Обзор Safe'n'Sec Enterprise Suite

6 апреля, 2010 - 15:11 — Александр Панасенко

Теги: Обзоры Корпорации S.N.Safe&Software Safe'n'Sec Enterprise Suite HIPS Антивирус Защита от утечек Политики



В данном обзоре мы рассмотрим Safe'n'Sec Enterprise Suite – новое поколение корпоративных систем защиты конечных точек от вредоносных программ и действий инсайдеров, базирующееся на проактивных технологиях сохранения целостности системы и поведенческом анализе. В первую очередь решение ориентировано на защиту типовых рабочих станций, банкоматов и платежных терминалов на



базе Microsoft Windows.

- 1. Введение
- 2. Системные требования
- 3. Концепция корпоративных продуктов Safe'n'Sec
- 4. Основные функции Safe'n'Sec Enterprise Suite
- 5. Установка Safe'n'Sec Enterprise Suite
- 6. Настройка и примеры использования Safe'n'Sec Enterprise Suite
- 7. Выводы

Введение

Основное назначение Safe'n'Sec Enterprise Suite – это защита информационного актива компании от внешних угроз, таких как вторжения хакеров и вредоносные программы, и внутренних угроз, таких как неосторожные или умышленно деструктивные действия сотрудников.

В основе Safe'n'Sec Enterprise Suite лежит передовая разработка компании S.N.Safe & Software технология V.I.P.O. (Valid Inside Permitted Operations), которая построена на гибком разграничении системных привилегий при работе компьютера. Продукты, использующие технологию проактивной защиты V.I.P.O, вообще не требуют никакой настройки для начала полноценного функционирования, они оснащены прочным запасом правил поведения (составленных и постоянно обновляемых специалистами по информационной безопасности компании S.N. Safe&Software), достаточным для большинства пользователей.

Использование проактивной технологии поведенческого анализа, списков доверенных приложений (whitelisting - белый список), безопасной виртуальной среды (sandbox - песочница), контроля приложений, доступа к данным и аппаратным компонентам конечных точек, совместимость со многими сторонним антивирусным программным обеспечением и оптимизированная консоль управления делают Safe'n'Sec Enterprise Suite мощным комплексом защиты с широкими возможностями.

С помощью Safe'n'Sec Enterprise Suite можно эффективно защитить типовые рабочие станции, сервера, банкоматы или POS-терминалы, работающие на операционной системе Microsoft Windows.

Системные требования

Системные требования для Safe'n'Sec Service Center

Аппаратные требования:

- 2 МБ свободного пространства на жестком диске для программных модулей;
- дополнительно 1 Гб свободного пространства на жестком диске для базы данных;
- дополнительно 50 МБ свободного пространства на жестком диске для хранения обновлений;

Для Microsoft Windows XP Professional (Service Pack 2)/XP Professional x64 Edition:

- Процессор Intel Pentium III 800 МГц;
- 256 МБ свободной оперативной памяти;

Для Microsoft Windows Vista (x86) Home Premium Edition/ Business Edition/ Enterprise Edition/Ultimate Edition, Microsoft Windows 7:

- Процессор Intel Pentium III 1 ГГц;
- 512 МБ свободной оперативной памяти;

Программные требования:

- Microsoft SQL 2005 Express (Service Pack) и выше;
- Microsoft Windows Instal ler v 4.5 и выше;
- Microsoft Internet Explorer 6.0 или выше (для обновления программных модулей через интернет).

Системные требования для Safe'n'Sec Client

Аппаратные требования:

- 20 МБ свободного пространства на жестком диске;
- 50 МБ свободного пространства на жестком диске для хранения антивирусных баз;

Для Microsoft Windows XP Professional (Service Pack 2), Microsoft Windows XP

Professional x64 Edition:

- Процессор Intel Pentium III 800 МГц;
- 256 МБ свободной оперативной памяти;

Для Microsoft Windows Vista (x86) Home Premium Edition/ Business Edition/ Enterprise Edition/Ultimate Edition, Microsoft Windows 7:

- Процессор Intel Pentium III 1 ГГц;
- 512 МБ свободной оперативной памяти;

Программные требования:

- Microsoft SQL Reporting Services для отчетов DLP Guard
- Microsoft Windows Instal ler v 4.5 и выше;
- Microsoft Internet Explorer 6.0 или выше (для обновления программных модулей через интернет).

Системные требования для Safe'n'Sec Admin Explorer

Аппаратные требования:

- 2 МБ свободного пространства на жестком диске или сменном носителе;
- Для Microsoft Windows XP Professional (Service Pack 2), Microsoft Windows XP

Professional x64 Edition:

- Процессор Intel Pentium III 800 МГц;
- 256 МБ свободной оперативной памяти;

Для Microsoft Windows Vista (x86) Home Premium Edition/ Business Edition/ Enterprise Edition/Ultimate Edition, Microsoft Windows 7:

- Процессор Intel Pentium III 1 ГГц;
- 512 МБ свободной оперативной памяти;

Программные требования:

Microsoft Internet Explorer 6.0 или выше (для обновления программных модулей через интернет).

Концепция корпоративных продуктов Safe'n'Sec

Интегрированный программный продукт Safe'n'Sec Enterprise Suite состоит из двух модулей SysWatch и DLP Guard, каждый из которых выполняет определенный набор функций и может быть приобретен отдельно как самостоятельный программный продукт. При использовании этих модулей вместе с консолью администрирования вы получаете единый продукт, обеспечивающий многоцелевую защиту корпоративной сети от внешних и внутренних угроз, а также экономию бюджета вследствие оптимального использования ресурсов.

Рисунок 1: Концепция Safe'n'Sec Enterprise Suite



Риснок 2: Схема работы Safe'n'Sec Enterprise Suite



Основные функции Safe'n'Sec Enterprise Suite

Основные функциональные компоненты и их возможности:

Как мы уже говорили, Safe'n'Sec Enterprise Suite состоит из двух модулей SysWatch и DLP Guard + консоль управления + сервисные центры.

Клиентские агенты SysWatch и DLP Guard устанавливаются на любой компьютер корпоративной сети. Они позволяют проводить анализ активности приложений, блокируют одасные действия, обеспециявают защити от вредоносного кода и закерских атак. Осуществляют

опасные деиствия, очеспечивают защиту от вредопосного кода и лакерскил атак. Осуществляют контроль доступа и использование системных ресурсов. Версии агентов с интегрированными антивирусными модулями дополнительно способны лечить зараженные системы или выполнять функцию второго антивируса в корпоративной среде, если это необходимо для удовлетворения требований безопасности. Давайте рассмотрим возможности этих модулей более подробно.

Safe'n'Sec SysWatch

Модуль Safe'n'Sec SysWatch – это новое поколение систем защиты конечных точек, базирующееся на проактивных технологиях сохранения целостности системы и поведенческом анализе. Он решает проблемы защиты конфиденциальной информации от хакерских вторжений и внедрения вредоносного кода. **SysWatch** можно приобрести в комплекте с антивирусным сканером BitDefender, VBA32 или Dr.Web.

