



Код безопасности
ГК «Информзащита»

Код Безопасности: Honeypot Manager 2.0

Что нового?



Security Studio Honeypot Manager

Проактивное средство обнаружения хакерских вторжений и несанкционированного доступа к информации ограниченного доступа, основанное на имитации данных и анализе обращений пользователей к имитируемым прикладным программам и сетевым сервисам.













НОВЫЕ ВОЗМОЖНОСТИ

- **Имитация систем хранения данных на основе файлового сервера**

В новой версии добавлен еще один тип сенсора – файловый сенсор, позволяющий имитировать файловые ресурсы организации, а также приложения, хранящие свои данные в файловой структуре с возможностью сетевого доступа, такие как 1С 7.х.

Объекты управления

-  HoneyPot Manager
-  Операторы
-  Сенсоры Oracle
-  Файловые сенсоры
-  Файловый сенсор N1
-  Отчеты
-  Последние уведомления
-  Статистический отчет
-  Подробный отчет
-  Отчет по событиям

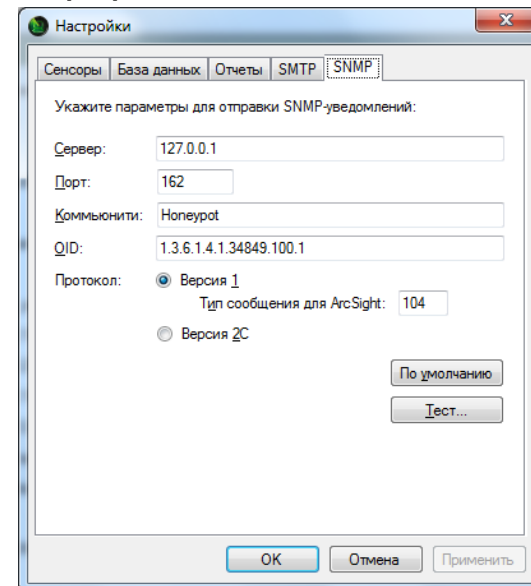


НОВЫЕ ВОЗМОЖНОСТИ

- **Оповещение о попытках НСД по протоколу SNMP**

Система Honeypot Manager теперь позволяет использовать для уведомлений о фактах НСД протокол SNMP, который является стандартным средством предоставления (рассылки) информации о событиях в устройствах или программах и поддерживается всеми системами централизованного мониторинга и управления.

В частности, это обеспечивает возможность интеграции Honeypot Manager с системой управления событиями информационной безопасности ArcSight 4.5.



НОВЫЕ ВОЗМОЖНОСТИ

- **Отчет о новых попытках НСД**

Данный отчет содержит информацию о последних срабатываниях настроенных правил на сенсорах, произошедших с момента последнего просмотра отчетов.

Последние срабатывания правил

Данный отчет отображает общую статистику по 6 последним срабатываниям настроенных правил на сенсорах.

Отчет создан 01 Apr 2010 21:34:51

Параметры отчета:

Количество: Последние 6
Сенсоры: File Server 1; File_server_01; Oracle_01; SMB_01
Правила: 12; 43; emp; sx; Доступ к ресурсам; Попытки входа; Попытки использования, расширенное; Правило_01; Правило_02; Событие 'Пульт'

Дата	Сенсор	Правило														
01 Apr 2010 12:48:24	FileServer_01	Попытки входа Класс правила: Подключение к сетевому ресурсу														
		<table border="1"><thead><tr><th>Атрибут события</th><th>Значение</th></tr></thead><tbody><tr><td>Время события</td><td>01 apr 2010 12:48:19.000</td></tr><tr><td>Количество событий</td><td>3</td></tr><tr><td>Настройка правила: Объекты наблюдения</td><td>Все</td></tr><tr><td>Объекты</td><td>share_01</td></tr><tr><td>Период (сек)</td><td>00 ч. 02 мин. 20 сек.</td></tr><tr><td>Хосты, с которых произошел доступ</td><td>172.16.0.67</td></tr></tbody></table>	Атрибут события	Значение	Время события	01 apr 2010 12:48:19.000	Количество событий	3	Настройка правила: Объекты наблюдения	Все	Объекты	share_01	Период (сек)	00 ч. 02 мин. 20 сек.	Хосты, с которых произошел доступ	172.16.0.67
Атрибут события	Значение															
Время события	01 apr 2010 12:48:19.000															
Количество событий	3															
Настройка правила: Объекты наблюдения	Все															
Объекты	share_01															
Период (сек)	00 ч. 02 мин. 20 сек.															
Хосты, с которых произошел доступ	172.16.0.67															

[Системные события, приведшие к срабатыванию правила \(1\)](#)



НОВЫЕ ВОЗМОЖНОСТИ

- **Поддержка современных операционных систем семейства Windows**

Версия 2.0 может быть установлена на системах Windows Server 2008, Windows Server 2008 R2, Windows 7, Windows Vista, Windows Server 2003, Windows Server 2003 R2 и Windows XP, работающих на платформах x86 и x64.

- **Переработанный пользовательский интерфейс программы**

