SoftControl

DLP 6.1.398

Методика тестирования

Уважаемый пользователь!

ООО "АРУДИТ СЕКЬЮРИТИ" благодарит Вас за то, что выбрали продукт SoftControl DLP Client. Специалисты компании постарались, чтобы наше программное обеспечение отвечало самым высоким требованиям в области защиты информации и в то же время было простым и удобным в работе. Мы надеемся, что SoftControl DLP Client будет Вам полезен.

Почтовый адрес:

127106, Россия, Москва

Нововладыкинский проезд, дом 8, стр. 3

ООО "АРУДИТ СЕКЬЮРИТИ"

Телефон:

+7 499 201-55-12

Факс:

+7 499 201-55-12

Электронная почта:

Общие вопросы и предложения: support@safensoft.com

Коммерческие вопросы: sales@safensoft.com

Веб-сайт компании: safensoft.com

Содержание

1. Введение

SoftControl DLP Client предназначен для контроля действий пользователей корпоративной сети и обеспечивает информационную безопасность компании путем защиты от инсайдерских инцидентов. SoftControl DLP Client осуществляет сбор данных об активности пользователей, позволяя службе безопасности вести полноценный мониторинг доступа персонала к информации, представляющей коммерческую тайну, и другим конфиденциальным данным. Полученные отчеты могут служить источником для ретроспективного анализа защиты от утечек информации, контроля эффективности использования рабочего времени и другой аналитики.

В данном документе приведена методика тестирования установленного продукта.

2. Подготовка стенда

Для проведения тестирования потребуются два компьютера – физических или виртуальных – с возможностью подключения USB-накопителей. Компьютеры должны быть доступны друг другу по сети. На первый компьютер («сервер») устанавливается SoftControl Service Center (см. «Руководство администратора SoftControl Service Center»). На второй компьютер (далее «клиентский компьютер») устанавливается SoftControl DLP Client (см. «Руководство по установке SoftControl DLP Client»). SoftControl DLP Client подключается к SoftControl Service Center.

3. Тестовые задания

Для выполнения каждого задания необходимо создать указанные в задании объекты на клиентском компьютере, создать в SoftControl Admin Console настройки подразделения, включающие соответствующее правило, применить созданные настройки, осуществить действия на клиентском компьютере, и затем просмотреть лог устройства в SoftControl Admin Console.

Во всех настройках на вкладке **DLP** → **Сбор данных** следует выставить флажок **Собирать данные**.

3.1 Наблюдение за файловой системой

В настройках вкладки **Лог устройств** в SoftControl Admin Console добавьте колонки **Путь к файлу** и **Маска доступа**, либо включите требуемый фильтр: **Фильтры** → **Фильтры событий DLP** → **Файл**.

Таблица 1. Тестирование наблюдения за файловой системой

Задание	Ожидаемый результат
Мониторинг чтения файла	
1) Создайте файл *C:\file1.txt*. 2) Задайте правило наблюдения за этим файлом: укажите путь *C:\file1.txt*, выставите флажок **Чтение**. Примените настройки. 3) Откройте файл с помощью Блокнота (*Notepad.exe*).	В логе должна появиться строка, содержащая *C:\file1.txt* в графе **Путь к файлу** и **Чтение** в графе **Маска доступа**.
Полный мониторинг файла и папки	
1) Создайте правило наблюдения за файлом *C:\file2.txt*, пока не существующим: укажите путь *C:\file2.txt*, выставите все флажки, кроме **Теневая копия** и **Запись видео**. 2) Создайте правило наблюдения за директорией *C:\dir1*, пока также не существующей. Укажите путь *C:\dir1\#**#*, также выставите все флажки, кроме **Теневая копия** и **Запись видео**. 3) Примените настройки. Примечание: наблюдение за переименованными объектами не производится. 4) Создайте файл *C:\file2.txt*. Откройте и запишите туда что-либо, сохраните. Переименуйте файл. Еще раз измените. Переименуйте файл, вернув его исходное название. Измените. Удалите. Создайте файл	В логе должна появиться строка на каждое действие, содержащая *C:\file2.txt* в графе **Путь к файлу** и **Создание**, **Чтение** и т.д. в графе **Маска доступа**. Такие же записи должны появиться для действий с директорией *C:\dir1*. Убедитесь, что после переименования *file2.txt* и *dir1* действия над ними не зафиксированы в логе, а после возврата файлу и каталогу исходных имен события снова отслеживаются.

