

staffcop®

Расследование инцидентов
внутренней безопасности

Мониторинг
Анализ
Оповещение
Блокировка
Интеграции

Sk  Участник

 академпарк

Оглавление

О компании	4
Преимущества	7
Архитектура	8
Как работает	10
Возможности интеграции	13
Совместимость	14
Ключевые нововведения Staffcop	16
Основные функции	18
Аналитические возможности	22
Расследование инцидентов информационной безопасности	28
Учет рабочего времени	32
Блокировки	35
Администрирование	36



Компания «АТОМ БЕЗОПАСНОСТЬ» — один из лидеров в области разработки программных решений для обеспечения информационной безопасности. Мы гордимся, что помогаем бизнесу становиться прозрачнее и эффективнее, защищаем наших клиентов от утечки конфиденциальных данных.

Выбрав нас, вы получаете не просто услуги по обеспечению безопасности, а настоящего партнера в лице команды экспертов. Мы стремимся к постоянному совершенствованию и инновациям, чтобы предоставить вашему бизнесу тот уровень защиты, который он заслуживает.

Вместе мы сформируем будущее, в котором ваш бизнес будет надежно защищен.

Иван Хаустов,
Генеральный директор
ООО «АТОМ БЕЗОПАСНОСТЬ»

О компании

«АТОМ БЕЗОПАСНОСТЬ» – аккредитованный российский разработчик IT-решений в области информационной безопасности и контроля действий персонала.

Более 10 лет мы разрабатываем программные решения для расследования инцидентов внутренней информационной безопасности. Среди наших клиентов представители крупного, среднего и малого бизнеса, коммерческие организации и государственные службы.

250 000+ ПК

под защитой Staffcop

3 000+ клиентов

в 40+ странах мира

**10+ лет
экспертизы**

в информационной
безопасности

**Лучшее ПО
для мониторинга
сотрудников**

по версии Forbes
Advisor, 2023 г.

 **минцифры_**

«АТОМ БЕЗОПАСНОСТЬ» внесена в Единый реестр IT-компаний Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации с регистрационным номером 9965 запись №95 от 15.03.2019 г.

Staffcop Enterprise внесен в Единый реестр российского ПО под №8828.



**ФСТЭК
России**

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), ЗБ.

Решаемые задачи

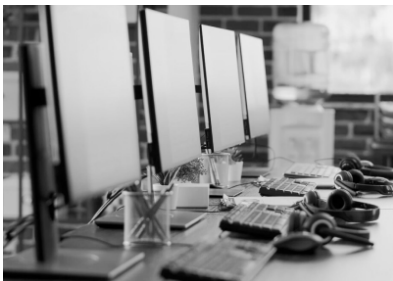


Информационная безопасность

- 1) Раннее обнаружение угроз ИБ
- 2) Расследование инцидентов
- 3) Анализ поведения пользователей

Эффективность работы персонала

- 1) Оценка продуктивности сотрудников
- 2) Мониторинг бизнес-процессов
- 3) Учет рабочего времени



Администрирование рабочих мест

- 1) Удаленное администрирование
- 2) Инвентаризация компьютеров
- 3) Индексирование файлов на ПК

О Staffcop Enterprise

Система для расследования инцидентов внутренней информационной безопасности Staffcop Enterprise состоит из двух частей: сервера и службы-агента.

Агент запускается на рабочих станциях сотрудников или терминальных серверах, собирает критичные данные, фиксирует подозрительные события. Затем он передает информацию на сервер для хранения и обработки. Функционал сервера включает быстрый поиск, анализ и визуализацию данных.

Staffcop Enterprise может работать как в рамках локального закрытого периметра, так и на компьютерах, находящихся за его пределами.

С помощью Staffcop Enterprise вы можете:



Расследовать

- Инциденты информационной безопасности
- Причины низкой продуктивности



Выявлять

- Мошеннические схемы внутри компании
- Работу на конкурентов



Предупреждать

- Утечки конфиденциальной информации
- Саботаж рабочих процессов
- Конфликтные ситуации в коллективе



Блокировать

- Копирование конфиденциальной информации на съемные носители
- Доступ и перемещение файлов с конфиденциальной информацией
- Доступ к нерегламентированным веб-ресурсам и приложениям

Преимущества

Кроссплатформенный

Функции мониторинга рабочих станций и терминальных серверов под управлением Windows, Linux и macOS систем.

Оптимальная стоимость покупки и владения

Минимальные требования к «железу», разумная цена, как результат – низкая стоимость владения и эксплуатации.

Качественная техподдержка

Подробная документация, оперативная и компетентная техническая поддержка. Команда проекта оказывает комплексную поддержку с начального этапа тестирования.

Расширенный пилот с полноценным функционалом

Бесплатное полнофункциональное тестирование на любом парке ПК. Помощь от инженеров внедрения еще до приобретения.

Быстрый

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

Отечественный

Нас уже выбрали многие предприятия из ВПК, госсектора, крупные коммерческие и производственные организации. Агент работает на Astra Linux, Альт, РЕД ОС, Атлант, Основа и прочих ОС.

