Информационная безопасности предприятия и контроль деятельности сотрудников

Даниил Бориславский
Руководитель проектного офиса
ООО Атом Безопасность
db@staffcop.ru

staffcop®

- 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.

Зачем нужен контроль?

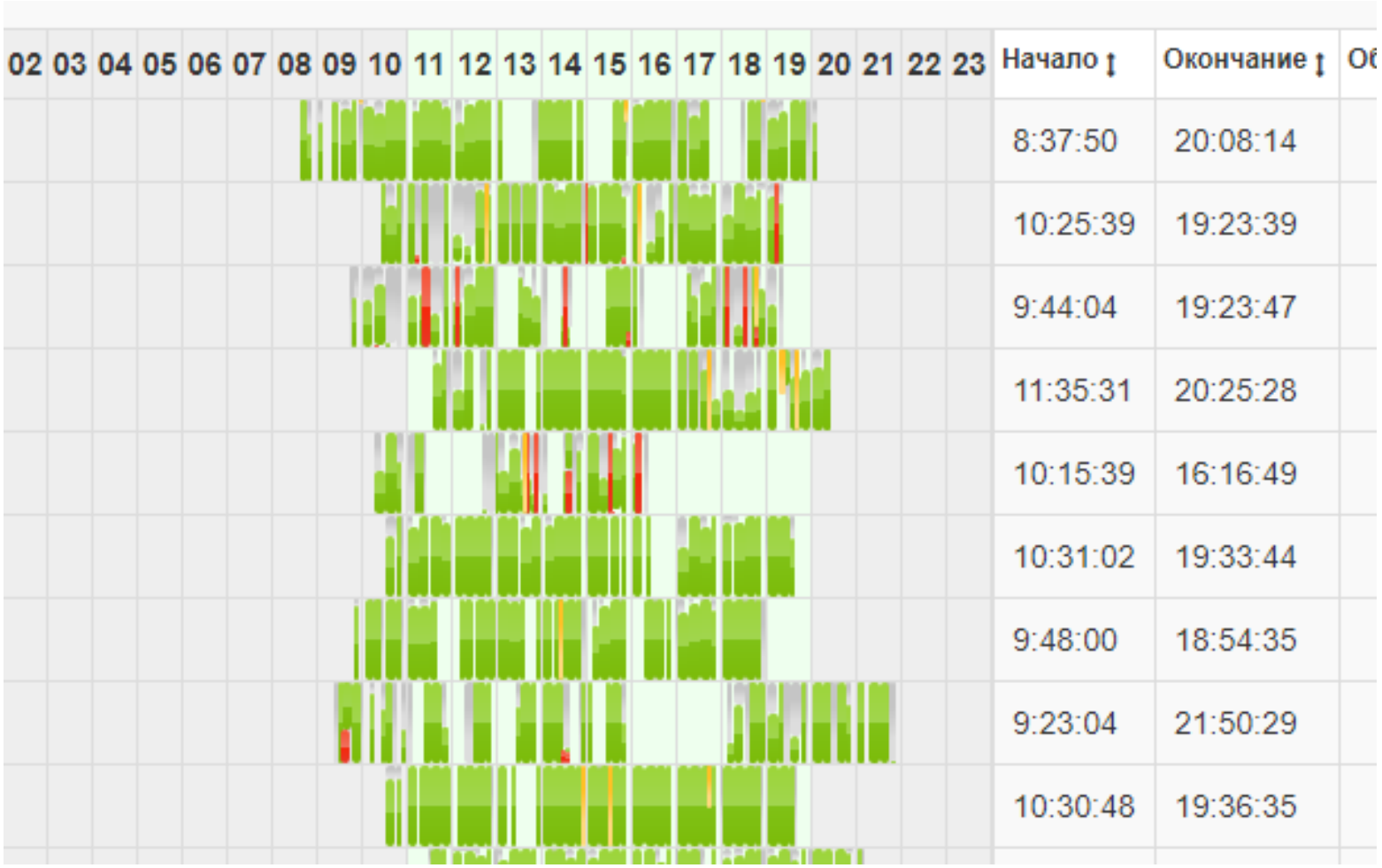
Лимит:

Учёт рабочего времени за период с 24 марта 2020 по 24 марта 2020

24 марта 2020 г. Вторник

Пользователь	00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23	Начало	Окончание	Общее время	Активное	Простой	Опоздание	Сверхурочные	Продуктивное	Непродуктивное	Нейтральное
		8:07:07	20:08:51	12ч 01м 44с	6ч 12м 31с	5ч 49м 13с	00с	1ч 09м 21с	00с	6ч 12м 31с	00с
Продуктивность											
Развлекательные ресурсы		6:12:53 (100.10%)									
Топ приложений											
chrome.exe		6:12:53 (100.10%)									
Топ сайтов											
youtube.com		5:40:29 (91.40%)									
twitch.tv		0:32:24 (8.70%)									

Зачем нужен контроль?



Дисциплина Активность Продуктивность

Зачем нужен контроль?

Общение с конкурентами | Выгрузка и печать | Панель управления | Админ | Меню (Admin)

События | Анализ | Учет времени | Отчеты | Добавить | Лимит:

Посещение сайтов

Пользователь: Полное имя	Дата: День	Сайт	Время активности
Арсений Есетовский	18-июнь-2020	searchinform.ru	00 ч 02 м 55 с

Переписка - количество

Пользователь: Полное имя	Дата: День	Переписка: Домен
Арсений Есетовский	18-июнь-2020	searchinform.ru

Переписка - подробно

Время	Тип	Компьютер	Пользователь	Приложение
2020-06-18 10:47:23	Почта	DemoZoneVM1	Арсений	thunderbird.exe

Панель управления | Админ | Меню (Admin)

Лимит:

						Контент
2020-06-14 16:05:0	DemoZoneVM2	Ксения	Ксения Касперов	Арсений Есетовс	Re: Проверка связи	
2020-06-14 16:01:1	DemoZoneVM2	Ксения	Ксения Касперов	Брославский Да	Данные	Скачать Входные цены.xlsx InterceptedFile
2020-06-14 15:45:3	DemoZoneVM2	Ксения	Ксения Касперов	Арсений Есетовс	Re: Проверка связи	Скачать Лист Microsoft Excel.xlsx InterceptedFile
2020-06-14 15:44:1	DemoZoneVM2	Ксения	Ксения Касперов	Арсений Есетовс	Проверка связи	

Зачем нужен контроль?

Пользователь: Полное имя	Сайт	Приложение: Заголовок окна	Количество событий
Арсений Есетовский	avito.ru	cisco asa - Авито — объявления в Новосибирске — Объявления на сайте Авито - Mozilla Firefox	6
Арсений Есетовский	avito.ru	Cisco 2821 ASA5510 Cisco 1760 Juniper srx100 купить в Кемерово с доставкой | Бытовая электро ника | Авито - Mozilla Firefox	2
Арсений Есетовский	avito.ru	Cisco asa5505 купить в Барнаул	
Арсений Есетовский	avito.ru	Cisco asa 5505 купить в Новоси х	
Арсений Есетовский	avito.ru	Cisco ASA 5505 купить в Новоси х	
Арсений Есетовский	avito.ru	Сетевой экран Cisco ASA5505 к - Mozilla Firefox	
Арсений Есетовский	avito.ru	Межсетевой экран Cisco ASA 5 вито - Mozilla Firefox	
Арсений Есетовский	avito.ru	Продам Cisco ASA5510-SEC-BU роника | Авито - Mozilla Firefox	
Арсений Есетовский	avito.ru	Авито — объявления в Новосиб	
Арсений Есетовский	avito.ru	Cisco asa5505 купить в Барнаул	
Арсений Есетовский	avito.ru	Cisco 2821 ASA5510 Cisco 1760 ника | Авито	

