staffcop®

Расследование инцидентов
информационной безопасности

Контроль над информационными потоками и действиями сотрудников

Дмитрий Кандыбович

Директор по развитию
ООО «Атом Безопасность»

dk@staffcop.ru

О компании

Участник

академпарк

ASTRA LINUX®

ФСТЭК России
Федеральная служба по техническому и экспортному контролю

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации

Минкомсвязь России

01 Более 10 лет разработки приложений контроля сотрудников

02 Академгородок, Новосибирск, резиденты Технопарка и Сколково

03 Высокотехнологичная компания, ~80 сотрудников

04 За 2020-й год продано:
~ 2200 серверных компонентов,
~ 171 000 АРМ

05 За 2021-й год продано:
~ 3100 серверных компонентов,
~ 230 000 АРМ

06 За 2022-й год продано:
~4300 серверных компонентов,
~ 340 000 АРМ

Зачем нужен контроль над информационными потоками?

01 Утечка информации

02 Работа на удаленке

03 Эффективность работы сотрудников

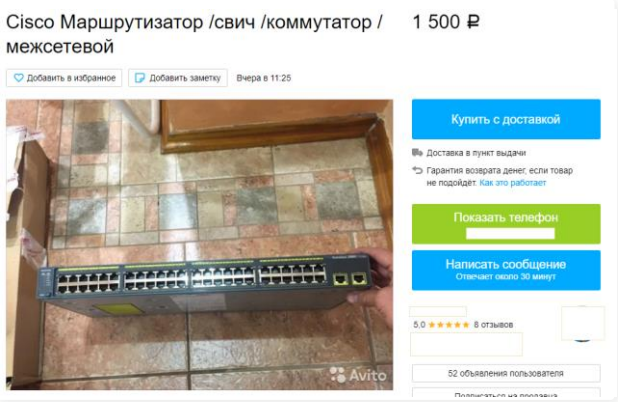
Банк России
Центральный банк Российской Федерации