Доступ к регулярным обновлениям

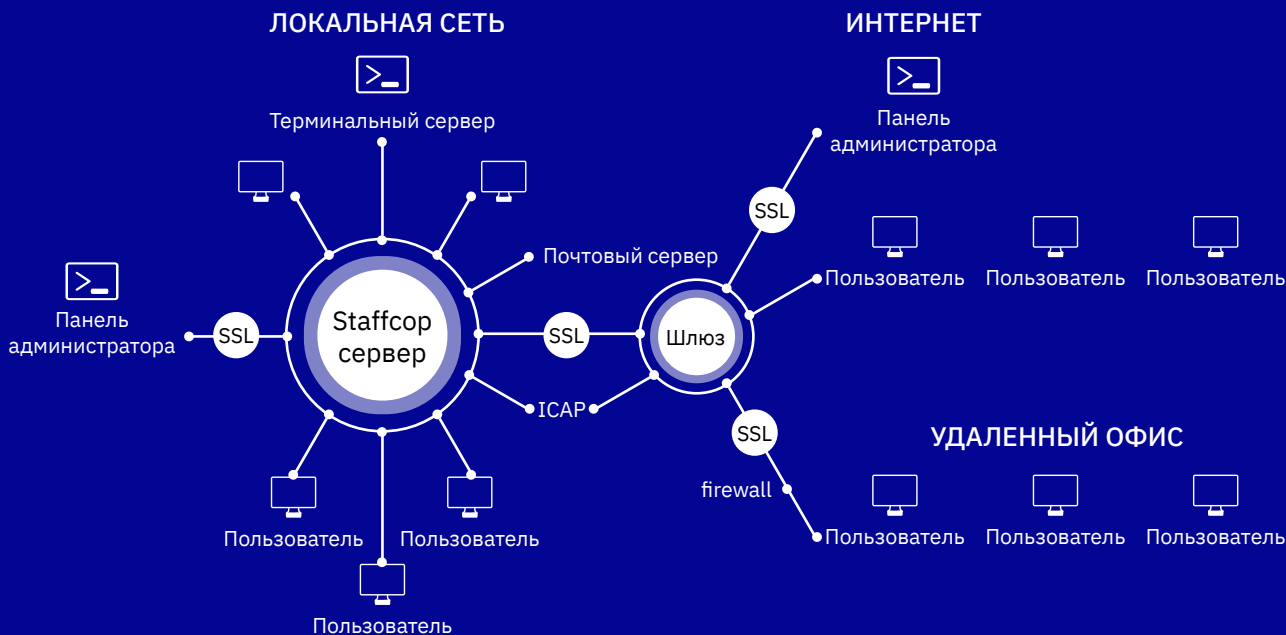
Регулярные обновления как самого ПО Staffcop, так и его компонентов для оперативного устранения уязвимостей и получения доступа к новому функционалу.

Индивидуальный подход, закрепленный менеджер

Развитие продукта в соответствии с задачами от клиентов; выделенные специалисты для проработки ТЗ и помощи в гибкой настройке ПО.

Архитектура

Работает в локальных, распределенных и смешанных сетях любой сложности



Единый веб-интерфейс

Взаимодействие с системой происходит через единый веб-интерфейс с гибким управлением, которое позволяет анализировать данные, устанавливать политики и реакции, настраивать работу системы и собирать статистику.

Современные технологии

В основе лежит OLAP – технология обработки данных для построения многомерных отчетов «на лету» и обработки больших объемов данных за секунды.

Для работы достаточно одного виртуального сервера

Сервер работает на операционной системе Linux (Astra, Ubuntu) и может быть установлен как на физической, так и на виртуальной машине.

Возможности интеграции

- Открытое API
- Получение данных об отсутствии из 1С
- Получение данных от СКУД
- Передача данных в SIEM посредством Syslog

Горизонтально масштабируется

Staffcop Enterprise эффективно работает как с несколькими компьютерами, так и с тысячами рабочих станций.

Агент для Windows, Linux, macOS

Контроль ведется на рабочих станциях, терминальных серверах, VDI. Агент работает на операционных системах Windows, Linux, macOS*.

* функциональность агента на разных операционных системах отличается.

Локальное хранение

Агент без доступа к серверу полноценно функционирует: собирает данные в локальную базу данных и ограничивает действия пользователь: блокирует доступ к каналам передачи данных и утечки.

Минимальные требования к инфраструктуре

Минимальные требования к серверу:

100 ПК <=> 6 CPU, 32 RAM.

1000 ПК <=> 14 CPU, 96 RAM.

Минимальная нагрузка от агента для данного класса решений.

Как работает?

01 Сбор данных



Агент собирает все необходимые специалистам для расследования данные и передает их на сервер. Сервер обрабатывает полученную информацию, что позволяет использовать ее для анализа, оповещения

02 Анализ



Визуальный и статистический анализ данных для выявления отклонений в поведении пользователей, поиска инцидентов, инсайдеров и нелояльных сотрудников.

03 Поиск



- 1) Поиск информации в любых событиях на основе морфологии, фраз и регулярных выражений.
- 2) Поиск похожих документов, печатей и паспортов, анализ ближайших событий и снимков экрана.

04 Расследование



1) Управление расследованиями через систему: организация, контроль и запись действий в ходе расследования, назначение ответственных и отметка фигурантов, работа на основе приоритетов и фильтров.

2) Возможность перехода из отчетов и графического анализа к конкретным событиям позволяет находить данные, очищенные от информационного шума, в несколько кликов.

05 Оповещение



Автоматическое оповещение отправленное на почту или в мессенджер о нарушении политики безопасности, опасной, аномальной и непродуктивной деятельности сотрудников.

06 Блокировка



1) Операций с файлами на основе содержимого, меток и атрибутов (пути, форматы, тип контента).

2) Доступа к съемным носителям, полная или только для чтения.

3) По классам и группам устройств, на основе черных и белых списков.

