Спецификация СпрутМонитор (локальная версия) https://sprutmonitor.ru/

Структура системы

Система построена по модульному принципу с использованием следующих подсистем:

- Сервер хранения и обработки данных
- Агентский модуль, устанавливаемый на АРМ пользователей
- Консоль управления
- Модуль OCR распознавания

Общие характеристики

- Возможность масштабирования и наращивания контура подключаемых АРМ пользователей
- Единая консоль управления настройками и конфигурациями.
- Удобный визуально-ориентированный интерфейс управления для использования основных функций системы и ее настройки без необходимости использования языков программирования и вызова внешних скриптов.
- Возможность анализа конфиденциальной информации (по словарям).
- Русскоязычный интерфейс управления.
- Возможность разграничения доступа различных категорий пользователей и администраторов к средствам управления системой.
- Возможность разделения прав между несколькими офицерами безопасности с сохранением функций по администрированию системы, с разделением прав просмотра с возможностью перекрестного контроля.
- Система полноценно функционирует на серверах под управлением ОС Microsoft Windows Server 2008 SP2/2008R2/2012/2012R2/2016/2019/2022 (x86 и x64)
- Клиентские модули работают на следующих ОС: Microsoft Vista, Windows 7/8/8.1, MS Windows Server 2003/2008/2008R2/2012/Windows 10/Windows 11 (x86 и x64)
- Система обеспечивает работу с СУБД Microsoft SQL Server (не ниже 2008).
- Система обеспечивает возможность работы в сетах как с доменной структурой (Active Directory), так и без нее.
- В системе реализован информационный обмен между компонентами системы на основе стандартного протокола TCP/IP.
- Система обеспечивает развертывание как вручную, так и через групповые политики домена Microsoft Active Directory.

Идентификация пользователей

- Система сопоставляет перехваченную информацию с учетными записями пользователями.
- Система опционально синхронизируется с Active Directory.

Контроль почты и веб трафика

- Перехват осуществляется непосредственно на АРМ пользователей.
- Система осуществляет контроль протоколов ICQ, Mail.Ru Агент, Jabber, Skype, Zoom, XMPP, Vkontakte, Facebook в режиме фильтрации.
- Система осуществляет перехват сообщений в web.whatsapp.com и web.telegram.org.
- Система осуществляет контроль протоколов FTP, IMAP, SMTP, POP3 в режиме фильтрации.

- Система имеет возможность осуществлять контроль протоколов HTTP/HTTPS в режиме фильтрации.
- Система имеет возможность контроля входящего и исходящего трафика, передаваемого по протоколу SMTP, электронных писем и вложений от MS Exchange Server, IBM Lotus Domino, Kerio MailServer, CommunigatePro, Sendmail, Postfix и других почтовых SMTP серверов.
- Система имеет возможность контроля исходящей почты и вложений в веб-почте mail.yandex.ru, mail.ru, gmail.com, roundcube, outlook.com.
- Система позволяет настраивать для перехваченного трафика проверочные условия.
- Система поддерживает отбор по следующим критериям:
    - Наличие вложений
    - Поиск текста в сообщениях по правилам: содержит, не содержит, совпадает, начинается, заканчивается (без учета регистра).
    - Поиск текстовых фрагментов по словарям терминов.
    - Проверка полей сообщения: отправитель (FROM), получатель (TO), обратный адрес (Reply To) на совпадение вхождения текстовых строк.
- Система поддерживает следующие автоматически выполняемые действия над сообщениями:
    - Вставку текста заданного содержания в начало или конец сообщения.
    - Доставлять сообщения адресату.
    - Осуществлять доставку уведомления заданного содержания об обрабатываемом сообщении на указанный адрес пользователя или администратора.
    - Осуществлять удаление вложения.
- Система имеет возможность задавать произвольное необходимое соответствие “Проверочное условие” – “Действие”.
- Система имеет возможность перехвата зашифрованных протоколов SSL. Сбор и расшифровка HTTPS трафика осуществляется локально на АРМ пользователя.
- Возможность задавать список приложений, интернет-трафик которых игнорируется.
- Возможность контроля облачных HTTP(S) сервисов и файл-хостингов: Google Docs, Office 365, Яндекс.Диск, Google.Drive, DropBox, Облако Mail.Ru, Microsoft OneDrive.
- Возможность контроля поисковых запросов: Google, Bing, Yandex, Rambler, Yahoo, Baidu, Aol, Ask.
- Возможность контроля сервисов социальных сетей: Facebook, Odnoklassniki, Vkontakte, Livejournal, Loveplanet, LinkedIn и других.
- Возможность контроля сервисов поиска работы superjob.ru, hh.ru, rabota.ru, job.ru, zarplata.ru, career.ru, vacansia.ru, rosrabota.ru, mnl.ru, vakant.ru и других.

