ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на оказание услуг по поставке лицензий системы контроля за утечками информации в информационных системах

Общие требования к программному обеспечению:

1. Программное обеспечение должно поддерживать работу в сетях любой конфигурации и сложности, а также поддерживать возможность подключения агентов к серверу через сеть Интернет.
2. Серверная и агентская части должны поддерживать возможность установки на операционные системы семейства Linux и использовать базы данных PostgreSQL и ClickHouse.
3. Серверная часть программного обеспечения, реализующая функционал управления агентами, хранения собираемой информации и формирования отчетов должна поддерживать возможность установки всех необходимых компонентов на одном сервере.
4. Для сбора информации должен устанавливаться только один модуль (агент) на один ПК.
5. Агент должен быть унифицирован для работы на терминальных серверах и рабочих станциях пользователя.
6. Для доступа к собранной информации, управления политиками безопасности, настройки конфигурации агента должна использоваться единая консоль администратора с возможностью разграничения по правам и ролям, реализованная на тонком клиенте.
7. Система должна иметь возможность вертикального и горизонтального масштабирования.
8. Серверные компоненты не должны требовать наличия у заказчика дополнительных платных лицензий на программное обеспечение.
9. Задержка обновления отчетов должна составлять не более 15 минут при максимальной загрузке системы.

Требования к архитектуре программного обеспечения:

1. Архитектура системы должна обеспечивать выполнение OLAP запросов в реальном режиме времени.
2. Для исполнения аналитических запросов в реальном режиме времени система должна иметь возможность дополнительно использовать БД типа columnar store (Clickhouse).
3. Метаданные должны хранится в БД, медиа файлы в файловом хранилище.
4. Хранение файлов должно обеспечиваться в режиме "кольцевой буфер" с возможностью автоматического перемещения на долговременное хранилище.
5. Протокол обмена между агентом и сервером, а так же доступ в панель администратора должен быть защищен шифрованием семейства TLS (на основе клиентских сертификатов).

6. Интерфейс администратора должен обеспечивать вывод суммарной (агрегированной) информации на основе больших массивов данных, структурированных по многомерному принципу.

7. Интерфейс администратора должен поддерживать распределение полномочий основанных на ролях, в том числе заданных в Active Directory

8. Модуль агента должен поддерживать работу под ОС: Microsoft Windows XP SP3, Vista SP2, 7, 8, 8.1, 10, Server 2003, Server 2008, Server 2008 R2, Server 2012, Server 2012 R2; Linux Debian, Ubuntu, Mint, Gentoo, Calculate, Astra, Rosa, Centos, Fedora, SuSe, Archlinux, Manjaro.

Требования к администрированию системы:

1. Установка агентов должна происходить централизована с помощью групповых политик AD, с помощью инсталлятора модуля агента и локально, с помощью запуска инсталлятора на машине пользователя.

2. Установка по списку ПК из AD: подключение из инсталлятора агента к контроллеру домена для выбора компьютеров для установки; назначение конфигураций мониторинга по группам AD; создание учетных записей веб-консоли через AD.

3. Модуль агента должен уметь отправлять собранные данные на несколько ip-адресов сервера.

4. Обновление агентов должно происходить автоматически, централизовано после подтверждения администратором системы.

5. Должна обеспечиваться возможность настройки длительности хранения информации в базе данных, в том числе возможность автоочистки файлового хранилища без удаления данных из базы данных.

6. Предупреждение о заполнении дисков БД. Отправка администратору системы уведомлений по электронной почте о системных событиях (системные ошибки, предупреждения, оповещение при срабатывании политик безопасности и т.д.).

7. Должна обеспечиваться настройка максимальной скорости передачи перехваченных данных от агента на сервер.

8. Журнал действий администраторов системы в консоли администратора.

9. Автосмена имени агента, при смене названия компьютера.