4) Запуска приложений и доступа к сайтам, использование Wi-Fi сети.

Тестируйте бесплатно

✓ **Легко**

Требуется минимум действий и ресурсов для запуска.
Сопровождение во время всего тестового периода:
помощь в настройке, консультации, помощь в защите проекта.

✓ **Комплексно**

Вы сможете оценить сразу весь комплекс решаемых задач
и выявить инцидент в процессе тестирования.

✓ **Быстро**

Развертывание пилотного проекта обычно занимает не более одного дня.

Полное техническое сопровождение
на этапе тестирования!

Дистрибутив и подробная
документация на сайте
www.staffcop.ru



Возможности интеграции



Открытый API и передача данных через Syslog позволяет дополнять данными SIEM-систему для комплексного анализа и обработки инцидентов.



Дополняйте профиль пользователя данными с помощью синхронизации с Active Directory. Группируйте и анализируйте данные по отделам, формируйте отчеты для руководителей.



Контролируйте и анализируйте рабочие коммуникации и передачу данных через почтовый сервер IMAP.



Для комплексного анализа рабочего дня сотрудников система позволяет дополнять расписание данными табеля отсутствия из 1С.



Получение данных сетевого трафика со стороны шлюзового решения посредством интеграции на основе ICAP-протокола.



Для проведения анализа нахождения сотрудников на рабочем месте реализована интеграция со СКУД.

Совместимость с решениями ИБ



Эшелонированная защита

Увеличение надежности защиты при нескольких решениях по ИБ.



Защита ваших филиалов

DLP более надежно контролирует сетевой трафик на шлюзе.
Staffcop контролирует действия пользователей на рабочих станциях.
При этом системы друг с другом не конфликтуют.



На одной группе риска DLP. На другой – Staffcop

DLP контролирует одну группу риска внутренней информационной безопасности,
Staffcop Enterprise контролирует действия пользователей и обнаруживает аномалии.



Оптимизация бюджета защиты ИБ

Если DLP защищает центральный офис, то на филиалах можно установить дополнительную защиту.



Staffcop Enterprise как дополнение

Система предоставляет инструментарий для помощи администраторам. В реальном времени можно не только удаленно подключиться к рабочей станции пользователя, для анализа проблем или детального изучения аномальной активности пользователя, но и получить доступ к управлению станцией.

Подтверждена совместимость:



Подходит для импортозамещения:

- ✓ Сертификат ФСТЭК
- ✓ Работает на открытом ПО, защищен от санкций
- ✓ Входит в реестр отечественного ПО
- ✓ СУБД: PostgreSQL, ClickHouse, Jatoba
- ✓ Сервер на Ubuntu и Astra Linux



Ключевые нововведения Staffcop Enterprise 5.3

Карточка сотрудника

Выявляйте аномалии в активности пользователей с помощью нового метода анализа информации.

Полноценная система управления задачами расследования

Оптимизируйте процесс расследования инцидентов в отдельной консоли.

Менеджер ВНИ

Управляйте использованием и доступом внешних носителей информации в рамках единого центра управления.

Перехват данных и файлов, отправляемых из черновиков электронной почты

Фиксируйте сохранение критически важной информации в черновике почтового сообщения, доступ к которому сотрудник может получить уже за пределами периметра.

Контроль передачи данных в популярных мессенджерах WhatsApp и Telegram

Отслеживайте передачу конфиденциальной информации и анализируйте переписку для выявления неправомерных действий сотрудников.

Агент на macOS в формате pkg

Функции блокировки сессии, контроля устройств и скачивания файлов расширяют возможности macOS-агента в направлении DLP и расследования инцидентов. Контроль носителей информации.

Расширенные возможности по контролю передачи данных посредством сети на Linux

Контроль корпоративных мессенджеров MS Teams и облачных ресурсов, веб-почты VK mail.

Hyperscan

Не только в разы увеличивает скорость анализа текстового контента, но и позволяет искать события на основе количества совпадений со словарем.

Контроль состояния сервера

Встроенная Graphana предоставляет администраторам широкие возможности по контролю работоспособности системы.

Основные функции



Действия пользователей

Учет рабочего времени

Мониторинг активности пользователя ПК. Интеграция со СКУД. Категоризация активности на продуктивную и непродуктивную.

Контроль пользовательской активности

Контроль пользовательской сессии, локальной и удаленной, логирование входа и выхода из системы. Контроль опозданий и ранних уходов.

Мониторинг бизнес-процессов

Поиск узких мест, выявление блокирующих факторов и расследование причин их появления. Анализ бизнес-процессов по KPI.

Снимки экрана и видеозапись рабочего стола

Обогащение данных по действиям пользователя за счет информации на экране сотрудника.

Контроль ввода данных

Контроль информации при вводе данных с клавиатуры и копировании в буфер обмена.

Запись аудио с микрофона и снимки с веб-камер

Контроль окружающего пространства рабочего места сотрудника. Идентификация сотрудника на основе распознавания лиц.

Контроль почтовой переписки

Контроль переписки и передачи файлов через почтовые сервисы по протоколам POP3, IMAP, SMTP, MAPI. Перехват переписки напрямую с корпоративного почтового сервера.

Контроль устройств

Фиксация времени подключения и отключения, перехват файлов при загрузке на устройства хранения и на самом устройстве; блокировка по типам и параметрам устройств, черным и белым спискам.

Контроль печати

Отслеживание файлов во время отправки на печать. Контроль количества страниц и времени отправки, теневого копирования файлов.