ГОСТ Р 57580.1-2017
Безопасность финансовых (банковских) операций

Федеральная служба по техническому и экспортному контролю

Приказ ведомства №35 от 20.02.2020
Об обеспечении безопасности КИИ

04 Государственные требования

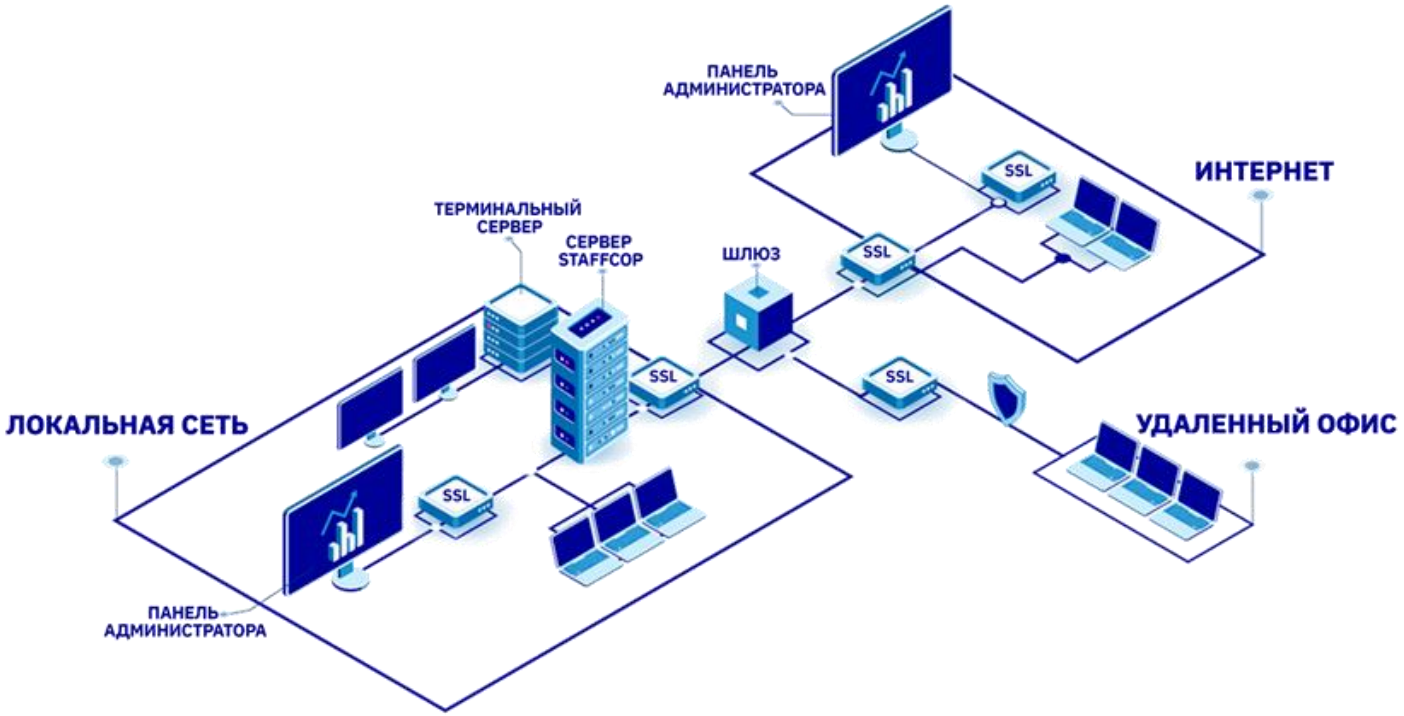


05 Мошенничество

06 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, 32RAM
- Локальные блокировки
- Нет дополнительных расходов за использованием системы
- Не требует платных лицензий, СТЭК отечественный, без рисков обслуживания



ubuntu PostgreSQL ASTRALINUX special edition

staffcop

Использование отечественного и независимого ПО

Технологии сервера:

open source initiative

ASTRA LINUX®

ClickHouse

PostgreSQL

OS рабочих ПК и АРМ:

ASTRA LINUX®

base alt

ROSA

РЕДОС

staffcop®

Основные функции

Снимки с web камеры

Скриншоты и запись видео с рабочего стола

Мониторинг посещенных сайтов

Контроль печати

Мониторинг действий в социальных сетях

Запись аудио с микрофона и колонок

Действия пользователей

Документы и файлы

Действия системы

Контроль почты

Перехват мессенджеров

Мониторинг доступа к файлам

Удаленное управление

Контроль съемных носителей

Инвентаризация железа и ПО

staffcop

Информационная безопасность

- Раннее обнаружение угроз ИБ
- Расследование инцидентов
- Анализ поведения пользователей

Эффективность работы персонала

- Оценка продуктивности сотрудников
- Мониторинг бизнес – процессов
- Учет рабочего времени

Администрирование рабочих мест

- Удаленное администрирование
- Инвентаризация компьютеров
- Индексирование файлов на ПК

Для кого?

Собственникам бизнеса

IT специалистам

ИБ специалистам

HR

staffcop

Аналитические возможности

01 Архив данных

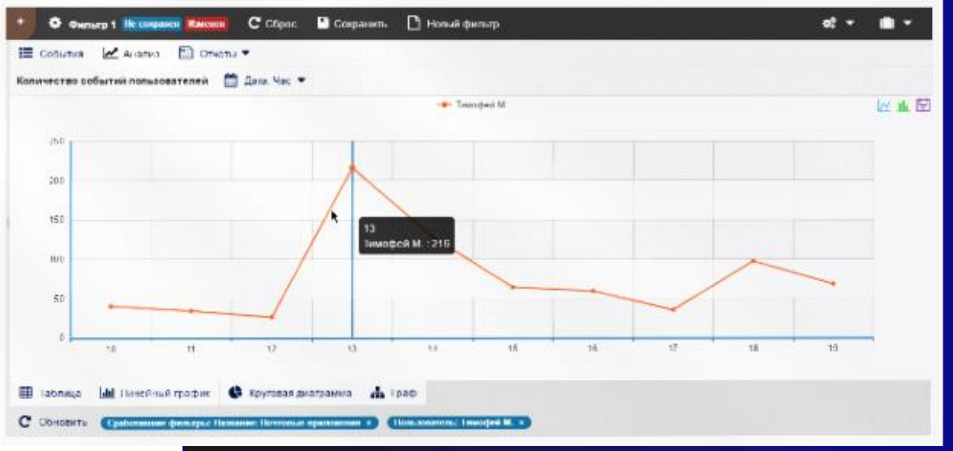
02 Поиск по словам и регулярным выражениям

