staffcop®

Система для расследования инцидентов внутренней информационной безопасности

Техническая презентация

Информационная безопасность

Раннее обнаружение угроз ИБ
Гибкая настройка фильтров и оповещений. Возможную утечку или вторжение удаётся обнаружить на ранней стадии, снижая уровень последствий

Расследование инцидентов
Работая с архивом, возвращайтесь назад и смотрите, что делал сотрудник в указанном промежутке времени.

Анализ поведения пользователей
Автоматический анализ появления аномалий. Средства визуализации: диаграммы, граф и дерево взаимосвязей.

Эффективность работы персонала

Оценка продуктивности сотрудников
Разделение использование программ, посещения сайтов на продуктивные и непродуктивные. Настройка для отдельных пользователей, групп и отделов. Сравнение показателей.

Мониторинг бизнес-процессов
Выявление блокирующих факторов и расследование причин их появления. Анализ бизнес-процессов по KPI.

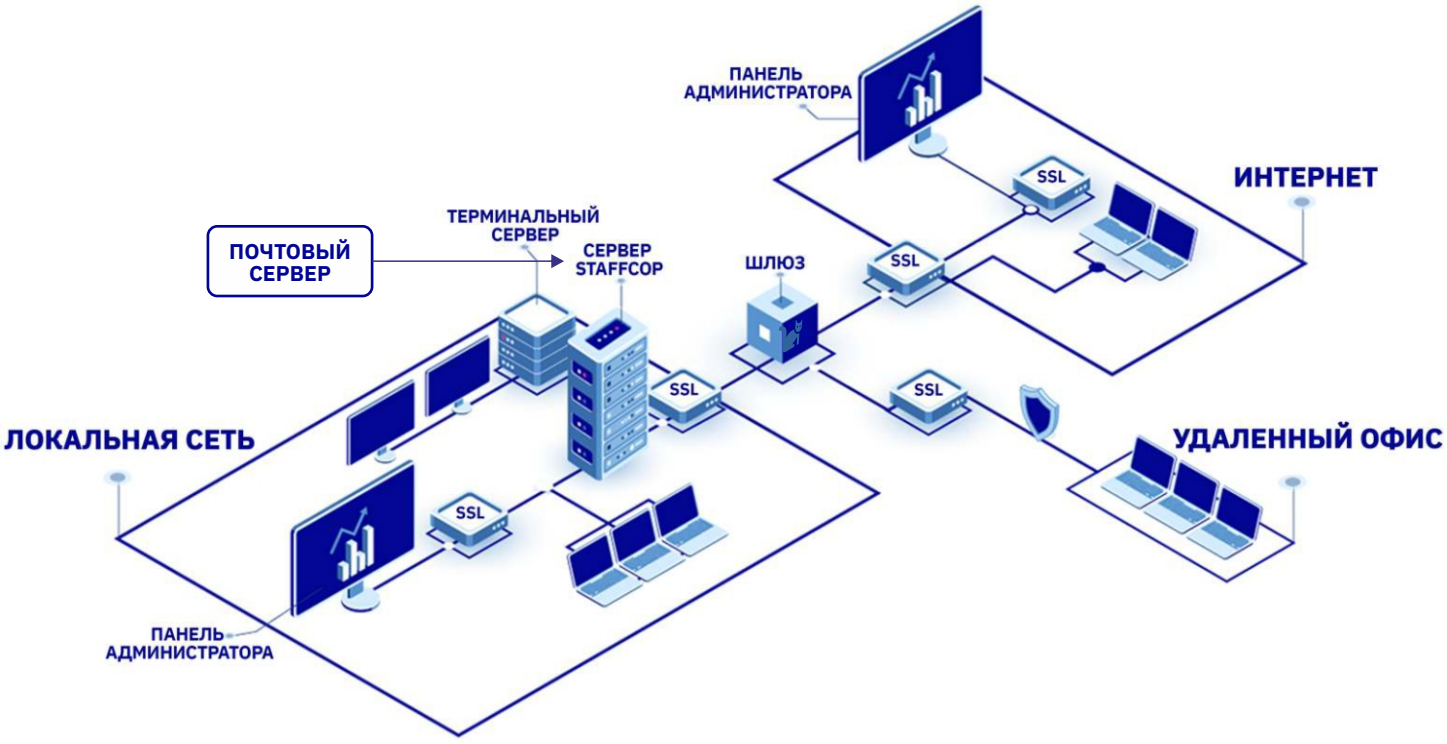
Учет рабочего времени
Мониторинг активности пользователя за ПК. Учет фактически отработанного времени, опозданий, ранних уходов и простоев.