Файловый сканер

Анализ содержимого и атрибутов файлов. Поиск конфиденциальной информации на рабочих станциях сотрудников.

Файловый мониторинг

Контроль файловых операций. Блокировка доступа перемещения и изменения файлов с конфиденциальной информацией.

Сетевой трафик

Перехват сообщений в корпоративных мессенджерах

Контроль внутренней переписки в мессенджерах: MS Teams, VK Teams, Express, Bitrix24. Анализ переписки для выявления неправомерных действий сотрудников.

Перехват сообщений в некорпоративных мессенджерах

Фиксация содержимого, вложенных файлов и времени отправки или получения сообщения в WhatsApp, Telegram, Skype. Контролируйте передачу конфиденциальной информации.

Контроль использования веб-ресурсов

- Мониторинг сайтов
- Контроль активности в социальных сетях
- Перехват поисковых запросов
- Блокировки доступа к веб-ресурсам

Контроль облачных ресурсов

Контролируйте данные, которые передаются посредством корпоративных и публичных облачных сервисов хранения информации.

Контроль АРМ

Контроль Wi-Fi

Возможность полноценно ограничить нерегламентированный доступ в интернет.

Удаленное администрирование

Перехват управления и блокировка рабочей сессии. Удаленный просмотр до 16 рабочих столов одновременно.

Инвентаризация компьютеров

Полный список программных продуктов и аппаратного обеспечения на рабочем ПК.

Блокировка приложений

Блокировка запуска нерегламентированных, запрещенных и опасных программных продуктов.

Аналитические возможности

Система позволяет точно выбирать, какие данные и в каком объеме хранить в архиве. Это помогает оптимально использовать свободное место без ущерба задачам.

2023-10-04 11:38:15	Операции с файлами	Olesya Aksenova	Олеся	igfbem.exe	C:\Users\Olesya\IntelGraphicsProfiles\Brighten_Video.man.igp1 Перезапись Brighten_Video.man.igp1 Hard HFS128G39TND-N210A
2023-10-04 11:38:27	Вход/выход из системы	Olesya Aksenova	Олеся	Сессия разблокирована	
2023-10-04 11:38:33	Посещение сайтов	Olesya Aksenova	Олеся	msedge.exe	https://ntp.man.com/edge/ntp? locale=ru&site=%D0%BD%D0%BE%D0%B2%D0%B0%D1%8F%20%D0% D0%B0%D0%B4%D0%BA%D0%B0&re=1&dsp=0&sp=%D0%AF%D0%BD %BA%D1%81&startpage=1&PCeUS31&pre-render=1
2023-10-04 11:38:36	Время активности	Olesya Aksenova	Олеся	explorer.exe	Program Manager Интерфейс системы
2023-10-04 11:38:36	Снимок экрана	Olesya Aksenova	Олеся	explorer.exe	Program Manager Screenshot.jpg

Время 2023-10-04 11:38:15

Сервер этот сервер

Приложение igfbem.exe

Тип события Операции с файлами

Агент Olesya Aksenova

Пользователь Олеся

Имя файла Brighten_Video.man.igp1

Путь C:\Users\Olesya\IntelGraphicsProfiles\Brighten_Video.man.igp1

Операция Перезапись

Производитель (Standard disk drives)

Устройство HFS128G39TND-N210A

HardwareId PCI\VEN_8086&DEV_282A&SUBSYS_12641025&REV_10\3&11593650&0800

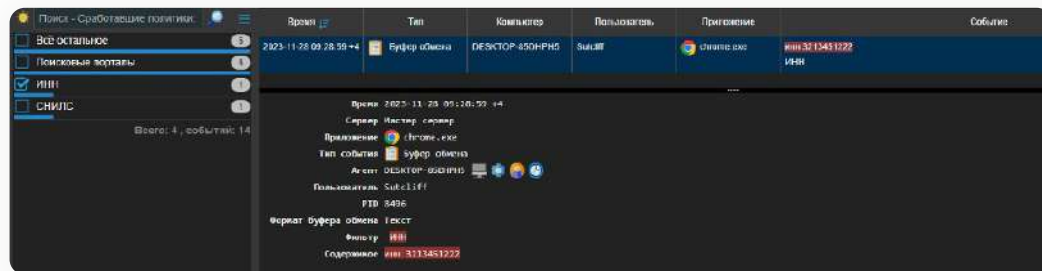
Размер диска ВНИ 118.5 GiB

Тип устройства Hard

Поиск по словам
и регулярным
выражениям

Выявляйте инциденты в передаваемых данных и действиях сотрудников с помощью слов-триггеров. Система позволяет настроить словари с реакцией не только на количество триггерных слов и выражений, но и учитывать общее содержание и атрибуты события. Это позволяет обнаружить утечку данных, получить представление о сотрудниках и предотвратить проблемы.

