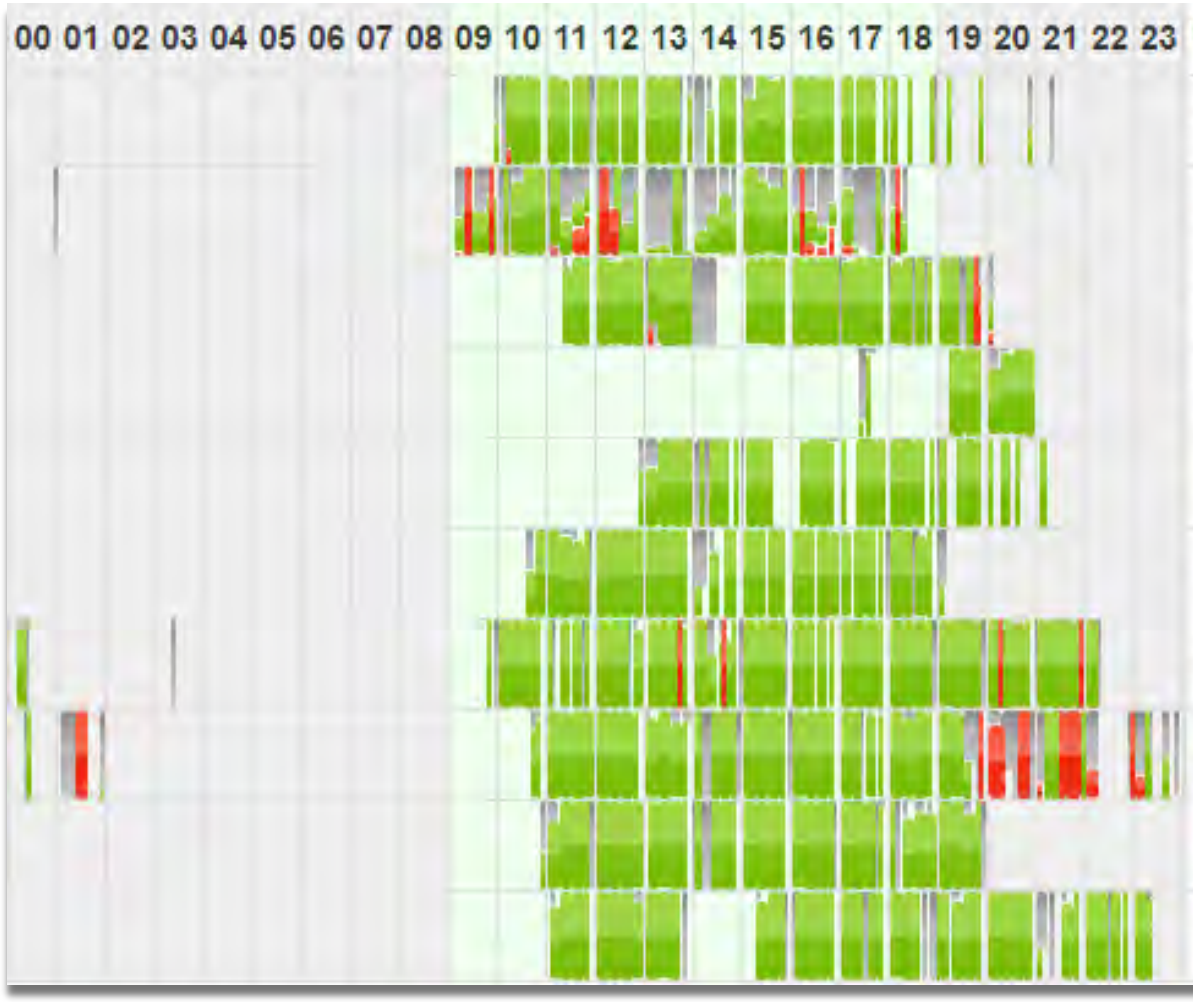
Теневое копирование файлов
— из электронной почты
— со съемных носителей
— переданных через интернет
— отправленных на печать

Хочу знать что происходит на удалёнке (и в офисе)

Хочу знать что происходит на удалёнке (и в офисе)

- Дисциплина
- Активность
- Продуктивность
- Разные группы контроля
- Разный уровень доступа
- Задачи для ИБ, СБ, УРВ

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

Хочу знать к чему готовиться

Хочу знать к чему готовиться

- Поиск работы
- Атмосфера в коллективе
- Заберу своё с собой
- Бонусный пакет «на дорожку»
- PAM, DCAP

Аналитические возможности

- Архив данных
- Конструктор многомерных отчетов
- Поиск по словам и регулярным выражениям
- Множество графов и диаграмм
- Синхронизация данных с AD

Помощь IT

Помощь IT

- Нарушение регламентов ИТ
- Инвентаризация ПО и оборудования
- Удалённое управление
- Аномалии
- Блокировки внешних устройств
- Форензика*

Управление и администрирование

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

Хочу чтобы полезно всем было

Хочу чтоб не дорого и честно

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

Обязан выполнить требования регуляторов

Федеральная служба по техническому и экспортному контролю

приказ ведомства №35 от 20.02.2020

об обеспечении безопасности КИИ

ГОСТ Р 57580.1-2017

Безопасность финансовых (банковских) операций.