Отчеты

Cisco Маршрутизатор /свич /коммутатор / межсетевой — 1 500 ₽

Добавить в избранное | Добавить заметку | Вчера в 11:25

Купить с доставкой

Доставка в пункт выдачи

Гарантия возврата денег, если товар не подойдёт. Как это работает

Показать телефон

Написать сообщение
Отвечает около 30 минут

5,0 ★★★★★ 8 отзывов

52 объявления пользователя

Подписаться на продавца

08.07.2020 12:47:12

08.07.2020 12:47:04

08.07.2020 12:46:15

08.07.2020 12:46:06

08.07.2020 12:45:49

08.07.2020 12:45:22

08.07.2020 12:45:07

Зачем нужен контроль?

Зачем нужен контроль?

Федеральная служба по техническому и экспортному контролю

приказ ведомства №35 от 20.02.2020

об обеспечении безопасности КИИ

staffcop®

Система мониторинга для расследования инцидентов и контроля работы сотрудников

Учет рабочего времени

Эффективность персонала

Информационная безопасность

Расследование и инцидентов

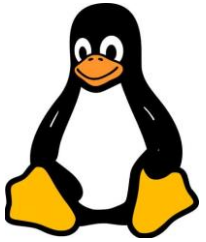
Удаленное администрирование

Новый уровень внутренней безопасности

Актуальные потребности

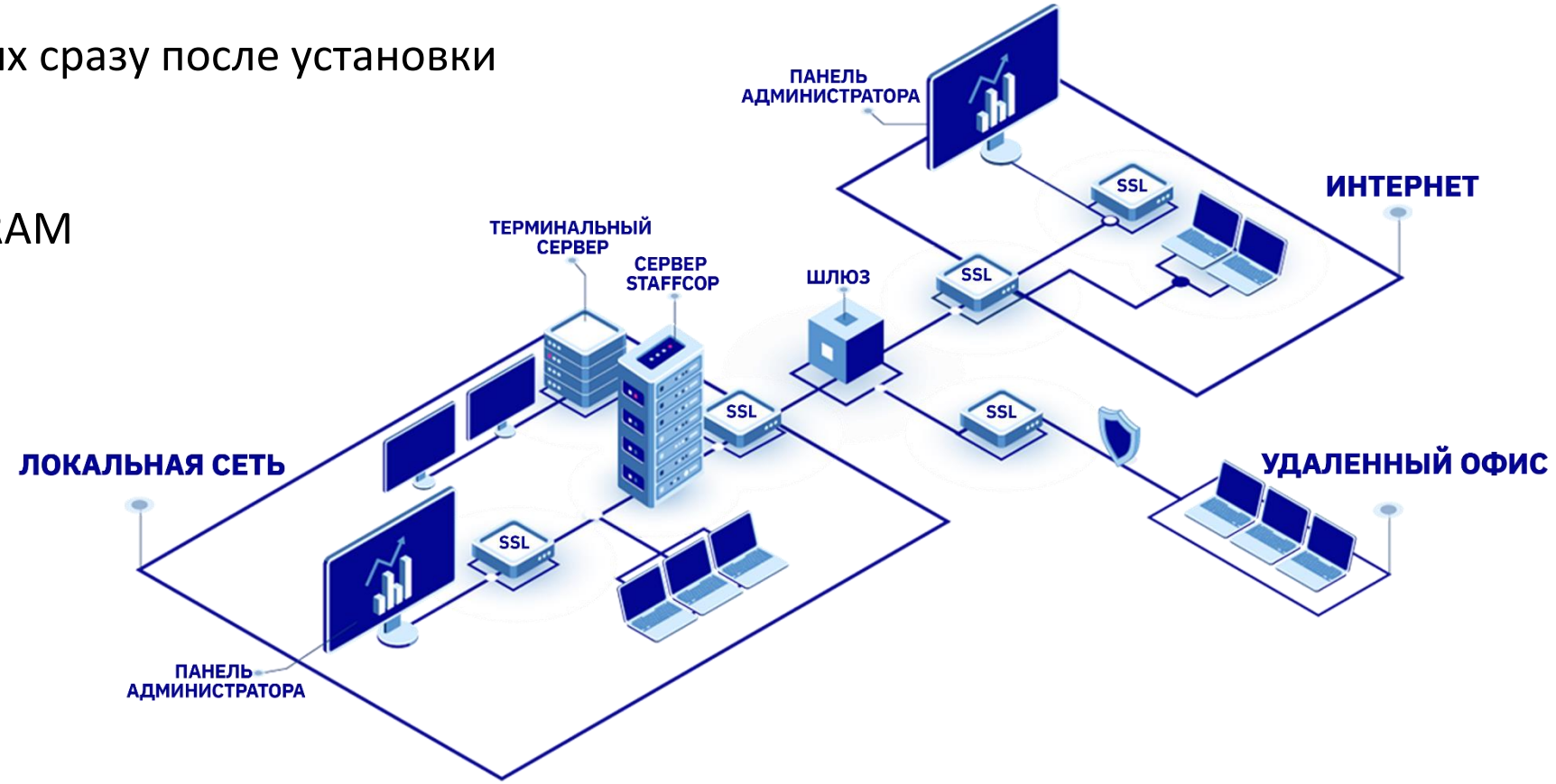
Технологии сервера:

ОС рабочих ПК и АРМ:



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



ubuntu

PostgreSQL

ASTRA LINUX®

- Нет дополнительных расходов за использование системы

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

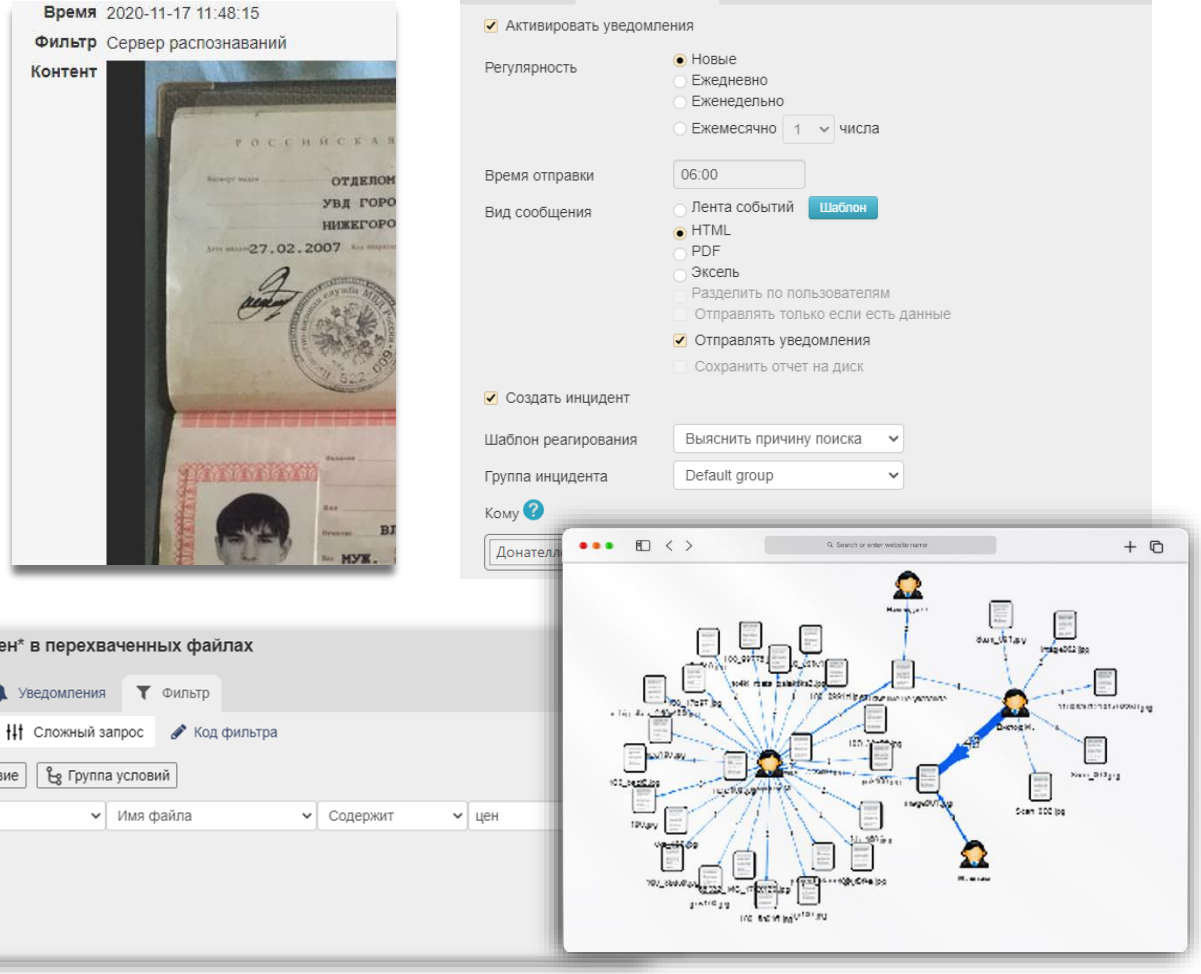
Теневое копирование файлов
— из электронной почты
— со съемных носителей
— переданных через интернет
— отправленных на печать