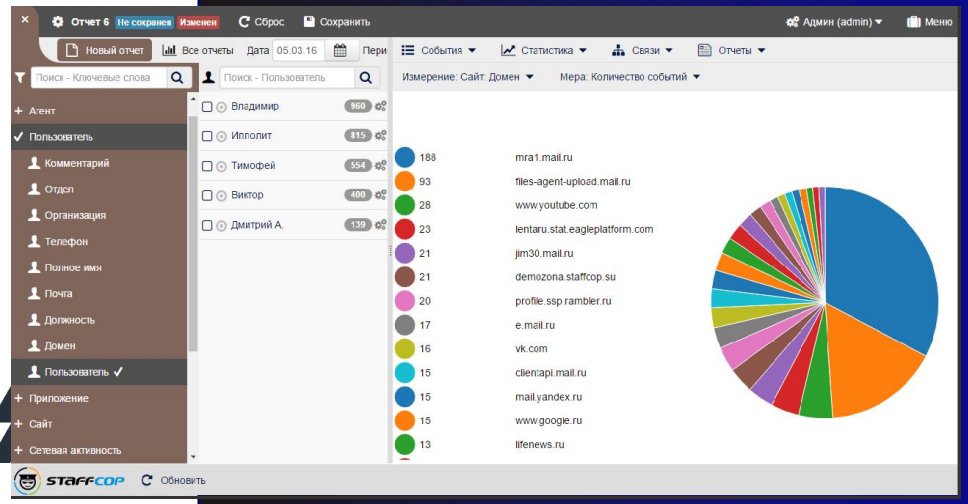
03 Синхронизация данных с AD

04 Конструктор многомерных отчетов

05 Множество графов и диаграмм

06 Speech-to-text





staffcop

Расследование инцидентов ИБ

01 Система оповещений

02 Гибкая система настройки фильтров

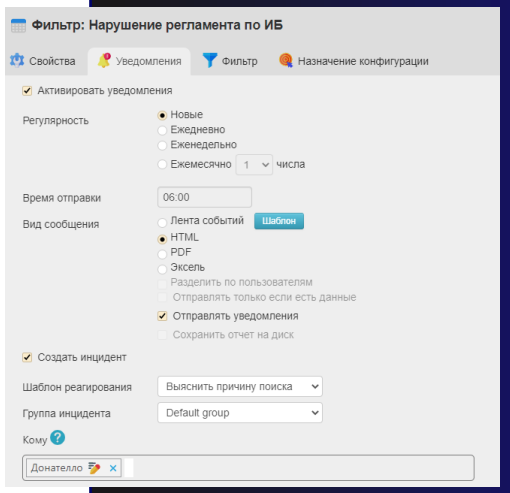
03 Графы взаимосвязей

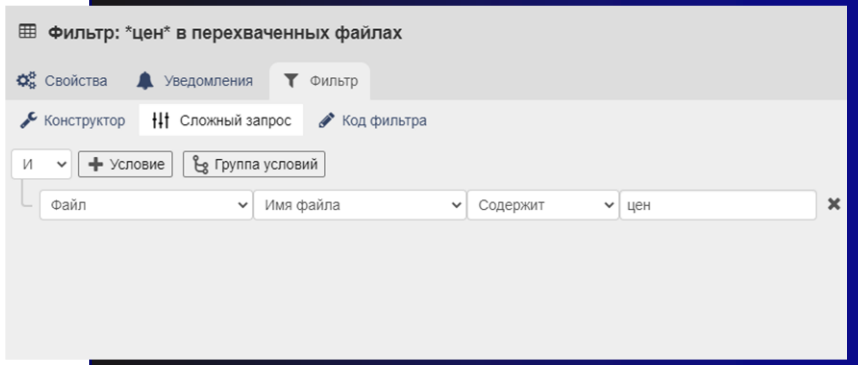
04 Метки для файлов

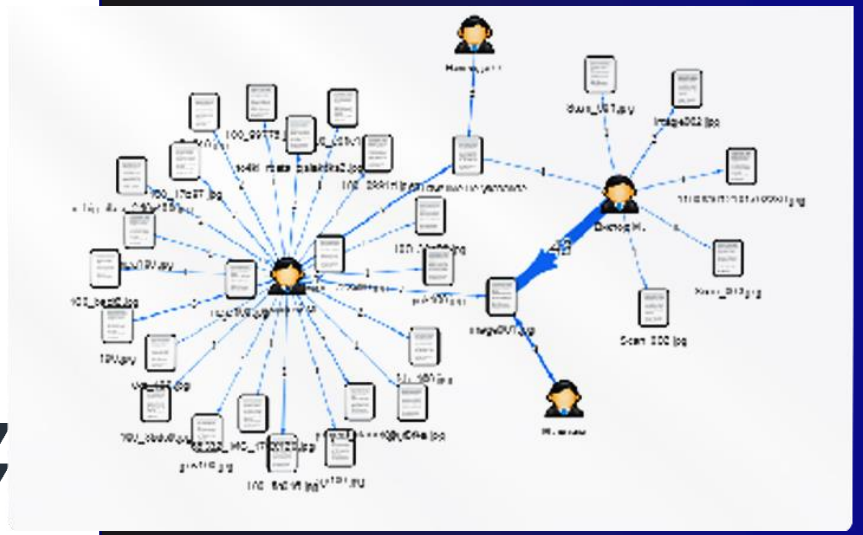
05 Изменение конфигурации контроля при наступлении определённого события