Модуль обеспечивает защиту конечных точек корпоративной сети, работающих на операционной системе Microsoft Windows от новейших (zero-day) и специально написанных (целевые атаки) вредоносных программ.

Основной функционал Safe'n'Sec SysWatch:

- защита от направленных хакерских атак любой сложности;
- защита от всех типов известных вредоносных программ, таких как вирусы, черви, трояны, программы-шпионы, руткиты, кейлоггеры и прочие;
- защита от новейших вредоносных программ (zero-day), сигнатуры которых еще не внесены в антивирусные базы;
- анализ активности приложений и автоматическая блокировка опасных действий, которые могут привести к неработоспособности системы или порче/потере конфиденциальной информации.
- создание правил, реализующих политики безопасности по доступу к данным, USB устройствам, установке стороннего ПО.

Safe'n'Sec DLPGuard

Модуль DLP Guard осуществляет постоянный мониторинг и контроль сетевой активности пользователей, имеющих доступ к конфиденциальной информации предприятия. Продукт защищает от утечек информации, происходящих вследствие неосторожных действий сотрудников и злоумышленных действий инсайдеров.

DLP Guard контролирует реализацию политики безопасности путем создания правил контроля доступа пользователей (или групп пользователей) к определенным информационным ресурсам. Возможность скрытной установки системы мониторинга обеспечит постоянное присутствие программы без возможности ее обнаружения и удаления.

Также DLP Guard обеспечивает офицера службы безопасности информацией обо всех действиях, осуществляемых пользователем в локальной сети, фиксирует все сетевые события и создает аналитический отчет для ретроспективного анализа и расследования конкретного инцидента.

Основные функции Safe'n'Sec DLPGuard:

- мониторинг использования конфиденциальных файлов (операции чтения, записи, удаления файлов);
- мониторинг использования внешних устройств, например, USB-накопителей (операции чтения, записи, удаления файлов с USB устройств);
- просмотр экрана пользователя в режиме реального времени;
- видеозапись и воспроизведение записи экрана пользователя для анализа в случае подозрения на инсайдерский инцидент;
- запись текста, введенного с клавиатуры для любого приложения с помощью клавиатурного регистратора нажатия клавиш (отчет "Клавиатурный шпион");
- учет рабочего времени пользователя (общего и с каждым приложением);
- мониторинг изменений системного реестра;
- мониторинг всех сетевых событий;
- учет всех отправленных пользователем e-mail;
- мониторинг файлов, отправленных для печати на принтер;
- теневое копирование данных и сохранение на специальном ресурсе всех скопированных пользователем на внешние съёмные носители (CD, DVD, USB) файлы *;
- мониторинг посещаемых пользователем Интернет ресурсов и возможность подсчета расхода входящего и исходящего сетевого трафика, запрет использования определенных web-сайтов *.
- создание аналитических отчетов;

*- функция в разработке

Консоль управления и дополнительные сервисные центры

Централизованная система удаленного управления и организации рабочей области администрирования корпоративной сети необходима для эффективного управления и мониторинга современных комплексов защиты. А дополнительные сервисные центры позволяют сегментировать сетевую инфраструктуру на несколько рабочих областей. Вот список основных задач, которые можно выполнять с помощью консоли управления:

- удаленная установка и настройка клиентских агентов, их автоматическому обновление;
- поиск и удаление известного вредоносного кода на удаленных компьютерах;
- групповые политики, единые настройки и общие задачи для группы компьютеров;
- импорт/экспорт настроек для последующего использования;
- разграничение прав администраторов на выполнение сервисных задач и изменение настроек клиентских программ;
- сервисные задачи и отчеты.

Установка Safe'n'Sec Enterprise Suite

Поскольку Safe'n'Sec Enterprise Suite продукт корпоративный, перед началом установки необходимо внимательно ознакомиться с Руководством по установке Safe'n'Sec Enterprise Suite, чётко и последовательно выполнять процесс установки и первоначальной настройки.

Для начала необходимо определиться с базой данных, которую нужно установить и настроить перед установкой Safe'n'Sec Enterprise Suite. Выбор базы данных прост — или Microsoft SQL Express (до 1000 клиентов), или Microsoft SQL Server (уже за деньги) при количестве клиентов больше 1000. Каждый экземпляр Safe'n'Sec Service Center, использующий Microsoft SQL Server, поддерживает до 5000 клиентов. Если требуется поддержка более 50 000 клиентов, то необходимо установить другой Safe'n'Sec Service Center.

Удалённая установка агентов на конечные точки сети требует соблюдение следующих условий:

- наличие прав локального администратора на компьютере, где осуществляется установка;
- работающая служба «Удалённый реестр»;
- настройка брандмауэра (открытие портов);
- для конечных точек на Windows Vista и Windows Server 2008, необходимо разрешить общий доступ к файлам и принтерам.

Список портов, которые используются приложением Safe'n'Sec Enterprise по умолчанию

Номер порта и протокол	Описание
TCP 3846	Связь между Safe'n'Sec Admin Explorer и Safe'n'Sec Service Center Связь между Safe'n'Sec Service Center и Safe'n'Sec Cl ient
тср 80	Обновление Safe'n'Sec Client через Safe'n'Sec Service Center
TCP 1433	Связь между Safe'n'Sec Service Center и сервером базы данных

Может потребоваться изменить некоторые параметры операционной системы на клиентских компьютерах, на которых будут устанавливаться модули клиентских агентов.

Операционная система	Конфигурация
Windows XP в рабочей группе	Выключите простой общий доступ к файлам. Простой общий доступ к файлам может препятствовать развертыванию клиента.
Windows Vista и Windows Server 2008	Выключите мастер общего доступа к файлам. Включите поиск компьютеров в сети с помощью окна "Сеть и общий доступ". Проверьте наличие повышенного уровня прав доступа у вашей учетной записи.
Windows Vista и Windows Server 2008 в домене Active Directory	Учетная запись, применяемая для развертывания клиента, должна являться администратором домена и иметь повышенные права доступа на клиентском компьютере.

Сама установка не вызывает особых сложностей и проходит в несколько этапов. Вначале устанавливается Safe'n'Sec Admin Explorer, далее с его помощью - Safe'n'Sec Service Center. Затем уже через Safe'n'Sec Service Center происходит удаленная установка клиентских агентов Safe'n'Sec Client на конечные точки сети.

Рисунок 3: Окно установки Safe'n'Sec Admin Explorer





Рисунок 4: Главное окно Safe'n'Sec Admin Explorer

Ceth Microsoft Windows Boe Komtworepu Ceth Microsoft Windows HI & Wakktabout	Obuse VM-2003TEST OC: Morea Image: Image: Table 1.7 Description Met Met	
Все контыстеры G Cens Microsoft Windows н 🗣 VORKGROUP		of this face face at 2022
Gens Microsoft Windows H 🔍 WORKGROUP		ALL MILLIONS DELAGE SAVE
	Клиентское приложение: Установлено	Команды
Producere	Ten nujeriou <u>Komprecise</u> Cob calchese (and) <u>B</u> Kontoeren Organizeren B	Odgał Bostowski somotne Bostowskondne Procesnysmi somotne Organi ostaniał pietry Cepenowa ujerty Votracenia Votracenia

После того, как мы установили Safe'n'Sec Admin Explorer, необходимо из него установить Safe'n'Sec Service Center. Для этого, в Safe'n'Sec Admin Explorer необходимо выбрать точку сети, на которую мы будем устанавливать сервисный центр. В нашем примере это будет VM-2003TEST (см. рисунок 5).