	Задание	Ожидаемый результат
	снова. 5) Создайте директорию *C:\dir1*. Создайте в этой директории файл *C:\dir1\file3.txt*. Откройте и запишите туда что-либо, сохраните файл. Переименуйте файл, затем удалите его. Переименуйте директорию в *dir12*. Создайте файл *C:\dir12\newfile.txt*. Переименуйте директорию, вернув ее исходное название – *dir1*. Измените файл *C:\dir1\newfile.txt*.	
	Наблюдение за объектами файловой системы с теневым копированием	
1	1) В разделе **DLP** → **Наблюдение** → **Теневое копирование** выставите флажок **Включить теневое копирование**. Оставьте поле **Локальный путь сохранения файлов** пустым; таким образом, копии будут сохраняться в *C:\Program Files\SafenSoft\DLP Client\Backups*. 2) Создайте на клиентском компьютере файлы *C:\file4.txt* и *C:\file5.txt*. Задайте правила наблюдения за этими файлами: укажите пути *C:\file4.txt* и *C:\file5.txt*, выставите флажки **Изменение**, **Теневая копия** в первом правиле и **Удаление**, **Теневая копия** во втором. 3) Примените настройки. 4) Измените оба файла. Убедитесь в том, что в директории с резервными копиями появился один файл с расширением *.bkp* . 5) Удалите оба файла.	При изменении обоих файлов в логе появляется строка, упоминающая о событии изменения *file4.txt*; нажатие на выделенное розовым поле в этой строке позволяет открыть резервную копию. Аналогично при удалении обоих файлов в логе появляется только запись о *file5.txt*.
2	В разделе **DLP** → **Наблюдение** → **Теневое копирование** в поле **Локальный путь сохранения файлов** введите *C:\copies*. Повторите первое задание и убедитесь, что копии теперь оказываются в указанной директории.	

3.2 Наблюдение за реестром

В настройках вкладки **Лог устройств** в SoftControl Admin Console добавьте колонки **Ветка реестра** и **Маска доступа**, либо включите требуемый фильтр: **Фильтры** → **Фильтры событий DLP** → **Реестр**.

Для выполнения этих заданий обязательны права администратора на клиентском компьютере либо просто наличие прав на изменение реестра. Корневые разделы реестра в пути, задаваемом в правилах, должны быть указаны следующим образом:

Таблица 2. Обозначения путей в реестре

Раздел реестра	Обозначение в правилах SoftControl DLP Client
HKEY_CLASSES_ROOT	*\REGISTRY\MACHINE\SOFTWARE\CLASSES*
HKEY_LOCAL_MACHINE	*\REGISTRY\MACHINE*
HKEY_CURRENT_USER	*\REGISTRY\USER\<SID>* для пользователя с указанным идентификатором безопасности (*<SID>*)
HKEY_USERS	*\REGISTRY\USER*

Таблица 3. Тестирование наблюдения за реестром

Задание	Ожидаемый результат
Наблюдение за ключом реестра	
1) Задайте правило для реестра, укажите путь *\REGISTRY\MACHINE\SYSTEM\Key1*, выставите все флажки, кроме **Теневая копия** и **Запись видео**. Примените настройки. 2) Создайте ключ *HKEY_LOCAL_MACHINE\SYSTEM\Key1*. Создайте параметр *VALUE1* произвольного типа и с любым значением. Измените его значение. 3) Создайте подключ *Subkey1*, а в нем параметр *VALUE2*. Измените его значение. 4) Переименуйте *Key1*. Верните исходное название.	В логе в SoftControl Admin Console должны отразиться действия для *Key1* и *VALUE1*, но не для *Subkey1* и *VALUE2*.
Мониторинг ключа и всех вложенных объектов реестра	
1) Задайте правило для реестра, укажите путь *\REGISTRY\MACHINE\SYSTEM\Key2\#**#*. Маска #**# подразумевает наблюдение за всеми вложенными объектами, а не только за самим разделом. Также выставите все флажки, кроме **Теневая копия** и **Запись видео**. 2) Примените настройки. 3) Создайте ключ *HKEY_LOCAL_MACHINE\SYSTEM\Key2*. Создайте параметр *VALUE3* произвольного типа и с любым значением. Измените его значение. 4) Создайте подключ *Subkey2*, а в нем параметр *VALUE4*. Измените его значение.	Для *Key2* будут отражены в логе все действия с ним и его подключами и параметрами.
Наблюдение за объектами реестра с теневым копированием	
1) В разделе **DLP** → **Наблюдение** → **Теневое копирование** выставите флажок **Включить теневое копирование**. Оставьте поле **Локальный путь сохранения файлов** пустым; таким образом, копии будут сохраняться в *C:\Program Files\SafenSoft\DLP Client\Backups*. 2) Создайте ключ *HKEY_LOCAL_MACHINE\SYSTEM\Key3*, а в нем – пара-	После изменения *VALUE5* в логе появляется строка, упоминающая о событии изменения этого ключа; нажатие на выделенное розовым поле в этой строке поз-