Администрирование рабочих мест

Удаленное администрирование
Подключение к рабочему столу пользователя и удаленый захват управления ПК.

Инвентаризация компьютеров
Список использования программных продуктов и аппаратного обеспечения. Интенсивность использования и архив состояний.

Индексирование файлов на ПК
Поиск по атрибутам и содержимому среди файлов, находящихся на рабочих станциях сотрудников.



Интеграция с 1С календарь

Интеграция с SIEM системами

Интеграция со СКУД

Интеграция с почтовыми серверами

Для Windows-систем

• Логирование локального и удаленного выхода\выхода пользователя;
• Контроль активности пользователей в приложениях и на сайтах, контроль удаленной сессии пользователя;
• Контроль и блокировка запуска приложений. Контроль установки приложений;
• Снимки и видеозапись экрана пользователей по интервалу и действиям пользователй;
• Контроль ввода данных с клавиатуры;
• Контроль и блокировка буффера обмена;
• Агентский контроль сетевого траффика, передачи данных по http\https, блокировка сайтов, POST и GET запросы;
• Контроль почтовой переписки: POP, IMAP, SMTP, MAPI протоколы. Перехват веб-почты;
• Перехват переписки в мессенджерах: Telegram, Bitrix 24, MS Teams, Skype и прочие по протоколам ICQ, MMP, XMPP.
• Контроль файловой активности и создание теневых копий перехваченых файлов. Блокировка файловой активности на основе контента, меток и аттрибутов файлов и файловых операций;
• Контроль печати документов;
• Снимки и запись с веб-камеры по интервалу и действиям пользователей;
• Запись звука с микрофона и устройств вывода, запись переговоров;
• Возможность удаленного подключения с перехватом управления, возможность блокировки сессии пользователя;
• Анализ реестра оборудования и программного обеспечения;
• Пользовательское управление агентом и защита агента от привелигированных пользователей;
• Контроль и блокировка подключения к беспроводным сетям;
• Сканирование контента и аттрибутов файлов на АРМ пользователя.

Для GNU/LINUX-систем

• Логирование локального и удаленного выхода\выхода пользователя. Контроль ssh-подключений;
• Контроль активности пользователей в приложениях и на сайтах.;
• Контроль установки и запуска приложений;
• Снимки и видеозапись экрана пользователей по интервалу и действиям пользователй;
• Контроль ввода данных с клавиатуры и буффера обмена;
Перехват терминальных linux-сессий в виде gif-файла;
Поддержка перехвата с клавиатуры вне X Windows;
• Контроль почтовой переписки передаваемой посредством почтовых клиентов на основе движка "akonadi";
• Перехват переписки в мессенджере Telegram;
• DLP-модуль;
• Файловый сканер;
• Перехват сетевых протоколов;
• Возможность блокировки доступа к веб-сайтам и перехват SNAP-пакетов браузеров;
• Контроль файловой активности и создание теневых копий перехваченных файлов;
• Контроль и блокировка USB устройств;
• Контроль печати документов;
• Слежение за системными лог-файлами;
• Возможность удаленного подключения с перехватом управления;
• Снимки с веб-камеры по интервалу и действиям пользователей; возможность удаленного подключения к веб-камере;
• Запись звука с микрофона, запись переговоров;
• Анализ реестра оборудования и программного обеспечения;
• Перехват SMTP-протокола на уровне сети;
• Работу железа на основе архитектуры ARM;
• Пакет распространения для менеджера пакетов Portage в Gentoo;

Для MacOS

• Логирование выхода\выхода пользователя из системы;
• Контроль активности пользователей в приложениях и на сайтах;
• Контроль ввода данных с клавиатуры и буфера обмена;
• Снимки экрана пользователей по интервалу и действиям пользователей;
• Обновление агента с сервера;
• Файловый мониторинг;
• Универсальный инсталлятор для Intel и M;
• Файловый сканер;

Для сервера

• Возможность формирования фильтров поиска информации на основе OLAP технологии;

• Возможность гибкого представления данных в формате визуального анализа: отчеты, дашборды, таблицы, графики и графы;

• Контентный анализ и поиск информации на основе словарей и цифровых отпечатков;

• Возможность поиска с учетом морфологии и регулярных выражений;

• Возможность автоматического поиска аномалий и создание политик реагирующих на количественные пороги;

• Возможность распознавания графического контента: текст в перехваченных изображениях и снимках с экрана, распознавание лиц, паспортов и печатей.