Рисунок 5: Выбор точки сети и задание параметров установки сервисного центра

Как мы видим, можно сразу проверить возможность удалённой установки на конечную точку сети.

Важно не забыть создать новую базу данных перед установкой. Micrsoft SQL Server должен быть уже установлен на один из серверов в сети, проверен и настроен.

В параметрах установки указываем и лицензионный ключ.

Рисунок 6: Создание базы данных для сервисного центра





Не забываем проверить соединение с сервером базы данных, кликнув по ссылку внизу окна установки сервисного центра.

После того, как был заданы все параметры, можно начинать установку сервисного центра. В итоге, при выборе в Safe'n'Sec Admin Explorer конечной точки сети, куда мы устанавливали сервисный центр, мы увидим полученный результат - сервисный центр запущен, проблем нет (клиентская часть ещё не установлена). Также можно просмотреть информацию о лицензии, а также список команд, которые можно выполнить на удалённой точке сети.

Рисунок 7: Просмотр статуса удаленной точки сети



Когда сервисный центр успешно установлен, можно приступать непосредственно к развертыванию защиты конечных точек сети, т.е. установке модулей SySWatch и DLP Guard. Ее можно производить сразу на несколько конечных точек сети.

Перед установкой Safe'n'Sec Admin Explorer проверяет ее возможность, выводы экспресс-отчет. Как видим на рисунке 8, проблем не возникло.

Рисунок 8: Выбор конечных точек сети для установки SySWatch и DLP Guard



Далее необходимо указать какой именно пакет установки (SySWatch или DLP Guard) мы собираемся использовать и указать лицензионный ключ.

Рисунок 9: Выбор пакетов для установки (SySWatch или DLP Guard)



WORKGROUP	Kowne	sorep: VM-2003TEST	Конанды
VM-2003TEST	Konne	KOTED: VM-XP	ne
P-ongoint	Koney Consolit Consolitation - Rencorecut - Rencorecut	Longe: Vir 30 ² mercen SAG*X See Advent Epidear Preserve: UV Guard (eds).me Respon: Resp	AL

Рисунок 10: Задание учётной записи, от имени которой будет производиться установка

Cene Microsoft Windows	* 06sar				
Зсе конпьютеры	- 2	Budgano obsect 3			
Cets Microsoft Windows	Konta	NOTED: VM-2003TEST		Команды	
WH-2003TEST	Konta	women: VM-XP			
УМ-ХРІ Установка	stanticeoro epsit	owerses Safe'n'Secili Admin Explorer		×	ADADAGTED
Канактер Пакт устан Устан вт Затуск	котеры установни ин зимко.	С заравното такущи К назначить учёткую за		-	ть изнатьютер рудить констер ь изнатьютер
- Jatyo	¢	Ronesceare.re:	feat		
		Dapone:			itte
			ОК	Отнеча	

В завершение процедуры нужно указать время установки пакетов. Есть возможность сделать это немедленно или запланировать установку на определенное время, например, когда нагрузка на сеть и сами удаленные точки сети будет минимальная.

Рисунок 11: Выбор времени установки

Des entrestripuir	Cete Hicrosoft Windows	· Ofune]		
Contracting: Montacting: Montacting:	Все хонтьютеры	. 🧕 🗉	зыбрана объект 3		
Version Konnuorep: VM-30 Marco Volume Marco Marco Marco - Ponusero - Ponusero - Ponusero - Ponusero -	G Cette Microsoft Windows	Конпью	rep: VM-2003TEST		
	WH-2003TEST	Конпью	rep: VM-XP	ne	a l
OK Others	Cr IP-hadeter	CHILE COLUMN	Constant Constant Constant Constant Constant Constant Constant Constant Constant Constant Constant Constant Constant Constant Constant	eren di sur	Bierte estendente ingenere estendente regenere estendente regenere estendente regenere estendente regenere regenere estendente regenere re
				Отнена	

Для корректной работы модуля DLP Guard после его установки на конечных точках, их необходимо перезагрузить. После перезагрузки в Safe'n'Sec Admin Explorer увидим радостную картину в виде работающего модуля (галочки зелёного цвета возле областей контроля системы показывают, что DLP Guard ведёт за ними наблюдение).

Рисунок 12: Модуль DLP Guard, общее состояние

10 VH 2003TEST, VH 3091\Test : Safe

Cets Hicrosoft Windows	• Общие Информация Задачи Наблюдение Safe n 5	ecă iCamera
Все контьклеры	Inst VM-XP1 DC: Marea IP agent: 192.158.1.6 Deserver: DLP G	oft Windows XP Cepterceuili unimp: Het ward v 3.5.0
Cens Microsoft Windows	Статус: Ведется наблюдение	Конанды
	 ✓ Файловая система ✓ Системий деястр ✓ Приловаемий ✓ Клавозкура ✓ Клавозкура ✓ Прилов Элерисскийсканий сумоваемий Мет. Данник Коментосой приложений: Коментосой приложений: Установление: 	Odupe * Buddevirs experiating * Dodevirs experiating * Dodevirs experiating * Dodevirs experiation * Organization * Organization * Addisets exercises * Madpalae Kuebri * Votesteins * Votesteins * Votesteins * Votesteins * Votesteins * Votesteins

Установка модуля SysWatch проходит аналогично. После установки клиентов SySWatch, SySWatch + BitDefender или SySWatch TPSecure необходимо выполнить автоматическую настройку клиентов.

Рисунок 13: Задание параметров автоматической настройки клиентов SySWatch, SySWatch + BitDefender, SySWatch TPSecure



Автоматическая настройка займёт некоторое время. После ее окончания мы увидим, что в окне состояния конечной точки сети добавился модуль SysWatch, а также список областей системы, за которыми он ведёт наблюдение (рисунок 14).