06 Защита от массового копирования

07 Нейронная сеть распознавания изображений

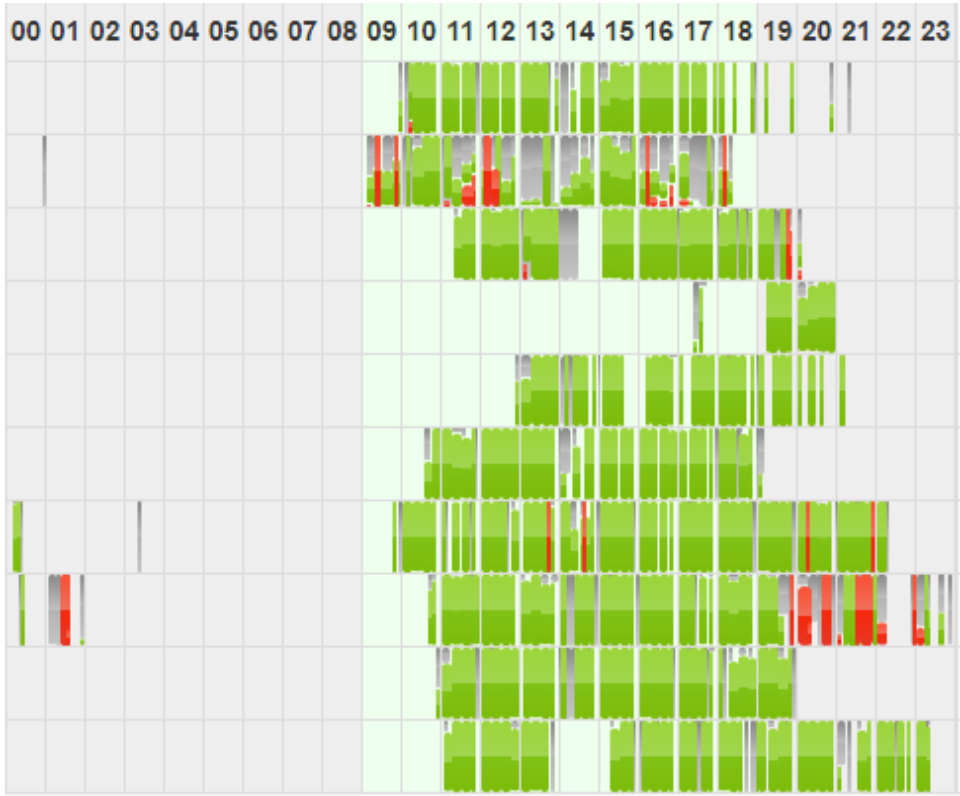






staffcop®

Учет 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

24%
Заняты работой

37%
Личные дела

7%
Опоздания

13%
Простой в работе

19%
Прочее

staffcop

Администрирование

01 Мониторинг аномальной активности

02 Блокировки съёмных накопителей

03 Инвентаризация ПО и «железа»