Аналитические возможности

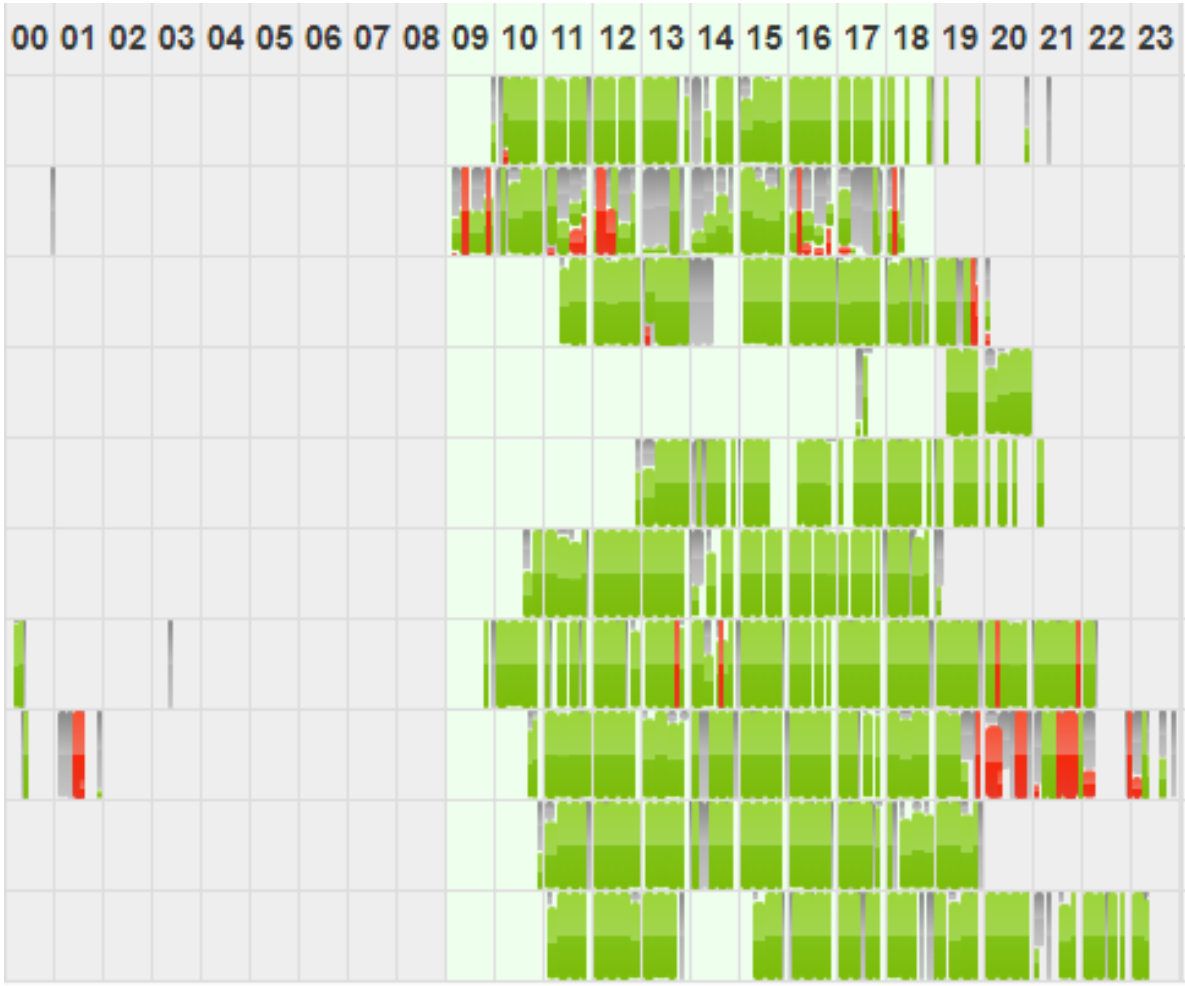
- Архив данных
- Конструктор многомерных отчетов
- Поиск по словам и регулярным выражениям
- Множество графов и диаграмм
- Синхронизация данных с AD