-16 ×

Cere Microsoft Windows	• Общие Процессы и приложения	Области контрола	1040	орнация	385844	Наблодение	Safe's 4 >
Все конпьютеры	2 (Marg) (Marg) (Marg)	OC: He Recovered DO	rosoft Gust	Windows : d v 3.5.0	кР Сервно Труппа	n united w	
Cets Microsoft Windows	Статус: Конпьютер защищен		-	Конанда	u		
Prodestrie				OGupte bay	уронть на ната про ната про на про на на на на на на на на на на на на на	сланатар манатар солонастор орнан аналери настройка ак настройка р	
and on the line of the	-					-	and the second se

Рисунок 14: Окно состояния после автоматической настройки

Теперь наши рабочие станции находятся под контролем. Давайте теперь посмотрим, на возможности продукта в действие, да и настроить весь этот комплекс не мешало бы под наши потребности. Мы ведь хотим контролировать доступ к важной информации, а также отслеживать какие неблагонадежные сотрудники решили за бочку варенья и корзину печенья разжиться конфиденциальной информацией :)

Настройка и примеры использования Safe'n'Sec Enterprise Suite

Ну что ж, начнём настройку решения. Напоминаем, что мы работаем в консоли Safe'n'Sec Admin Explorer. Во вкладке **Общие** (см. рисунок 14) можно увидеть какие области системы контролируются, исключать из наблюдения ту или иную область, удалённо выключать/перезапускать компьютер, выполнять настройку установленных клиентских модулей (см. рисунок. 15), а также осуществлять антивирусную проверку рабочей станции (см. рисунки 16, 17) и ряд других задач.

Рисунок 15: Окно настройки установленных клиентских модулей



Рисунок 16: Задание области проверки антивирусным сканером



Рисунок 17: Задание параметров проверки антивирусным сканером





Во вкладке **Процессы и приложения** отображаются все запущенные и известные приложения и процессы на выбранной нами конечной точке сети. Часть из них находится в списке Доверенных. Для Доверенных и известных приложений действуют частные правила разрешений и ограничений.

Рисунок 18: Процессы и приложения, общий вид

Cens Microsoft Windows	1	Общие Процес	сы и приложения С	области контроля	Инфорнация Задени	Hadnogenne Sefe')
Все конпьютеры	2	the street	VM-XP	OC: Mere	soft Windows XP Capana	Her Istman Bar
Con Househ Wedness		TP Adject	192.168.1.8	fipsoyetw: DUP	Guard v 3.5.0 Toynna	WORKSRO
WORKGROUP		Vina	fignazonataria	Orpanir-mail A	Toorsegamente	Distance week
VM-2003TEST		Доверенные, И	звестные приложе	ния (действуют Ча	стные разрешения и	ограничения)
VM-XP		_	and the states		and the second	
VM-XF1		ALC.EXE	AVIER SOMMOLES	*VacTread	Microsoft Corporatio	A C:WINDOWS/SYSTEM
P-no.doeni		CSRSS.EXE	SYSTEM	HACTHUR	Microsoft Corporatio	n C:\WINDOWS\SYSTEM
		CTEMOLEXE	Test	Частные	Microsoft Corporatio	A C:\WINDOWS\SYSTEM
		EXPLORER.EXE	Test	Harmine	Корпорация Майкр.	C:\WINDOWS\EXPLORE
		HELPSVC.EXE	FRET ARRENTS	Wadtware	Microsoft Corporatio	# CIWINDOWS/PCHEAL
		*LOGON.SCR	SYSTEM	VACTINUE	Корпорация Майкр.	C:\WINDOWS\SYSTEM
		-LOGONUS.EKE	-CHET GROUNDST	Hactivite	Корпорация Найкр.	C:/WINDOWS\SYSTEM
		LSASS.EXE	SYSTEM	Частные	Microsoft Cerporatio	n CI\WINDOWS\SYSTEM
		BURGLENEC.ENE	снет данныху	Mattean	Hicrosoft Carporatio	A CI/WINDOWS/SYSTEM
		TADFINIT_EXE	CHRT ZZHNART	Mattena	Hicrosoft Corporatio	A COMMODIANS/SYSTEM
		SAFENSEC-EXE	SYSTEM	Hactivia	© 5.N.SafeSoftware	CIVPROGRAM FILESISN
		SERVICEREMOT.	A SHET ZANNER -	Hartwood	© 5.N.SefeSchware	C.WINDOWS SERVIC
		SERVICES.EXE	SYSTEM	Частные	Корпорация Майкр.	C:\WINDOWS\SYSTEM
		SETUPHELPER.ED	E CHET ZAHNEEN	NUCTION	© S.N.SafeSoftware	C:UROGRAM FILESUSN
		SH55.EXE	SYSTEM	Частные	Корпорация Майкр.	C:\WINDOWS\SYSTEM
		SNSMCON.EXE	Test	Vacmule	© 5.N.SafeSoftware	C:UROGRAM FILES\SN
		SNSODS.EXE	-EHET GANNALLY	Hactions.	© S.N.SafeSchuere	C-VPROGRAM FILES (SP
		THISDPOLEKE	wavent (channeld to	Histowell	© S.N.SafeSulturin	CIVEROGILAH FILEIMAN
		SPOOLSV,EXE	SYSTEM	Hactnuid	Microsoft Corporatio	A CIWINDOWSISYSTEM
		SVCHOST.EXE	SYSTEM	Частные	Microsoft Corporatio	n C:\WINDOWS\SYSTEM
		SVCHOST.EXE	NETWORK SERVICE	Частные	Microsoft Corporatio	IN C:\WINDOWS\SYSTEM
		SVCHOST.EXE	SYSTEM	Частные	Microsoft Corporatio	IN CIWINDOWSISYSTEM
		SVCHOST,EXE	NETWORK SERVICE	Частные	Microsoft Corporatio	n CIWINDOWS\SYSTEM
	-	SVCHOST.EXE	LOCAL SERVICE	Nacreals	Microsoft Corporatio	n C:\WINDOWS\SYSTEM
	_	SVOIOST.EXE	LOCAL SERVICE	Частные	Microsoft Corporatio	IN C:\WINDOWS\SYSTEM
		EVCHOST.EXE	SYSTEM	Vacroant	Hicrosoft Corporatio	e CIWINDOWSVSYSTEM
		UNSECAPT.EXE	CHET CONNER!	Machane	Microsoft Corporatio	A CIWINDOWSVSYSTEM
		C.SERINTLEXE	CHET ZENNER?	Vacrowill	Rophobauas Mallect	C:WINDOWENSYSTEM
		THERCLASID. PAR	GHET (Growing)	HALTHING	Microsoft Corporatio	IN COMMONITORIES
		PVHSRVC.EXE	SYSTEM	Vactorie	Microsoft Corporatio	IN COUROGRAM FILESWE
		MARINA VC. PXP	Test	Unitedation	Miccosoft Comoratio	COROCRAM PRIPEWO
		 Annecession 				and the second se

Приложения и процессы можно удаленно завершать, просматривать их свойства, задавать частные условия выполнения и ограничения, вести историю активности. Также можно проверить запущенное приложение антивирусным сканером, добавлять/удалять приложение в/из доверенных.