04 Удалённое наблюдение за АРМ и перехват управления

05 Интеграция с SIEM, AD, 1С, СКУД и другими системами ИБ и ИТ

06 Разные доступы для разных пользователей системы

staffcop

Интеграции с другими системами

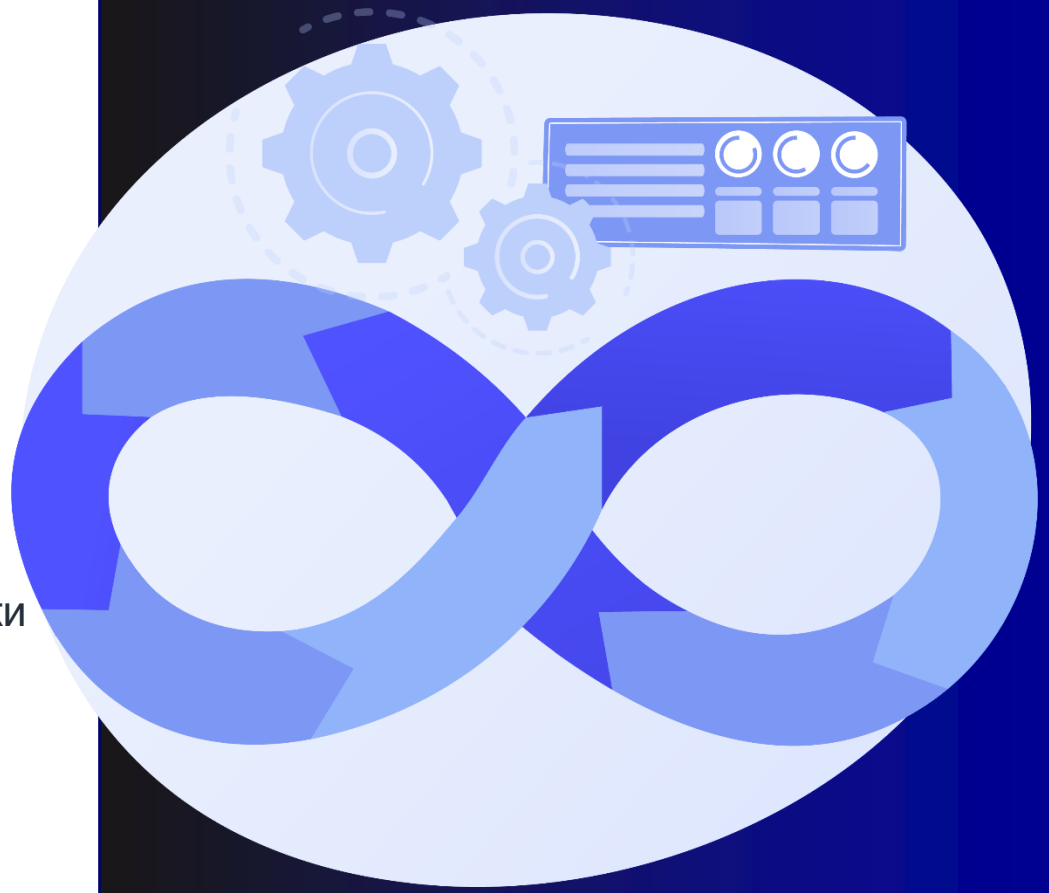
01 Передача данных через Syslog.
Можно гибко настроить какие данные направлять в syslog.

02 Получение данных через RestAPI.
Можно использовать обработанные Staffcop данные.

03 Прозрачная архитектура.
По описанию таблиц и полей можно делать выборки и выгрузки самостоятельно.

04 Подтверждённое взаимодействие с SIEM системами

05 Подтверждённая совместимость Staffcop с BaseAlt, Astralinux, RedOS, Rosa



staffcop®

Преимущества Staffcop Enterprise

Кроссплатформенный

Уникальные функции мониторинга рабочих станций и терминальных серверов под управлением Windows, Linux и MacOS систем.

Быстрый и легкий

Высокая скорость на больших объемах данных за счет использования современных баз данных ClickHouse и PostgreSQL на технологии OLAP-кубов.

Оптимальная стоимость покупки и владения

Минимальные требования к «железу», разумная стоимость, как результат - низкая стоимость приобретения, внедрения и эксплуатации.

Отечественный

Нас уже выбрали многие предприятия из ВПК, госсектора, крупные коммерческие и производственные организации.

Тестируйте Staffcop бесплатно в течение **3 месяцев!**

Дистрибутив и подробная документация на сайте www.staffcop.ru

Быстро

Развертывание пилотного проекта обычно занимает не более одного дня.

Легко

Требуется минимум усилий и ресурсов для запуска .

Комплексно

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

Полное техническое сопровождение на этапе тестирования!

staffcop®

Лицензия

Гибкая политика лицензирования согласно тарифного плана*

Обновления

Входят в стоимость тарифного плана

Техническая поддержка (стандарт)

Входит в стоимость тарифного плана

Тарифный план: лицензия, обновления, техническая поддержка

Стоимость лицензии

Количество пользователей

- Рабочая станция
- Учетная запись

Виды лицензии

- Срочная 3, 12, 24 мес.
- Бессрочная: на весь срок исключительных прав

Тех. Поддержка (стандарт) и обновления

- В течение срока действия без ограничений
- 12 месяцев с даты приобретения лицензии (продление по тарифному плану*)

staffcop

staffcop®

Расследование инцидентов
информационной безопасности

Спасибо за внимание!

staffcop.ru

Telegram

Дмитрий Кандыбович

Директор по развитию
ООО «Атом Безопасность»