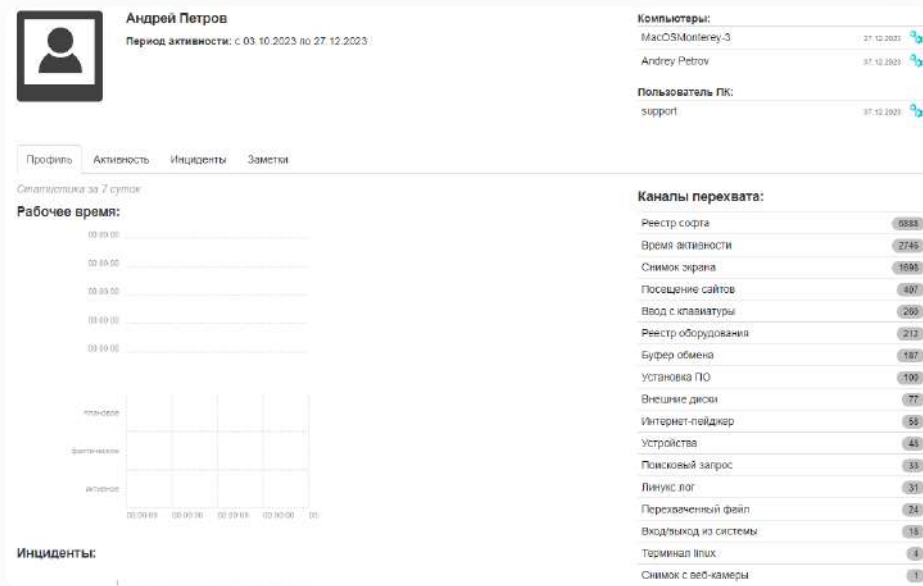
Регулярные выражения точно выявляют передачу структурированной информации, такой как личные данные, конфиденциальные документы и служебная информация.



Синхронизация данных с AD

При синхронизации данных с Active Directory система обогащается информацией о профилях пользователей. Это позволяет выявлять инциденты, создавать политики безопасности и продуктивности. Например, можно открыть доступ к сайтам по трудоустройству для отдела кадров и уведомлять администратора о получении конфиденциальных документов сотрудниками на испытательном сроке.

Для доступа настройте права доменных пользователей или установите агент на рабочие станции напрямую из веб-консоли в рамках домена.

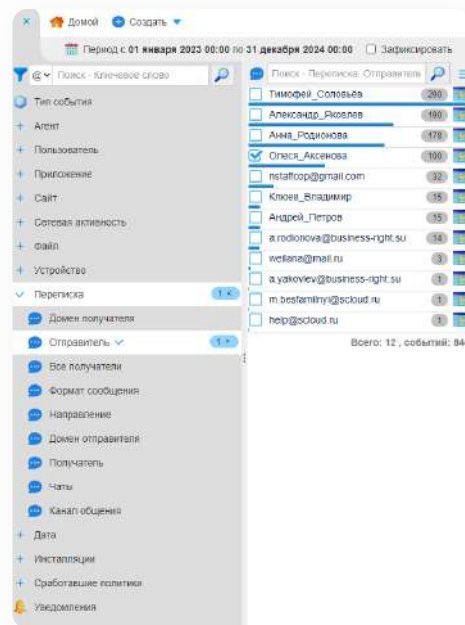


Гибкий и интерактивный конструктор отчетов и фильтров

Создавайте новые фильтры и отчеты.

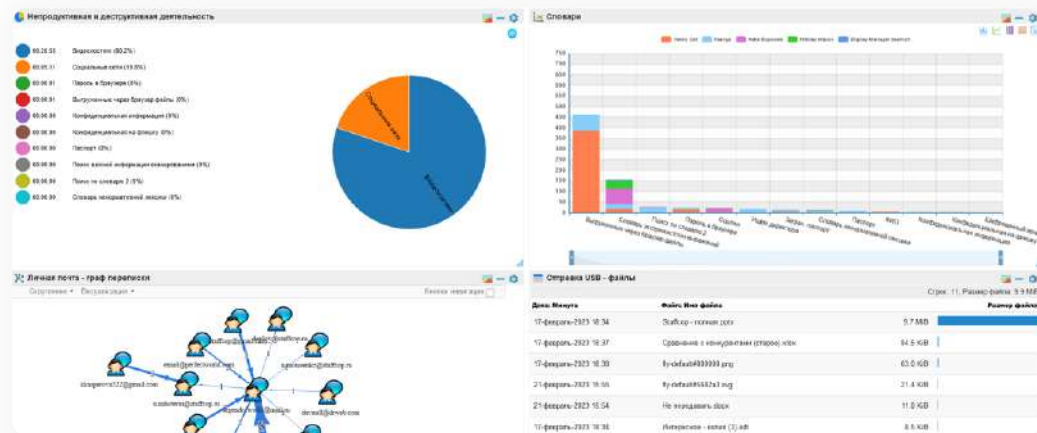
Для поиска и анализа информации используется прием последовательного наложения ограничивающих фильтров. Наложение каждого фильтра в режиме реального времени отсекает лишнюю информацию, что позволяет находить данные в 2-3 клика. Выбирайте форму и содержимое визуализации выбранных данных. Сохраняйте и используйте настроенные фильтры, чтобы не собирать нужные отчеты заново.

Также можно настроить в отчетах отправку уведомлений при появлении новых событий или отправку отчета по новым событиям за период.