• Возможность выгрузки и регулярной рассылки отчетов и событий в форматах html, pdf, xlsx;

• Возможность одновременного подключения квадратором вплоть до 16 удаленных рабочих столов;

• Возможность централизованного управления установкой агентов, правилами работы агента и возможность автоматической реакции на инциденты, обнаруженные системой;

• Возможность категоризации событий и времени активности для формирования УРВ;

• Возможность интеграции с внешними системами для получения передачи данных;

• Возможность создания инцидента на основе обнаруженного политикой\ фильтром события. Возможность отправки уведомлений на почту или в Telegram.

ОС для работы агента

Linux

Linux агент находится в стадии активного развития, и предназначен для любых linux-систем. Проверена работоспособность:

- CentOS;
- Ubuntu;
- Debian;
- Astra Linux;
- РЕД ОС
- Arch linux;
- Rosa linux;
- AltLinux.

Windows

Агент работает под управлением любой версии операционной системы Windows

- Windows XP (ограничено)
- Windows Vista;
- Windows 7, 8, 8.1, 10, 11

MacOS

Поддерживается работа на версиях MacOS:

- MacOS 10.13(High Sierra);
- MacOS 10.14(Mojave);
- MacOS 10.15(Catalina);
- MacOS 11.*(BigSur).

Терминальные сервера

Поддерживаемые системы:

- Windows 2008
- Windows 2008 R2
- Windows 2012 R2
- Windows 2016
- Windows Server 2019

Требования к серверу

Агентов	Память	Процессор	Диск (архив 1 месяц)	Диск (архив 3 месяца)	Диск (архив 12 месяцев)
10	4 ГБ	2	34 ГБ для БД и файлов	101 ГБ для БД и файлов	402 ГБ для БД и файлов
50	16 ГБ	4	170 ГБ для БД и файлов	502 ГБ для БД и файлов	2 ТБ для БД и файлов
100	32 ГБ	6	35 ГБ SSD для БД + 300 ГБ для файлов	103 ГБ SSD для БД + 900 ГБ для файлов	411 ГБ SSD для БД + 3.6 ТБ для файлов
200	48 ГБ	8	69 ГБ SSD для БД + 600 ГБ для файлов	206 ГБ SSD для БД + 1.8 ТБ для файлов	821 ГБ SSD для БД + 7.2 ТБ для файлов
500	64 ГБ	10	171 ГБ SSD для БД + 1.5 ТБ для файлов	513 ГБ SSD для БД + 4.5 ТБ для файлов	2051 ГБ SSD для БД + 18 ТБ для файлов
1000	96 ГБ	12	342 ГБ SSD для БД + 3 ТБ для файлов	1026 ГБ SSD для БД + 9 ТБ для файлов	4102 ГБ SSD для БД + 36 ТБ для файлов

Лицензии и сертификаты

Входит в реестр отечественного ПО

Сертификат ФСТЭК №4234.

Соответствует требованиям документов: Требования к СКН, Профиль защиты СКН (контроля подключения съемных машинных носителей информации четвертого класса защиты. ИТ.СКН.П4.ПЗ), 3Б

Успешно пройденные тематические исследования ТИ-69 на:

- Соответствие декларированных и реальных возможностей программного обеспечения;
- Отсутствие недекларированных возможностей программного обеспечения;
- Совместимость со средствами защиты информации;
- Возможность работы в безопасной среде.

Staffcop Enterprise может использоваться в составе:

- Автоматизированных систем (АС) до класса защищенности 1Г;
- Информационных систем персональных данных (ИСПДн);
- Государственных информационных систем (ГИС);
- Объектов критической информационной структуры (КИИ);
- Автоматизированных систем управления производственными и технологическими процессами на критически важных объектах, опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей среды до 1 класса (уровня) защищенности включительно.

Политика лицензирования:

Что лицензируем

Лицензии на пользователей

Рабочая станция

Учетная запись

Виды лицензий

Срочная
3, 12, 24 мес.

Бессрочная

Тех. поддержка (стандарт) и обновления

Включено в стоимость

Включено в стоимость на 1 год

StaffCop Enterprise имеет клиент-серверную архитектуру. Агент мониторинга имеет плавающий характер, предусмотрена возможность переносить агент на другие ПК без потери лицензии и архива данных.
Установленный агент на рабочей станции осуществляет мониторинг активных учётных записей. При отсутствии учетных записей пользователей агент осуществляет мониторинг самой рабочей станции.

Бесплатная техническая поддержка и доступ к обновлениям программы предоставляются на срок лицензирования, но не более 12 месяцев с момента покупки.
Тарифы на продление технической поддержки и доступа к обновлениям уточняйте вашего менеджера.