Контроль печати

- Перехват информации о напечатанных документах, отправленных на печать при помощи локальных и сетевых принтеров.
- Перехват напечатанных документов путем сохранения файла спулера печати.
- Снятие скриншотов в момент печати документа.

Файловый контроль

- Перехват информации о файловых операциях (открытие, чтение, запись, переименование, удаление)
- Система имеет возможность разграничения доступа к внешним устройствам по серийному номеру устройства, пользователю, дате и времени.

- Разграничение операций с файлами на основе политик доступа, регламентирующих разрешенные операции с файлами, в т.ч. на USB-носителях и сетевых папках.
- Контроль доступа по названию файла.
- Теневое копирование файлов при следующих операциях, выполняемых на АРМ пользователя: операций с использованием буфера обмена, файловые операции, файловые операции с USB-дисками.

Контроль экрана

- Функционал снятия снимков экрана с АРМ пользователей с заданной периодичностью в форматах PNG, JPG, GIF, в т.ч. в привязке с заданному процессу ОС.
- При наличии на компьютере нескольких активных сессий (терминальный сервер) снимки экранов будут создаваться с каждой пользовательской сессии.
- При наличии нескольких мониторов при снятии снимков будет создаваться один графический файл, содержащий снимки всех рабочих столов пользователей.
- Возможность скорректировать расписание снятия скриншотов при посещении определенных (настроенных заранее) вебсайтов, активации видеоконференций, нажатии клавиши PrintScreen.
- Видеозапись происходящего на экранах мониторов согласно настроенному расписанию или событиям.
- Создание снимков посредством подключенной к АРМ веб-камеры по заданному расписанию.
- Возможность просмотра процессов, которые выполнялись в момент снятия экрана или видеозаписи.
- Одновременный просмотр экрана одного или нескольких пользователей в режиме реального времени.
- Возможность экспорта и сохранения снимков.
- Защита экрана методом наложения водяных знаков.

Контроль активности пользователей и приложений

- Контроль активности сотрудников в запускаемых ими приложениях или на сайтах.
- Поиск перехваченных данных за указанный период времени применительно к заданным пользователям, имени активного процесса, продолжительности активности.
- Использование перехваченных данных для генерации отчетов и оповещений.
- Возможность автоматической категоризации любых посещенных сайтов на тематические группы, используя локальный классификатор сайтов.
- Возможность автоматической категоризации любых запущенных программ на тематические группы, используя локальный классификатор программ
- Возможность ограничения работы пользователей с приложениями на АРМ по черному или белому списку, включая приложения терминальной сессии.
- Возможность ограничения использования буфера обмена.

Контроль данных, вводимых с клавиатуры и буфера обмена

- Перехват нажатий клавиш в любых запущенных приложениях, включая нажатия системных клавиш и их сочетаний.
- Перехват текстовой и графической информации, помещенной пользователем в буфер обмена.
- Блокировка нажатий клавиши PrintScreen.
- Возможность задать правила логирования пользователям или группам.
- Индексирование перехваченных текстов, файлов.

- Возможность поиска вводимого с клавиатуры или помещаемого в буфер обмена содержимого за определенный период времени применительно к заданным пользователям, процессам.
- Экспорт

Подсистема OCR распознавания графических файлов

- Возможность извлечения текста на русском и английском языке из графических файлов с помощью технологии OCR посредством свободно распространяемого OCR модуля Tesseract и облачной версии ABBYY.
- Распознавание текста осуществляется на сервере распознавания.

Подсистема AR распознавания аудио записей

- Возможность извлечения текста на русском и английском языке из аудио-записей с помощью технологии Audio Recognition посредством движков Facebook Wix и Yandex.SpeechKit.
- Распознавание текста осуществляется на сервере распознавания.

Подсистема отчетов

- Система имеет подсистему отчетности в виде графических отчетов и сводных таблиц.
- Возможность разделения прав доступа к отчетам.
- Возможность выставлять метки на выбранные записи.
- Возможность генерации отчетов по расписанию.
- Возможность рассылки сгенерированных отчетов на почтовые адреса выбранных пользователей.

Дополнительные возможности

- Экспорт информации и отчетов в форматы Doc, Csv, Pdf, HTML.
- Фильтр инциндентов ИБ по типам данных, времени, сотрудникам и другим критериям.

Функционал консоли управления и администрирования

- Возможность назначения конфигураций агентским модулям с использованием визуального дерева подключенных АРМ.
- Возможность назначения конфигурации как отдельному пользователю, так и группе пользователей.