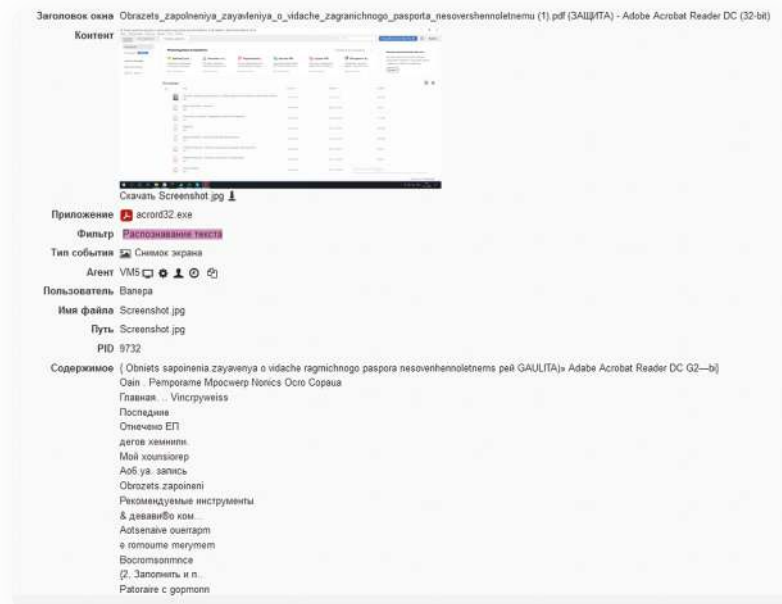
Множество графов и диаграмм

Сводные отчеты в простом и удобном виде в рамках одного окна отображают самые важные характеристики и связанные события для выбранного объекта. Карточки сотрудников позволяют быстро получать агрегированную информацию по работнику, выявлять аномалии в активности и действиях, переводить сотрудника на особый контроль. Комплексный профиль содержит большой объем необходимой статистической информации по сотруднику.



Распознавание
текста
в графическом
и аудиоконтенте


Передаваемая информация содержится не только в текстовых файлах. Зачастую это могут быть сканы документов, графики или чертежи. Система извлекает и анализирует текстовую информацию из таких документов. Можно распознать и снимки рабочего стола сотрудника, чтобы превентивно определить, что сотрудник получил доступ к нерегламентированной информации до того, как решил ее передать. Распознавание аудиоконтента позволяет обнаруживать мошеннические действия и расследовать конфликты сотрудников за счет анализа аудиотрафика с микрофона рабочей станции.



Расследование инцидентов ИБ

При сборе больших объемов информации важно оперативно реагировать на обнаружение инцидентов. Система позволяет настроить отправку уведомлений специалисту на почту или в Telegram при обнаружении действия сотрудника, требующего особого внимания. Она также позволяет регулярно отправлять отчеты с агрегированными данными для анализа действий сотрудников.

Уведомление для фильтра "Фильтр 42" от 26.05.23 15:57

 Staffcop Enterprise Notification m.chepliev@staffcop.ru 26 мая в 15:57
[И >](#)

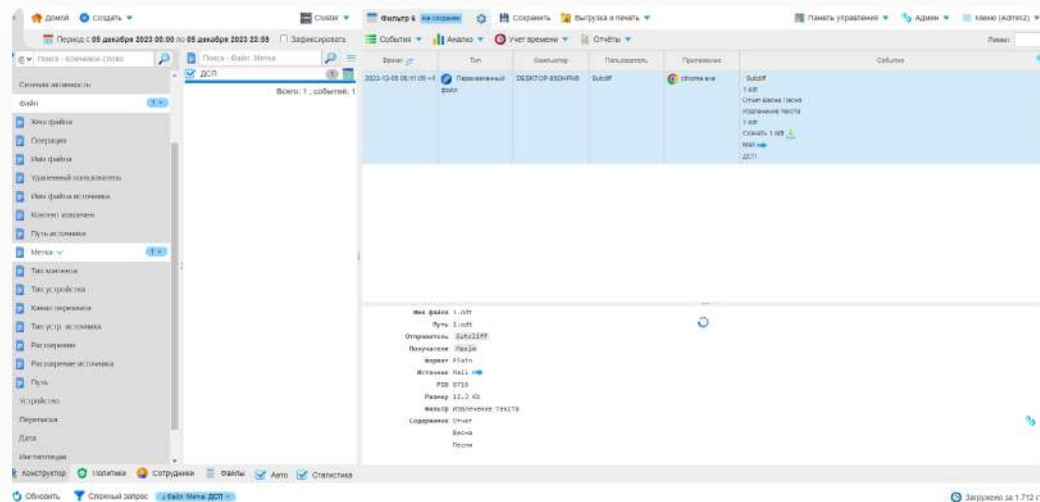
Фильтр 42

Локальное время	Тип события	Компьютер	Пользователь	Приложение	Событие
2023-05-26 15:56:59	Действие администратор		m.chepliev		Фильтр Добавлено "Создан объект #1678 Фильтр 42 типа analytics.filter пользователем m.chepliev", m.chepliev
2023-05-26 15:56:38	Действие администратор		m.chepliev		Почтовые настройки Изменено "m.chepliev@staffcop.ru@smtp.yandex.ru" - Изменен active. m.chepliev

Для просмотра обнаруженных событий [перейдите по ссылке](#).
Если Вы больше не хотите получать оповещения [нажмите по ссылке](#), во вкладке "Уведомления", удалите почтовый ящик из поля "Кому" и нажмите кнопку "Сохранить".

Метки для файлов

Не всегда можно выделить слова-триггеры в документах с конфиденциальной информацией. Установка в структуре самого файла метки, невидимой рядовому пользователю, позволяет не только контролировать движение файла в организации, но и ограничивать его перемещение и даже доступ пользователей к нему.



Помогает управлять задачами по расследованию инцидентов ИБ, что повышает эффективность работы. Консоль сокращает затраты за счет управления процессом расследования и быстрого получения данных.