Задание	Ожидаемый результат
метр *VALUE5*. 3) Задайте правило для реестра, укажите путь *\REGISTRY\MACHINE \SYSTEM\Key3\#**#*. Выставите флажки **Изменение**, **Удаление**, **Теневая копия**. 4) Примените настройки. 5) Измените значение *VALUE5*. Убедитесь в появлении в директории с резервными копиями экспортированного ключа *HKEY_LOCAL_MACHINE \SYSTEM\Key3* со старым значением *VALUE5*. 6) Удалите ключ. Убедитесь в том, что была сохранена еще одна копия ключа. 7) В разделе **DLP** → **Наблюдение** → **Теневое копирование** в поле **Локальный путь сохранения файлов** введите *C:\copies*. Повторите первое задание и убедитесь, что копии теперь оказываются в указанной директории.	воляет открыть резервную копию. После удаления появляется еще одна запись в логе, уже со вторым значением *VALUE5*.

3.3 Мониторинг ввода с клавиатуры

Таблица 4. Тестирование мониторинга ввода с клавиатуры

Задание	Ожидаемый результат
1) В настройках вкладки **Лог устройств** в SoftControl Admin Console добавьте колонку **Записанные данные**, либо включите требуемый фильтр: **Фильтры** → **Фильтры событий DLP** → **Монитор клавиатуры**. В настройках подразделения на вкладке **Сбор данных** выставите флажок **Ввод текста с клавиатуры**. 2) Примените настройки. 3) На клиентском компьютере произвольно вводите текст в любых программах – Блокнот (*Notepad.exe*), командная строка, поиск в меню **Пуск**.	В логе SoftControl Admin Console должны появиться записи, содержащие введенные последовательности символов в поле **Записанные данные**.

3.4 Отслеживание подключения внешнего носителя

Для проведения данного тестирования потребуется съемный носитель – USB-накопитель.

Таблица 5. Тестирование подключения USB-носителя

Задание	Ожидаемый результат
1) В настройках вкладки **Лог устройств** в SoftControl Admin Console до-	В логах появятся записи о присо-

Задание	Ожидаемый результат
бавьте колонки **Класс устройства**, **Описание устройства**. В настройках подразделения на вкладке **Сбор данных** выставите флажок **Использование USB устройств**. 2) Примените настройки. 3) Подключите USB-накопитель. 4) Извлеките USB-накопитель.	единении и отсоединении устройства, его тип отобразится в поле **Класс устройства**, а название – в поле **Описание устройства**.

3.5 Запись видео события

Данный вид тестирования проверяет наблюдение за объектами файловой системы с помощью видеозаписи.

Таблица 6. Тестирование записи видео

Задание	Ожидаемый результат
1) Создайте на клиентском компьютере файл *C:\file10.txt*. Задайте правило наблюдения за ним, укажите путь *C:\file10.txt*, выставите флажки **Чтение**, **Изменение**, **Запись видео**. 2) Примените настройки. Измените файл. 3) В разделе **DLP** → **Наблюдение** → **Запись видео** выставите продолжительность 15 секунд, частоту 500 мс, ширину кадра 640 пикселей. Повторите первое задание.	При изменении файла в логе появляется строка, упоминающая о событии изменения *file10.txt*; нажатие правой кнопкой на выделенное розовым поле в этой строке позволяет открыть видео продолжительностью 15 секунд с момента события.

4. Техническая поддержка

При возникновении вопросов по установке, настройке и работе SoftControl DLP Client вы можете обращаться в техническую поддержку по электронной почте support@safensoft.com.