Рисунок 19: Просмотр свойств запущенного приложения

Conserver Conserver Conserver MORGROU Conserver Conserver MORGROU MORGROU Conserver MORGROU MORGROU MORGROU Conserver MORGROU MORGROU MORGROU Conserver MORGROU MORGROU MORGROU Conserver MORGROU MORGROU MORGROU Conserver SPOOLSV.EXE Morganic Morganic MORGROU Onserver Conserver SPOOLSV.EXE Morganic Morganic Morganic Onserver SPOOLSV.EXE Morganic Morganic Morganic Morganic Onserver SPOOLSV.EXE Morganic Morganic Morganic Morganic Onserver Spools Spools Spools Morganic Morganic Morganic Morganic Spools Spools Spools Spools Morganic	Cen, Hicrosoft Windows	2	Of use	Процессы и приложения	Области контроля	знфорнация	Задачи	Наблюдение	Safe'r 4 I
Control Statement (Control	Все контьютеры	Свойства прахожения		N= 1.5		210	XI Capazo	North Laterton Ma	n ORKGROUP
Criptelas OK Onesa Publicada OK	Chr. Norsach Wedes Wolk-Ortest Wolk-Ortes	Offsame Tyropenet in SPOOL Offsame Provide P	CCI SV.ED CCI S78 578 14. 14. 14. Spp Mec SVT Her SVT Aut	A J Hompsei Organeseesse a CE WhiteColorSI/STEM32USPOD See Soot 314-41-12 PA-2008 131-41-12 PA-2008 131-41-12 PA-2008 131-41-12 Sooter SubSystem App reachT Corporation STEM r r co we off-sopyreano resplayment r r	poopsureers USV-DR p System Decemponts 2010 22:37:34		Hite Mailey, Mailey, Mailey, Porsto porsto	Distributions inter- constructions in the inter- construction of the inter- ence of the inter- tion of the inter- t	SYSTEMS SYSTEMS SYSTEMS SYSTEMS SYSTEMS SYSTEMS SYSTEMS SYSTEMS SYSTEMS SYSTEMS SYSTEMS SYSTEMS SYSTEMS SYSTEMS SYSTEMS SYSTEMS SYSTEMS SYSTEMS SYSTEMS SYSTEMS
Contractor Section Research Contractor Distribution Contractors Contractors		Отревна		[ОК Отнен	Toreering	porato	 C:/WINDOWS' C:/WINDOWS' 	GYSTERS GYSTERS
				ST.EE SHELLING	Harmore	Hicrosoft	Corporatio	 climbows/ 	distero.

Рисунок 20: Задание частных ограничений работы приложения с сетью

2	Общие	Процессы и приложения	Области контро	ля Информация	3acaret	Наблюдение	Safe'i 41
Could the special access	1			_10	X Capital	sali userp: He	
Общие Условия в Частные ограничи данных по сели. 1	ыполнени ений и раз Предотвра	а История Ограничения и решения: Установка сетево цение вторжения извне и к	разрешения по совдинения, Пр ражи конфиденци	или и передача Клиных данных,	Malep.	Criwindows	SYSTEMS. SYSTEMS
Ceta			Cerenal pecype			_	×
Hassanie	14	Каправл Протокал Л	Hazzane:	New ace 10001			1
			Направление:	Входящее/Чоход	FLUE F		-
			Протокол	TCP/UDP			
			Покальные во Ф. Любой вр С. Определя С. Диалазон	ICP ICP UDP uper possid IP-apper sapecce			
	Country Countr	Ofune O	Officer Polycoccu anguesteenen Officer Polycoccu anguesteenenenenenenenenenenenenenenenenenen	Общите Троцисски и приложения Области контро Общите Условия високологии Общите Условия Общите Усл	Offiner Production in Transmission Officeron economics Independants Officeron economics Officeron Officeron	Offuer Option/Colume /	Offsame Production or rigonocesses Offsame Production Offsame Offsame Production O



Рисунок 21: Задание частных ограничений работы приложения с реестром



Во вкладке **Области контроля** задаются общие ограничения и разрешения: чтение, изменение, удаление каталогов и файлов, ключей и ветвей системного реестра. Это даёт возможность предотвратить доступ к конфиденциальной информации, а также предотвратить несанкционированное изменение настроек системы. В том числе предусмотрена возможность блокировки работы с USB устройствами, отслеживание использования привилегий процессов основными группами пользователей, настройка работы с сетью (задание сетевых правил) и взаимодействие процессов с системой. Всё это позволяет гибко настроить доступ к наиболее важным данным и критическим областям системы.

Общие правила действуют для всех приложений, которые не находятся в списке Доверенных и известных.

Рисунок 22: Общий вид окна Области контроля



Можно выбрать какую область контроля мы хотим просмотреть и настроить (файловая система, системный реестр, сеть, привилегии процессов, устройства, взаимодействия процессов). Рассмотрим настройки области контроля более подробно.

Рисунок 23: Области контроля, файловая система

WH 2003TEST, WH 2011 Test E Safe's Sec. Admin Explorer Dalle But Karandar Cepanic Orpania		to and a						1012
Ceru Microsoft Windows	Ofure	fipouer	сы и приложения	Области контро	нь Ниформация	Задачи	Наблюдение	Safe) 41
Все контьютеры	Vie	(best)	VM-XP	OCI.	Microsoft Windows	XP Cepero	nañ izerez: H	et.
Cets Horosoft Windows	Общие	IP Ampeti orpanister spacetered	192.168.1.8 иля и разрешения: изненения настрое	Продукты: Чтение, Создани ок систены и неса	DLP Guard v 3.5.0 е, Поненение, Удал икционированного	Группа сние катал доступа к е	W вонфиденциаль	IORKGROUP



Настройка разрешений может проводиться как для одного файла, так и для каталога. Главное чётко понимать, что делаем иначе можно наломать дров.

Рисунок 24: Области контроля, системный реестр



Здесь всё аналогично контролю файловой системы. Работаем внимательно и аккуратно, крайне желательно вести документирование своих действий.

Рисунок 25: Области контроля, сеть



Для сети набор готовых правил обширен. Если вдруг, чего-то не хватает, то можно создавать свои собственные правила.

Рисунок 26: Области контроля, привилегии процессов

W VH 2003TEST, VH 30911	ext : Safe'n'Sec@ Admin Explorer	1012
Galin Bra Kontrasi Co	perc Opania	

Все контьютеры		d Alexan	VM·XP	OC1	Microsoft Windows XP Capasional Laserph	Her				
G Ceru Microsoft Windows		IF ADJect	192.168.1.8	Прадукты	DLP Guerd y 3.5.0 (pynna)	WORKGROU				
WORKGROUP	00	пользования с	ия и разрешения: стемных функций,	предотерещение и	Повышение привилегий процессов. Огра- эксплуатации указаности приложений.	N-HERING				
VIEW	12	ривилетии прок	ACCOR	in the state of the	contraining of the second states of the					
Princacety				Де	Actese					
		BUILTING	дчинистраторы							
		All Ynpass	ение мудитон и жу	рналон безопасн	OCTM					
		Apxies	рование файлов и	Katanoros						
		#1 Boccta	oanerere daknos e	xaranoroe						
		and streame	HAR CALTERHOLD BO	and the second se						
		III Inserts	нине работы ристе	ana.						
		and Cinetatory	ormitalant with these	to here the second second						
		and Canada	and the second second	anna chastana						
		and Country	a passanani	President and an an an an an an						
		and strength	a roorpann							
		Self subverse	HAR HEREITENE ID	etter interfactories	-					
		Doofunance and presente on control on the set								
		Mill reducing or an and a second second								
		Увеличение приоритета диспетчирования								
		Загрузка и выпрузка драйверов успройств								
	Ославние страничного файла									
		間 Hactpo	Ака квот паняти дл	In repounded						
	В Обход перекрестной проверки									
		Нателение контиктера из стыховочного узла								
		Al Janyos	onepauxil no ofice	уживанию тона						
		Cineties	ворение клиента п	осле проверки по	адлинности					
		fil Conney	не глобальных об	sextos						
	3	BUILTINUT	wnatesocatio							
		All Saseou	ные работы систе	-						
		AND OFWER	перекрестной доон	MACHINE .						
		and strength	ever component	AT CTARGED AND A	C. 1.1.					
		On SALES WEATING								
			The second							
		eaj runene	-	ENERGY		1				
					Gonad-write.num	e Tipereners				
						to the second second				

Как видим, в настройках области контроля привилегий процессов уже учтено все самое необходимое, разработчики экономят наше время.