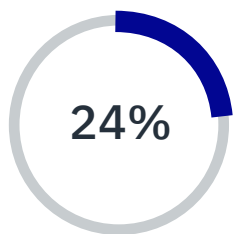
ID ↓	Дата	Тема	Группа	Статус	Создал	Назначен	Приоритет	Шаблон реагирования	Фильтр	Дата последнего изменения
17878	18.10.2023 14:41	На основании фильтра 1758 "Фильтр 63"		New	Admin User <admin@example.com>	Admin User <admin@example.com>	Незначительный		Фильтр 63	
17877	18.10.2023 14:41	На основании фильтра 1690 "Фильтр 54"	Default group	New	Admin User <admin@example.com>	Admin User <admin@example.com>	Незначительный	Default pattern	Фильтр 54	
17876	18.10.2023 14:40	На основании фильтра 1690 "Фильтр 54"	Default group	New	Admin User <admin@example.com>	Admin User <admin@example.com>	Незначительный	Default pattern	Фильтр 54	
17875	18.10.2023 14:39	На основании фильтра 1690 "Фильтр 54"	Default group	New	Admin User <admin@example.com>	Admin User <admin@example.com>	Незначительный	Default pattern	Фильтр 54	
17874	18.10.2023 14:36	На основании фильтра 1758 "Фильтр 63"		New	Admin User <admin@example.com>	Admin User <admin@example.com>	Незначительный		Фильтр 63	
17873	18.10.2023 14:36	На основании фильтра 1690 "Фильтр 54"	Default group	New	Admin User <admin@example.com>	Admin User <admin@example.com>	Незначительный	Default pattern	Фильтр 54	
17872	18.10.2023 14:34	На основании фильтра 1690 "Фильтр 54"	Default group	New	Admin User <admin@example.com>	Admin User <admin@example.com>	Незначительный	Default pattern	Фильтр 54	
17871	18.10.2023 14:33	На основании фильтра 1690 "Фильтр 54"	Default group	New	Admin User <admin@example.com>	Admin User <admin@example.com>	Незначительный	Default pattern	Фильтр 54	
17870	18.10.2023 14:32	На основании фильтра 1690 "Фильтр 54"	Default group	New	Admin User <admin@example.com>	Admin User <admin@example.com>	Незначительный	Default pattern	Фильтр 54	
17869	18.10.2023 14:31	На основании фильтра 1758 "Фильтр 63"		New	Admin User <admin@example.com>	Admin User <admin@example.com>	Незначительный		Фильтр 63	

Учет рабочего времени

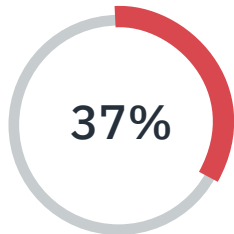
Повышение эффективности труда

Мы опросили* наших клиентов, использующих Staffcop Enterprise, и составили картину распределения рабочего времени среднестатистического сотрудника.

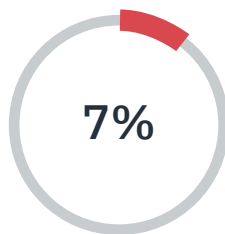
Staffcop Enterprise не только фиксирует начало, перерывы и окончание рабочего дня, но и показывает детальную картину активности сотрудников.



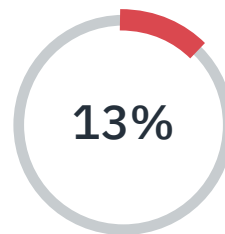
Заняты работой



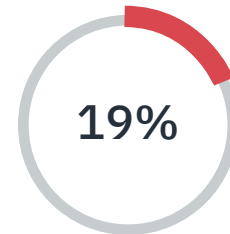
Личные дела



Опоздания



Простой в работе



Прочее

* собственное исследование ООО «АТОМ БЕЗОПАСНОСТЬ», 2023 год

Гибкая настройка расписаний и категоризации приложений и сайтов

Для разных категорий сотрудников можно настроить список разрешенных программ и сайтов, а доступ к нежелательным ресурсам запретить. Кроме этого, настройки позволяют создавать уникальное расписание рабочего дня.

История

Название:

Тип периода учета:

Рабочие дни

День недели	Выбран	Начало работы	Окончание работы	Начало перерыва	Окончание перерыва	Рабочее время
Едине	<input checked="" type="checkbox"/>	<input type="text" value="09:00"/>	<input type="text" value="18:00"/>	<input type="text" value="12:00"/>	<input type="text" value="13:00"/>	<input type="text"/>
Понедельник	<input checked="" type="checkbox"/>	<input type="text" value="09:00"/>	<input type="text" value="18:00"/>	<input type="text" value="12:00"/>	<input type="text" value="13:00"/>	<input type="text"/>
Вторник	<input checked="" type="checkbox"/>	<input type="text" value="09:00"/>	<input type="text" value="18:00"/>	<input type="text" value="12:00"/>	<input type="text" value="13:00"/>	<input type="text"/>
Орда	<input checked="" type="checkbox"/>	<input type="text" value="09:00"/>	<input type="text" value="18:00"/>	<input type="text" value="12:00"/>	<input type="text" value="13:00"/>	<input type="text"/>
Четверг	<input checked="" type="checkbox"/>	<input type="text" value="09:00"/>	<input type="text" value="18:00"/>	<input type="text" value="12:00"/>	<input type="text" value="13:00"/>	<input type="text"/>
Пятница	<input checked="" type="checkbox"/>	<input type="text" value="09:00"/>	<input type="text" value="18:00"/>	<input type="text" value="12:00"/>	<input type="text" value="13:00"/>	<input type="text"/>
Суббота	<input checked="" type="checkbox"/>	<input type="text" value="09:00"/>	<input type="text" value="18:00"/>	<input type="text" value="12:00"/>	<input type="text" value="13:00"/>	<input type="text"/>
Воскресенье	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

"Рабочее время" используется при построении отчетов по учету рабочего времени. График обеденного перерыва и "Рабочее время" указывать не обязательно. Если указан перерыв, "Рабочее время" считается по разнице длительности рабочего дня и перерыва. "Рабочее время" не указано – для отчетов берется полная длительность рабочего дня.
Для выбора рабочих дней недели активируйте чекбокс рядом с необходимыми днями. Если расписание для разных дней недели различается – отключите чекбокс напротив "Едине", тогда сможете указать разные расписания для разных дней.