Банк России

Центральный банк Российской Федерации

Снизить ущерб от санкций; использовать отечественное ПО

Технологии сервера:

open source initiative

PostgreSQL

ASTRA LINUX®

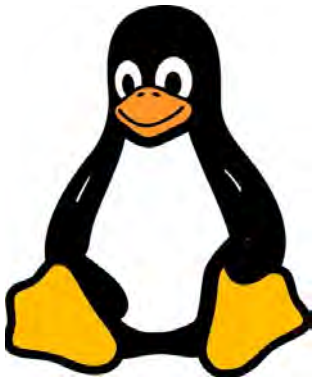
OS рабочих ПК и АРМ:

ASTRA LINUX®

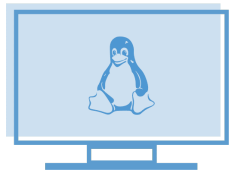
base alt

РЕДОС

ROSA



Преимущества Staffcop Enterprise



На opensource решениях, не требует дополнительного платного ПО.

Цена.

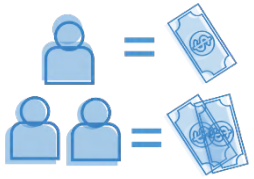
Входим в реестр отечественного ПО и имеет сертификат ФСТЭК.

Небольшие требования к ресурсам для сервера. Единая web-консоль.

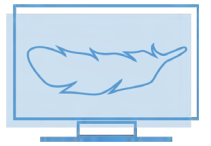
Настраиваемые отчёты и OLAP.

Не блокирует работу бизнеса.

Решает задачи разных подразделений



Единое решение и гибкая политика лицензирования.



Лёгкий и функциональный агент.

Обоснование для внедрения

Политика лицензирования и стоимость

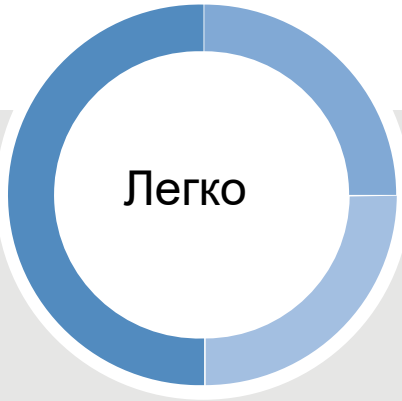
Количество компьютеров	Лицензия на 12 месяцев	Лицензия на 3 месяца
5–25	3 350 ₽ / 1 ПК	1 117 ₽ / 1 ПК
26–50	3 150 ₽ / 1 ПК	1 050 ₽ / 1 ПК
51–150	2 990 ₽ / 1 ПК	997 ₽ / 1 ПК
151–250	2 890 ₽ / 1 ПК	963 ₽ / 1 ПК
251–500	2 790 ₽ / 1 ПК	930 ₽ / 1 ПК
501–1000	2 690 ₽ / 1 ПК	897 ₽ / 1 ПК
1000+	2 590 ₽ / 1 ПК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

Тестируйте бесплатно на парке АРМ любого размера.

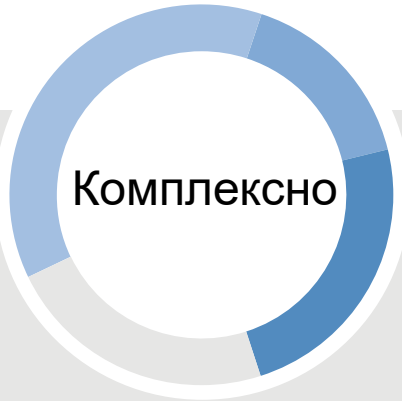
Полнофункциональная версия.

Техническое сопровождение проекта на всём протяжении тестирования.

Развертывание пилотного проекта обычно занимает не более одного дня



Требуется минимум усилий и ресурсов для запуска Staffcop Enterprise



Вы сможете оценить сразу весь комплекс решаемых задач Принять правильное решение

Кандыбович Дмитрий
Директор по развитию
ООО Атом Безопасность

+79139152137
dk@staffcop.ru