Cets Microsoft Windows		общие	Процессы и приложения	Области контроля	Информация	Задачи	Наблюдение	Safe) 41
Все контьютеры		1	Unit: VM-XP	DC: Mit	rosoft Windows P Guard v 3.5.0	XP Capazo	Hand Laterta: Ha	*
Cets Microsoft Windows	-	Общие	ограничения и разрешения мотер нежелятельных прог	Использовение разли	чных устройства.	Предотер	вщение проник	OBENNA
VM-XEST		Verpoil	crea					2
St IP-педсети		10	USB ycroolcras	Тип устройства			Attende I	taxentrate
						Дe		umesors,
Proved (2) (2) (2) (2) (2) (2) (2)	-328						2-010	A 10. 23 12

Рисунок 27: Области контроля, устройства

В плане возможностей контроля устройств пока что выбор небогатый, но по заявлениям вендора разработка в этом направлении активно идет.

	CHARGE EVENING AND A								- 0
Balin Bira Konsinalu Cepesic Choseka						155			
Cety Hicrosoft Windows	•	общие	(Inpoured	сы и приложения	Области контр	информация	Задачи	Наблюдение	Safe'r 4
Все контьютеры	-	101	Ave:	VH-XP	OC:	Hicrosoft Windows	XP Capitor	Hand Latertal H	
Werkgeoue Werkgeoue		4aCtmedia Barrio2 U γcra βαστ	е организация объектина войстина на произо на прои на прои на про	ала и разредени Транова Калана и разредени Транова Калана и разредени Транова Калана и разредени Калана и разредени и разредени Калана и разредени Калана и разредени Калана и разреден	на (Ваничадайстверодания) адани изобрадания боенна миник Ледекавлика и и дание (nouecos e certe al ante a contra de la contr	HUJ, Hexru	ingescence	

В настройке взаимодействия процессов для каждого правила можно выбрать пользователя, для которого оно будет действовать, а также период его действия (см. рисунок 29). Обратите внимание, что можно задать несколько периодов действия правила.

Рисунок 29: Выбор пользователей, на которых будет распространяться данное правило

AND ROAD AND AND REAL COLORS AND IN SUCH	Advin Cryberry	-							_(#) :
Cers Hicrosoft Windows		06w#8	Процессы и прило	Edminik .	Области контроля	Информация	Задачи	Наблюдение	Safe) 4
все контьютеры		1	Ings VH-XP		<u>Дополеет стыне</u>				×
Christopat Worker Workgonzer Workgonzer Denacere		Ofuer rightmenters in palposeters. Polagorgauture systemeters and the Pelifysic Ballocase octeves Pelifysic Bill Dir Bill Dir Bi		Ronszoszeni () Buőspirra nonso zamiot nosso Box	ar adressr				
Budget some Budget son a Romannes WORKROUT Basers Gener Decomments	60%			Janu of hearing		Con Con	The Vigatur		
	Веланта днена и	албараени 0]	x ofuerte (<u>taneta</u>)		Dicketoria lond	TRESISS	NNNNNNNN		
	1-339	H P Orof	🗅 D: ражать объекты, для	катары	у на определены от	20-er-do-erat	50 "A:		18. aos

Рисунок 30: Задание периода времени для действия правила

Carla Manageri Milliona	• Общие Процессы и приложения	Области контроля	Информация	Sagavet Ha	блюдение	Safe) 4
бсе конлькотеры	Inst VM-XP	Доосликтельно				×
VM-SOUTEST VM-SOUTEST VM-SOUTEST VM-SOUTEST VM-SOUTEST VM-SOUTEST VM-SOUTEST	Prace 32.146.13 Conserved as a patients and approximate assessments as a patients and approximate assessments ascrop estimates and approximates and a	Полазование В Dudgores pare refresent pare C C 0.000 C 0.000		a, 1 1940004 80 18.400 夏 국 (00012 관 (00012 관 (00012 관 (00012 관 (00012 관 (00012 관 (00012 관 (00012 관) (00012 관 (00012 관) (00012 문) (00012 E) (00012 E) (0001	nopeus Eyzar	

Давайте, в качестве примера, запретим пользователям использовать USB-диски. Для этого открываем **Область контроля — Устройства** и снимаем галочки «Чтение» и «Изменение», после чего нажимаем **Применить**.

Рисунок 31: Изменение разрешений для USB-устройств

Cets Microsoft Windows	*	Ofuse	Процессы и приложения	Области контроля	Информация.	38,08%	Наблюдения	salei 41
Все контькотеры		10	New VM-XP	OC: No	rosoft Windows	XP Cepero	ный центр:	Her
Cerly Microsoft Windows		Общие на конт	ограничения и разрешения ограничения и разрешения мотер нежелательных прог	Использование разли рани через внешние у	чила устройств стройства	. Ppedotec	acienze npova	кновония
VN-XP1		()()()()	USB ympolenaa	ип устройства			Чтение	itorerenze
						л	nonwearant.	Openeos/tw
1 Nycal 🕑 😹 🛃 🔂 WH- 2003TEST, VA	1-XP_						2-05	. 0-23

Рисунок 32: Результат действия настроенного правила для USB-устройств

Delicrose • USB • Cepauc • Chi+Ab+Del		0.
Carrente propanteres	x	
Порториз		



Как видим, при подключении USB-устройства запускается автоматическая проверка накопителя на наличие вредоносного кода. А вот с самим устройством мы работать не можем — отказано в доступе. Это сработало наше только что созданное правило. Теперь «слить» что-либо на флэшку не выйдет. Кстати, заодно получилось кардинальное решение проблемы Autorun-вирусов. Нет зубов - нет кариеса. Ещё один плюс к уровню защиты сети.

Аналогично действуем и для других областей контроля. Не забываем, что это общие правила, которые действуют для всех недоверенных и неизвестных приложений. Для доверенных и известных приложений существую частные ограничения, правила в которых создаются аналогично.