Наглядная статистика в отчетах и таблицах

- Опоздания
- Простои на работе
- Активное время за компьютером
- Продуктивное время
- Время, затраченное на личные нужды
- Статистика по сотрудникам и отделам

Staffcop Enterprise умеет в автоматическом режиме по расписанию отправлять подробный отчет в PDF, HTML или XLS на электронную почту.

2 февраля 2022 г. Среда

Пользователь ↓																								Начало		Окончание		Общее время		Дисциплина		
	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	факт ↓	распис ↓	факт ↓	распис ↓	факт ↓	план ↓	сверх ↓	опозд ↓
Донателло																									8:54:54	10:00:00	17:22:45	18:00:00	8ч 27м 51с	8ч 00м 00с	27м 51с	00с
Кейси																									11:15:29	10:00:00	19:35:53	18:00:00	8ч 20м 24с	8ч 00м 00с	20м 24с	1ч 15м 29с
Леонардо																									10:48:59	10:00:00	19:43:50	18:00:00	8ч 54м 51с	8ч 00м 00с	54м 51с	48м 59с
Микеланджело																									10:42:09	10:00:00	20:25:23	18:00:00	9ч 43м 14с	8ч 00м 00с	1ч 43м 14с	42м 09с
Рафаэль																									9:40:38	10:00:00	18:37:20	18:00:00	8ч 56м 42с	8ч 00м 00с	56м 42с	00с

3 февраля 2022 г. Четверг

Пользователь ↓																								Начало		Окончание		Общее время		Дисциплина		
	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	факт ↓	распис ↓	факт ↓	распис ↓	факт ↓	план ↓	сверх ↓	опозд ↓
Донателло																									8:46:44	10:00:00	15:54:58	18:00:00	7ч 08м 14с	8ч 00м 00с	00с	00с
Кейси																									12:02:43	нераб.	19:31:58	нераб.	7ч 29м 15с	00с	7ч 29м 15с	00с
Леонардо																									10:19:58	10:00:00	19:27:41	18:00:00	9ч 07м 43с	8ч 00м 00с	1ч 07м 43с	19м 58с
Микеланджело																									10:55:04	10:00:00	19:47:54	18:00:00	8ч 52м 50с	8ч 00м 00с	52м 50с	55м 04с
Рафаэль																									9:41:07	10:00:00	18:38:22	18:00:00	8ч 57м 15с	8ч 00м 00с	57м 15с	00с

Блокировки

Staffcop Enterprise позволяет предотвратить утечку данных путем блокировки каналов передачи в формате черных или белых списков на компьютерах и терминальных серверах, умеет автоматически изменять уровень контроля за сотрудником при обнаружении подозрительных действий.

Блокируйте файловые операции на основе правил.

- Блокировки запуска процессов и приложений
- Блокировка доступа к сайтам
- Блокировка USB-устройств по задаваемым группам файлов и идентификаторам
- Ограничение записи на съемные носители
- Блокировка буфера обмена при передаче контента в другое приложение
- Блокировка операций с файлами по контенту, атрибутам и цифровым меткам
- Блокировка подключения к Wi-Fi сетям
- Блокировка носителей информации при превышении порога передачи данных
- Блокировка APM по команде сервера

Удаленное
наблюдение
за АРМ
и перехват
управления

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

Администрирование

Система предоставляет инструментарий для помощи администраторам. В реальном времени можно не только удаленно подключиться к рабочей станции пользователя, чтобы проанализировать проблемы или детально изучить аномальную активность, но и получить доступ к управлению станцией. Например, чтобы оказать пользователю помощь или убрать из доступа нелегитимный файл.

Staffcop Enterprise позволяет работать с другими информационными системами, чтобы передавать или дополнять данные. Например, информация о присутствии сотрудников на работе поступает от СКУД или 1С. При расследования инцидентов данные из других систем могут передаваться в SIEM с помощью Syslog или API.

Изменение конфигурации контроля при наступлении определенного события

Ролевой доступ

Не всегда у администратора есть возможность оперативно среагировать на инцидент. При аномалиях в активности пользователя система автоматически изменяет набор правил для работы агента. Таким образом пользователь будет переведен под особый, более плотный контроль.

Система решает широкий спектр задач и зачастую для этого не нужен доступ ко всем ее элементам. В системе используется широкий набор прав для администраторов, позволяющий ограничить доступ вплоть до просмотра нужного отчета. Также можно предоставить доступ для управления системой, но ограничить доступ к данным.

Полное техническое сопровождение на этапе тестирования!

Дистрибутив и подробная документация на сайте www.staffcop.ru



Отдел продаж
+7 (499) 653 71 52
sales@staffcop.ru

Техническая поддержка
+7 (499) 638 28 09
support@staffcop.ru

ООО «АТОМ БЕЗОПАСНОСТЬ»