Требования к функциональным возможностям системы:

Общие требования к логируемой информации:

Должны фиксироваться следующие типы событий действий пользователя:

- вход/выход из системы;
- активность пользователя в приложениях и на сайтах;
- подключение к удаленному рабочему столу, перехват управления;
- запись видео рабочего стола;
- снимок экрана;
- снимок с веб-камеры;

- операции с файлами;
- теневые копии перехваченных файлов;
- печать документов;
- буфер обмена;
- ввод с клавиатуры;
- реестр оборудования;
- реестр установленных программ;
- запись с микрофона;
- посещение веб-ресурсов;
- FTP;
- сетевые подключения;
- интернет-мессенджеры;
- почта;
- установка ПО;
- запуск и завершение приложения;
- внешние диски и устройства;
- присутствие на рабочем месте.

Должны фиксироваться следующие атрибуты логируемой информации:

- агент:
    - ip-адрес;
    - дополнительная метка;
    - название ПК;
    - статус;
    - версия OS;
    - версия агента;
- учетная запись пользователя:
    - комментарий;
    - отдел;
    - организация;
    - телефон;
    - полное имя;
    - почта;
    - должность;
    - домен;
    - пользователь;
- приложение:
    - полный путь;
    - название;
    - описание;
- сайт:
    - полный домен;
    - протокол;
    - URL;
    - основной домен;
    - тип контента;
- сетевая активность:

- ip-адрес;
- сетевой порт;

- файл:
  - хеш файла;
  - операции;
  - тип контента;
  - имя файла;
  - тип диска;
  - расширение;
  - путь;
- устройства:
  - устройства;
  - ID устройства;
  - тип диска;
  - класс устройства;
  - тип устройства;
- переписка:
  - домен получателя;
  - отправитель;
  - все получатели;
  - формат сообщения;
  - направление;
  - домен отправителя;
  - получатель;
  - чаты;
  - канал общения;
- дата:
  - час суток;
  - часовой пояс;
  - день недели;
  - по годам;
  - по месяцам;
  - по дням;
  - по часам;
  - по минутам;

Требования к реализации функционала мониторинга системы:

Модуль агента под ОС Windows:

- вход/выход из системы:
  - фиксация времени логина/логаута пользователя под учетной записью. В случае использования системы в разных часовых поясах, время логина/логаута в отчетах пользователя фиксируется в часовом поясе ПК/, где установлен агент.

- активность пользователя в приложениях и на сайтах:

- фиксация активности пользователя в приложениях и на сайтах, общее время работы пользователя за сутки, время простоя, опозданий, переработок. Автоматическое распределение активности пользователя в продуктивных и непродуктивных приложениях и сайтах и их группах. Активность пользователя считается с учетом плавающего, скользящего графика, праздничных дней. Активность пользователя на разных ПК должна содержаться в одном агрегированном отчете по пользователю.

- видео рабочего стола:

- запись видео должна производиться непрерывно на всех ПК в оригинальном разрешении, должна быть возможность настраивать временный интервалы видео.

- подключение к удаленному рабочему столу, перехват управления:

- подключение к удаленному рабочему столу должно быть реализовано с помощью VNC. Должна иметься возможность захвата управления мышью и клавиатурой. Должна иметься возможность заблокировать управление удаленной машиной пользователем.

- снимок экрана:

- снятие снимков экрана должно настраиваться в зависимости от смены активного окна на рабочем столе, с определенной периодичностью.

- возможность устанавливать периодичность снятия скриншотов для определенных приложений и сайтов с изменяемым интервалом времени для каждого приложения. Должна иметься возможность изменять качество снимков экрана в процентном отношении.

- снимок с веб-камеры:

- снимки с веб-камеры должны настраиваться и выполняться с определенной частотой.

- операции с файлами:

- должен обеспечивать на локальных и сетевых дисках регистрацию следующих событий с файлами: создание, чтение, запись, удаление, переименование, изменение расширения, перемещение, копирование.

- фильтрация событий операций с файлами по расширению файла, типу контента, типу диска, имени файла, пути.

- настраивание автоматическое создание теневой копии файла при операциях с файлами: создание, чтение, запись, удаление, переименование, изменение расширения, перемещение, копирование, по имени файла, директории нахождения;

- обнаружение шифрованных ZIP/RAR архивов;

- должна иметься возможность добавлять или исключать из мониторинга файловой активности файлы по расширению, по имени, по месторасположению, по ip, по приложениям с помощью черного и белого списка.