Во вкладке **Информация** отображаются сообщения и предупреждениях о различных событиях на подконтрольной точке сети. На **рисунке 33** мы видим два предупреждения сообщения о том, что сработало наше созданное выше правило — запрет работы с USB-устройствами. Пользователь попытался открыть подключенный внешний диск.

Рисунок 33: Сообщения от модуля DLP Guard - пользователь пытался открыть флэшку



Во вкладке **Задачи** отображаются все выполненные, текущие и запланированные задания на конечной точке. Задания можно запускать, останавливать, удалять и просматривать их свойства. Отображается время начала и окончания выполнения, а также состояние выполнения (см. рисунок 34). В нашем случае видим, что выбранной точки сети ряд задач уже присутствует.

Рисунок 34: Список задач и их состояние

Cere Microsoft Windows	2	Ofure	Процессы и приложе	ния Области контрол	a Indopeaues (2)	Задачи	Наблюдение	514
Все конпьютеры		10	ilmai VM-XP	OC.	ticrosoft Windows XP	Серенсный	Lanetas Het	
Cens Hicrosoft Windows			P Annec: 192-168,1.5	(bodikan)	ole chreve A 3'2'0	rpyma	WORK	GROUP
VM-2003TEST		12 1/7 1		21.03.2010.23-23-53	Marta Arte	CBCTI	Notes Linder	Date:
S MACKE		() YOR	deva napaveripos koverita	21.03.2010 23:23:55	VM-XP	3000	pueva voteu	21.03
IP-noncerne		PAnto	чатическая настройка	22.03.2010 21:04:30	VM-30P	Dert	Invitence	22.03
1 THERE IS	2 06+0	Anne stents	22.03.2010 22:07:54	VM-XP	Den		22.63	



Во вкладке **Наблюдения** мы можем создавать правила слежения за объектами системного реестра и файловой системы – это очень важная функция. По-молчанию здесь нет никаких правил, их нужно создавать самостоятельно.

Рисунок 35. Окно наолюдения, правила еще не	кно наблюдения, правила ещё не созданы
---	--

Galin Briz Kinstelau Cepeur Organia									
Cerle Microsoft Windows		Общие Процессы и	приложения	Области контроля	Информация (2)	Задачи	Наблюд	Store .	51 41
Все контьютеры		Test VM	9.0P	OC: M	icrosoft Windows XP	Серенсны	А центра	Het	0000
Cart Morale Works		P sale: 13 Distinct con Continued per	2.166.1.8	(historia) D	P Gard v 33.0	Pprove	Interest	Con	SECUP
		Roberto Havenin	. Yaabets					forme	
El Thyce () # 🛃 🔄 VH-2003TEST, VH	-XIP_						T - 0	200	1:04

Давайте создадим пару правил для наблюдения и посмотрим на результат. Для начала, создадим правило для слежения за текстовым файлом, который находится на рабочей станции пользователя. Для этого достаточно щёлкнуть правой кнопкой мыши на разделе **Файловая** система и выполнить команду **Добавить**. В открывшемся окне выбираем объект файловой системы, за которым будем вести слежение (см. рисунок 36).

Рисунок 36: Выбираем объект для правила наблюдения



Правило создано, не забываем кликнуть по ссылке Применить в нижней части экрана.

Рисунок 37: Созданное правило наблюдения

Ceru Microsoft Windows	•	общие	Проце	ссы и приложения	Области контро	ила Информация (2)	Задачия	Наблю	Denne Si e
Все контьютеры		1	Heat .	VM-XP	001	Horosoft Windows XP	Сервисные	ң шентрі	Her
H WORKGROUP		80	Dalacea	a cacteria	Ресурс			WIRENAU	Cosaener
VM-XP1		0	CACTERING	ень захная нифори ий реестр	ацин Секретно, Б	4		14	14



Аналогично создадим правило и для системного реестра. Будем отслеживать манипуляции с одной из веток автозапуска.

Certs Microsoft Windows		Of use	Процессы и прил	CHEHRS	Области контроля	Пефорнация (2)	Задачи	Наблюд	serves Si
бсе контьютеры	•	1	Inter VM-XP	1.0	OC: No	resoft Windows XP	Ceptercoul	userp	Her
Gers Microsoft Windows					Pecype		pprox.	10terest	Созден
VM-2003TEST VM-007 VM-007		80	райловая систена С:10чень важна	я информа	uня/\cexperies.txt			30	50
th-nadcere		80	AREGISTRY MACH	NINE\SOFT	NAREUNicrosoftUNing	dows\CurrentVersion	(Run),*	82	R
		Dolear	damenta X	ala terta					Tomesin

Рисунок 38: Правила для файловой системы и системного реестра готовы

Не стоит излишне увлекаться созданием правил и попытками контроля всего и вся, иначе в ворохе сообщений мы пропустим действительно важные события.

Теперь пришло время посмотреть на результат наших действий. Заходим во вкладку Информация и видим так новые сообщения о том, что подконтрольный файл открывался и изменялся, а в подконтрольной ветке реестра появился новый параметр. Подобным образом может быть отслежен несанкционированный доступ к конфиденциальной информации или установка вредоносной программы.

Рисунок 39: Правила наблюдения сработали

Cens Microsoft Windows	• Общие Процессы и	приложения Области контроля	Информация (6)	Задачи Наблюдение S: 4
Все конпьютеры	🕥 👔 Hari VM-	-XP OCI Micro	sach Windows XP C	epercinal unity: Het
VICTOR	Тип событая В. Порасупрокалние В. Порасупрокалние В. Порасупрокалние В. Порасупрокалние В. Порасупрокалние В. Порасупрокалние В. Порасупрокалние	April in Section 21.03.2010 00:3400 22.03.2010 00:3400 23.03.2010 01:1514 23.03.2010 01:1514 23.03.2010 01:1514 23.03.2010 01:1514 23.03.2010 01:1514	Kornwotten 194-30 194-30 194-30 194-30 194-30 194-30 194-30	Horowen, DuP Guard DuP Guard DuP Guard DuP Guard DuP Guard DuP Guard
	 Xyahera Rometrika 	rak ngo-newde		Catoryn
	x Salvers Toesters Xalvers Toesters Tpegympe Normalities Normalities	сак протичнов ЖДСНИС Ил-бал Сий-бана	Basenictus Offe Coctument: He f	Cakjurys Cakjurys sportnes

И в заключение рассмотрим очень интересную вкладку **Safe'n'Sec iCamera**. В ней мы можем вести удалённое видеонаблюдение за рабочей станцией или какой-либо другой точкой сети с возможностью записи видео-роликов. Как правило, в организациях часто уже применяются системы удалённого управления и видеонаблюдения типа Radmin или семейство VNC. Не стоит отказываться от них, если они уже развёрнуты. Они прекрасно дополнят друг друга.

Записанные видео-фрагменты систематизируются по времени, что очень удобно для их последующего поиска и анализа, см. рисунок 40.