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



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

Управление и администрирование

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


Картинки о том как всё будет работать
Скриншоты и примеры как работает

Учёт рабочего времени

Инцидент: почта не из домена

Инцидент: переданный файл

Аспекты эксплуатации

Правовые

Технические

Административные

Правовые аспекты внедрения

- **№149 ФЗ «Об информации, информационных технологиях и о защите информации».**
- **№98 ФЗ «О коммерческой тайне».**
- **№152 ФЗ «О защите персональных данных».**

- Определить и довести до работников правила использования средств хранения, обработки и передачи информации .
- Разработать и довести до работников регламент проведения мониторинга.
- Получить согласие работников на проведение мониторинга использования им средств хранения, обработки и передачи информации.
- Включить положения об обязательстве работника соблюдать правила использования средств коммуникации и согласие на мониторинг в трудовой договор (дополнительное соглашение к трудовому договору).

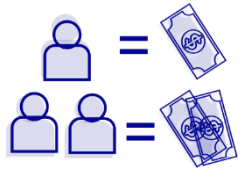
Технические аспекты внедрения и эксплуатации

- 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.
- Возможно, потребуется сертифицированная ФСТЭК версия.

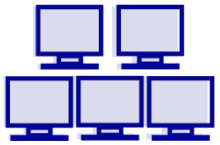
Преимущества Staffcop Enterprise

На opensource решениях,
не требует дополнительного
платного ПО.

Цена.



Единое решение
и гибкая политика
лицензирования.



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

Настраиваемые
отчёты и OLAP.

Решает задачи
разных подразделений

Входим в реестр отечественного
ПО и имеет
сертификат ФСТЭК.

Не блокирует
работу бизнеса.

Лёгкий и
функциональный
агент.

Тестируйте бесплатно до 3-х месяцев на парке машин любого размера.
Полнофункциональная версия. Техническое сопровождение проекта на всем протяжении.

Быстро

Развертывание пилотного проекта занимает не более одного дня.

Легко

Минимум усилий и ресурсов для запуска.

Комплексно

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

Благодарю за внимание!

Даниил Бориславский
Руководитель проектного офиса
ООО Атом Безопасность

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