- перехваченные файлы:

- теневая копия файлов отправленных по Skype;

- теневая копия файлов отправленных на внешние носители;
- теневая копия файлов отправленных на печать;
- теневая копия файлов отправленных на сетевые диски
- подсчет хеш-суммы теневых копий файлов;
- исключение создания теневых копий файлов по размеру, по названию приложения;
- система должна индексировать файлы следующих форматов:

- Adobe Acrobat (*.pdf);
- Ansi Text (*.txt);
- ASCII Text;
- ASF (метаданные) (*.asf);
- CSV (Comma-separated values) (*.csv);
- DBF (*.dbf);
- EML files (электронные письма, сохраненные Outlook Express) (*.eml);
- HTML (*.htm, *.html);
- JPEG (метаданные) (*.jpg);
- MHT-архивы (HTML-архивы, сохраненные Internet Explorer) (*.mht);
- MSG files (электронные письма, сохраненные Outlook) (*.msg);
- Microsoft Excel (*.xls) Microsoft Excel 2003 XML (*.xml);
- Microsoft Excel 2007 и выше (*.xlsx);
- Microsoft Outlook Express 5 и 6: базы сообщений (*.dbx);
- Microsoft PowerPoint (*.ppt);
- Microsoft Rich Text Format (*.rtf);
- Microsoft Word for DOS (*.doc);
- Microsoft Word for Windows (*.doc);
- Microsoft Word 2003 XML (*.xml);
- Microsoft Word 2007 и выше (*.docx);
- Multimate version 4 (*.doc);
- OpenOffice версий 1, 2 и 3: документы, электронные таблицы и презентации (*.sxc, *.sxd, *.sxi, *.sxw, *.sxg, *.stc, *.sti, *.stw, *.stm, *.odt, *.ott, *.odg, *.otg, *.odp, *.otp, *.ods, *.ots, *.odf) (включая OASIS Open Document Format для офисных приложений).

- ввод с клавиатуры:
  - поддержка ввода символов Unicode.
  - низкоуровневый кейлоггер для перехвата паролей при входе в ОС;
  - перехват паролей в диалоговых окнах windows;
  - отключение функции перехвата паролей;
  - визуализация удаленных пользователем символов;
  - исключение перехвата ввода клавиатуры в приложениях по черному и белому списку.

- запись с микрофона:
  - запись звука должна вестись непрерывно со всех микрофонов подключенных к ПК пользователей, где установлен агент;

- задавать длительность аудиофайлов;
- задавать длительность тишины в аудиодорожке для автоматического выключения записи;
- задавать уровень записи;
- задавать качество аудиозаписи;
- задавать шумовой порог, для игнорирования сигнала ниже заданного;
- прослушивать аудиофайл в формате: mp3, ogg, wav, wma.
- просмотреть все действия пользователей в интервале записи аудиопотока.

- посещение сайтов:
- фиксация всех посещенных сайтов по http/s;
- перехват содержимого форм на сайтах;
- фиксация поисковых запросов;
- возможность переименования сертификата для перехвата шифрованного трафика;
- добавление в исключение подмены сертификата для шифрованного трафика;
- добавление в исключение мониторинга http/s сайтов по ip-адресу, порту, названию приложения.

- сеть:
- мониторинг используемых ip-адресов и портов;

- интернет-мессенджеры:
- перехват исходящих/входящих сообщений skype7, skype12, VK, по протоколам: SIP, XMPP, OSCAR(icq), WIM(icq), MRIM(mailruagent), Yahoo и шифрованные их аналоги;
- создание теневой копии файла отправленного через интернет-мессенджер;
- фиксация звонка через интернет-мессенджеры с указанием длительности звонка и абонентов;

- почта:
- перехват исходящих/входящих сообщений по протоколам: pop, smtp, imap, mapi (через outlook), шифрованные их аналоги, отправленных через веб-почту (gmail, mail, yandex, rambler, yahoo и т.д.);
- перехват теневых копий файлов отправленных по почте;
- фильтрация почтовых отправлений по домену получателя, домену отправителя, каналу общения, направления, формата сообщения, содержимого файлов и их форматов.