Рисунок 40: Записанный видео-фрагмент действий пользователя при помощи Safe'n'Sec iCamera



На сервере с установленным сервисным центром доступны дополнительные возможности в Safe'n'Sec Admin Explorer, а именно просмотр списка конечных точек сети обслуживаемых этим сервисным центром и управление лицензиями. В окнах **Информация** и **Задачи** отображаются все сообщения и задачи со всех конечных точек сети обслуживаемых этим сервисным центром.

Рисунок 41: Главной окно Safe'n'Sec Admin Explorer



Видим, что кроме установленных SysWatch и DLPGuard на данном узле есть ещё и Safe'n'Sec Service Center.

Рисунок 42: Список конечных точек сети, обслуживаемых данным сервисным центром

Balle Big Konandar Cepter Crosena							-1012
Cerls Microsoft Windows		Общие Конпьютеры	Процессы и приложения	Области контроля	Лицензия	Безопасность	10-4
Все контькотеры	-	The Store VM-2	OC:	Microsoft Windows	Cepercre	ацентр: Устан	овлен
Cent Monden Workdoup Wooddoup Wooddoup		G [™] P ages: 1971 = € Ver-2021E37 ¥ Ver-207 ¥ Ver	44.1.7 Openyote Hea	EUF Guerd V 3.16. IP Apper 195.166.17 195.166.13 195.166.14	Portes Moneset Microsoft Microsoft	WOBJ Multiplead Conten- Windows XP Windows XP	- 1.5. 3.5 2.5

2 +6) 9. un

Рисунок 43: Установленные лицензии

W VH-2003TEST, VH-2011Test : Safe'n See	16 Admin Explorer								الع	U.×
Balle Brit Konanzar Cepters Cripters	-	Общие Ко	итыстеры	Процессы и	приложения	Области контроля	Лицензия	Besoned	HOCTS 1/2	
Все конпьютеры	•	Mil Hours	VH-	20037857	901	Microsoft Windows	- Cepercry	à unimpi	Устанскле	
© Cent Microsoft Windows ■ WindowsCoute WindowsCoute Windows		Паделарный Налан-ЭтаТа ЯКАК-WIЭн- 779935-QCPR 9728-X80C-3	5.465 5063-6754 5069-626-49 1600-43033	UTATADIV.9+1	Konvector 0 0 0 0	i Hononuodearta na Sydiviatch (udd).	nel			
		Удалить Добежнь Теп Лицендия Срок Акалетика (дией) Каличество коллиотерое					1	Root-	88 20 10	
		Konovertui Safe'n'Sec& Se	vice Center v	3.5.0.0	Konnecteo 1	Autoromulia Inter-AROC-P	904 100-19083-QUII	к-хэн	1	
1 Thyos 🕢 👩 🛃 🕒 VH-2003TEST,	(H-XP_							2	-130	34

Рисунок 44: Список сообщений всех конечных точек сети, обслуживаемых данным сервисным центром



Централизованный сбор и отображение всех событий со всех конечных точек сети избавляет офицера безопасности от необходимости просмотра каждой конечной точки сети в отдельности.

Рисунок 45: Список задач всех конечных точек сети обслуживаемых данным сервисным центром

WH-2003TEST, VH-XP1\Test : Safe'n'Sect	Admin Explorer	10				-18 2
Файл Вид Конанды Серенс Странка		V. 95		120	10	
Cets Microsoft Windows	1	Области контроля Лицензия	Безопасность Инф	оорнация (7) Задачи	Наблюдение Safe'n'S	iec8 4
Все контьютеры		VM-2003T	EST	Microsoft Windows	Cepercoval Lawrence Veraw	G876H
Cens Microsoft Windows		19 Auper: 192-168.1	-7 Продукты:	DLP Guard v 3.5.0	rpyrna: wok	GROUP
H WOAKGADUP		Passes	Carta of species	Какъютер	Составние	Датан
VM-XP		Проверка клиента	21.03.2010 22:50:47	VM-2003TEST	Seeepueve yoheu	21.03
VM-XPE		Этеновка парачетров клиент	na 21.03.2010 23:23:53	VM-XP	Завершена успеш	21.03
😭 DF-modicetie		Установка парачетров клиент	ne 21.03.2010 23:23:55	VM-XP	Завершена успеш	21.03
		Автонатическая настрожа	22.03.2010 21:04:30	VM-2003TEST	Benomerce	22.03
		Авточатическая настрожа	22.03.2010 21:04:30	A46-309	Выполняется	22.03
		Авточатическая настройка	22.03.2010 21:04:30	V96-30P1	Былогнаятся	22.03
		• Обновление клиента	22.03.2010 22:07:54	VM-XP	Beingshipetca	22.03
		1				-11

На этом мы заканчиваем обзор основных возможностей Safe'n'Sec Enterprise Suite

Выводы

Safe'n'Sec Enterprise Suite является мощным продуктом для обеспечения комплексной безопасности корпоративных сетей, контроля и разграничения доступа к конфиденциальной информации, основанным на самых современных технологиях.

К плюсам Safe'n'Sec Enterprise Suite стоит отнести обширный функционал по контролю и защите информации от внешних и внутренних угроз, достаточную простоту установки и лёгкость в работе, применение передовых инновационных технологий в работе продукта, хорошая совместимость с антивирусным программным обеспечением, а также низкие системные требования для клиентской части продукта.

Использование технологии "белых списков" прекрасно подходит для защиты типовых рабочих станций, платёжных терминалов и банкоматов. Так как программное обеспечение и оборудования там изменяется крайне редко, то блокирование всех недоверенных приложений и действий является наиболее логичным и эффективным подходом с точки зрения безопасности.

Стоит отметить встроенный клиент видеонаблюдения Safe'n'Sec iCamera, который предоставляет возможность записи видео-фрагментов с рабочего стола удаленной конечной точки сети. Это дает дополнительные возможности по сбору доказательной базы для службы безопасности.

К минусам продукта, как было уже сказано в начале обзора, можно отнести отсутствие возможности мониторинга сообщений интернет-мессенджеров (очень нужная функция, с учётом того, что они вошли прочно даже в рабочую жизнь), работы с беспроводными сетями и контроль над посещением интернет-ресурсов сотрудниками предприятия. Но это скорее не минусы, а пожелания для дальнейшего развития функционала продукта с нашей стороны, так как в большинстве случаев на фирмах уже используются системы контроля доступа сотрудников к сети Интернет.

Также в Safe'n'Sec Enterprise Suite явно не хватает возможности отслеживания изменений содержимого конфиденциальных документов, на наш взгляд, для продуктов такого класса она просто необходима. Также разработчикам стоит ввести в продукт возможность отправки уведомлений и отчётов не только по e-mail, но и по другим каналам, например, по ICQ, Jabber или по SMS.

Отдельно стоит отметить проблемы технического характера: были замечены сбои в работе сервисных компонентов продукта, проведённые изменения настроек не всегда сохранялись.

Тем не менее, наша субъективная оценка решения Safe'n'Sec Enterprise Suite - 8 из 10 баллов.

Продукт получает награду Approved by Anti-Malware.ru



Список рекомендуемых нами продуктов »

Автор обзора: Алексей Баранов

Средняя оценка: 4.2 (голосов: 15)