Введение

Возможности продукта

Staffcop Enterprise – это программный комплекс для мониторинга рабочего времени сотрудников. Руководители компаний, сотрудники службы безопасности и администраторы сетей, использующие Staffcop Enterprise, могут отслеживать практически все подозрительные события, происходящие на компьютерах предприятия, как в реальном времени, так и в ретроспективе. С помощью нашего программного комплекса Вы сможете реально оценить эффективность работы Ваших сотрудников, и узнать, на что они тратят рабочее время. Также это отличный инструмент для выявления инсайдеров и обнаружения утечки конфиденциальных данных.

- полный мониторинг сетевого трафика (в том числе шифрованного), корпоративной электронной и вебпочты (с вложениями), интернет мессенджеров, посещения веб-сайтов;
- мониторинг работы с файлами (файловая система, буфер обмена, копирование файлов на внешние носители, сетевые диски, анализ данных в архивах);
- мониторинг активности сотрудников на рабочем месте;
- мониторинг печати документов;
- удаленное подключение к рабочему столу;
- блокировка сайтов, запуска приложений и подключения USB-устройств;
- доступ к административной панели из любой точки мира, где есть интернет, через веб-интерфейс;
- мощная система многомерного анализа действий пользователя на основе технологии OLAP;
- детектор аномалий поведения пользователей;
- система оповещения о нарушении политик безопасности предприятия;
- гибкая система настройки сбора информации;
- разграничение прав доступа к накопленной информации по группам и пользователям;
- наглядное отображение полученных данных в табличном виде, в виде графиков и диаграмм.

Архитектура

Staffcop Enterprise является клиент-серверным приложением и состоит из двух основных частей: Сервер и Агенты.

Сервер

Серверная часть предназначена для сбора, хранения, анализа и отображения собранной от агентов информации. Устанавливается на машину под управлением ОС Ubuntu Server.

Сервер использует для базы данных:

- PostgreSQL – основное хранение,
- ClickHouse – вспомогательное, может отсутствовать.

Доступ к данным и управление мониторингом осуществляется через веб-интерфейс (веб-консоль), работа с которым возможна с любого компьютера при подключения к серверу через интернет или локальную сеть. Для загрузки веб-интерфейса рекомендуем использовать современный браузер Chrome или Firefox.

Агенты

Агент представляет собой службу, запущенную на рабочей станции. Он собирает и передаёт на сервер информацию о событиях на компьютере и действиях сотрудника. Работа агента происходит в скрытом режиме незаметно для пользователя. Данные накапливаются в локальной базе, а после передачи на Сервер автоматически удаляются. Если нет связи с сервером, то сбор продолжается, но по достижении лимита на максимальный размер локальной базы Агент начинает циклично перезаписывать информацию, затирая самые старые данные.

Установка агента для ОС семейства Windows производится локально на рабочем месте сотрудника или по сети с помощью средств удаленной установки.

Установка Linux-агента выполняется путём запуска инсталлятора с правами root.

Установка агента для macOS производится с компьютера, на котором будет работать mac-агент или с помощью удалённого рабочего стола.

Данные передаются по шифрованному каналу (openSSL) пакетами, максимальный размер и интервал отправки которых задаются в настройках. При установке можно установить адреса и порты основного и альтернативного серверов. Если основной сервер недоступен, Агент будет передавать данные на альтернативный адрес. Таким образом можно обеспечить связь с сервером при выходе за рамки локальной сети предприятия (ноутбуки мобильных сотрудников).

План установки

Для начала установки получите ссылку на скачивание дистрибутива: https://www.staffcop.ru/download .

Чтобы установить Staffcop Enterprise воспользуйтесь инструкцией по установке.

Основные этапы установки:

1. Ознакомьтесь с системными требованиями.
2. Выберите подходящий способ установки сервера.
3. Настройте исключения антивируса.
4. Установите агенты мониторинга.
5. Настройте конфигурации и исключения для антивирусов.

При возникновении вопросов специалисты технической поддержки проконсультируют вас и при необходимости подключатся к вашему серверу для помощи и настройки. Инструкция для удаленного подключения.

Работа с программой

После установки и настройки проверьте, что события приходят на сервер.

В Линзе событий веб-консоли должны появиться события, которые агент отправляет на сервер. Если событий нет, проверьте аппаратные межсетевые экраны, программные шлюзы-файрволлы и другие устройства, которые могут блокировать трафик от агента к серверу.

Если события с компьютеров пользователей пришли на сервер, изучите полученные данные:

- Стандартные типы отчётов
- Типовые сценарии поиска информации
- Что нового в версии 5.7