- устройства:
- мониторинг всех подключаемых устройств;
- распределение устройств по классам;
- фиксация файловых операций на съемных носителях.

- присутствие на рабочем месте:

- всплывающее диалоговое окно на ПК пользователя при неактивности в течении определенного времени для указания причины неактивности за ПК;

- всплывающее диалоговое окно с тестом на ПК пользователя для проверки нахождения на рабочем месте.

Требования к функционалу блокировки системы:

- блокировка сайтов по черному и белому списку, в том числе и на кириллице;
- блокировка подключения внешних устройств по классу устройств, по ID устройства по черному и белому списку;
- запрет копирования информации с usb-носителей, только чтение;
- блокировка записи на CD;
- блокировка запуска приложений по черному и белому списку;
- блокировка установки ПО.

Модуль агента под ОС Linux:

- локальный/удалённый вход/выход из системы (включая ssh подключения);
- слежение за .log файлами;
- активность пользователя на сайтах;
- история посещения сайтов;
- активность пользователя в приложениях;
- перехват буфера обмена;
- регистрация фактов печати на принтерах;
- запись звука со встроенных микрофонов;
- управление агентом через конфигурацию в веб-консоли Staffcop.
- скриншоты по интервалу;
- скриншоты по активности (по переключению/смене заголовка окна);
- степень компрессии и формат скриншотов;
- атрибуты приложений - имена окон и иконки;
- кейлоггер;
- альтернативный модуль кейлоггера, поддерживающий работу вне X Windows;
- кейлоггер на уровне ядра Линукс для контроля терминалов серверов, систем, где невозможен перехват клавиатуры X-сессий (Astra).
- привязка ввода с клавиатруры (X11-кейлоггер) к событиям активности на сайтах;
- поисковые запросы в браузерах;
- определения X-сессий;
- история ввода терминальных команд;
- функции управления агентом в командной строке;
- подключение USB устройств;
- подключение внешних дисков;
- интеграция с Astra Linux.
- слежение за системными лог-файлами с управлением правилами мониторинга через конфигурацию агента;

- файловые операции. Определение действий с файлами, поддержка правил мониторинга (черный/белый списки контроля);
- теневые копии файлов при перехвате файловых операций;
- тип событий «Запись лог-файла»

Требования к аналитике системы:

- сквозной поиск по всем событиям и теневым копиям текстовых файлов и документов (.txt, .doc, .rtf, .pdf и др.). Поиск можно производить по ключевым словам, фразам и регулярным выражениям. Поиск по ключевым словам и фразам производится с учетом морфологии;
- построение запросов для фильтров с условиями равно/не равно и содержит/не содержит, с возможность комбинировать условия логическими операторами И/ИЛИ;
- формирование отчетов и политик безопасности по атрибутам перехваченных событий;
- визуализация всех типов отчетов в любом из видов круговой, тепловой, линейной диаграммы, гистограммы, графов взаимосвязей, таблиц и списков;
- расследование инцидентов по цепочке, быстрый переход об общего к частному, составление аналитических отчетов по выбранным срезам данных;
- карточка измерения – сводный отчет, отображающий характеристики объекта или множества объектов и события, с ними связанные;
- автоматическое разграничение продуктивной и непродуктивной деятельности;
- возможность построения графа связей между сотрудниками;
- возможность построения схемы передачи информации между сотрудниками;
- вход под учётной записью сотрудника с нехарактерного ПК;
- увеличение количества распечаток;
- увеличение объёма почтовой переписки сотрудника;
- увеличение количества копируемых файлов;
- взаимодействие с контактами, нехарактерными для подразделения сотрудника;
- работа нестандартных процессов на АРМ;
- аномалии, связанные с фиксацией многократных попыток выполнения запрещённых действий;
- попытки доступа/чтения файлов из нехарактерных для сотрудника директорий;
- большое количество создаваемых сотрудником снимков экрана;
- проявление активности под учётной записью сотрудника в нерабочее время.

Требования к возможностям интеграции системы:

- возможность выгрузки данных в форматы SQL, CSV, HTML;
- возможность выгрузки данных посредством web-API;
- возможность интеграции со сторонними источниками данных