REDLAB
A member of CompuLink Group

REDCENTER
A member of CompuLink Group

REDSecure: семейство продуктов комплексной защиты информационных систем

http://www.redsecure.ru/

Угрозы информационным ресурсам

- Нарушение конфиденциальности

- Нарушение целостности

- Нарушение доступности

Внешние угрозы

- DDoS-атаки
- Ботнеты
- Эпидемии вирусов и сетевых червей
- Script-kiddies
- Криминальная деятельность и промышленный шпионаж

Внутренние угрозы

- Любопытные сотрудники
- Корыстные сотрудники
- Неумелые сотрудники

Немного свежей статистики

Первые 6 мест по данным atlas.arbor.net за последние 24 часа:

Страна	Место	Число атак на подсеть	Объём сканирований на подсеть	Число ботнетов	Число попыток фишинга	Число DoS-атак
США	1	130	201Кб	264	39107	5030
Китай	2	469	1.43Мб	26	771	541
Голландия	3	2	7Кб	9	14465	144
Польша	4	2	13Кб	7	7781	99
Ю.Корея	5	4	18Кб	10	3191	1670
Россия	**6**	**10**	**30Кб**	**10**	**4795**	**251**

Подробнее по России

Статистика ФСБ об инцидентах в информационных ресурсах государственной власти:

- **Более 600 000 атак за 2003 год**
- **Более 730 000 атак за 2004 год**
- **Более миллиона атак за 2005 год, из них 170 000 на официальный сайт президента РФ**

Громкие инциденты

- Кража базы данных пенсионного фонда (Красноярск)
- Кража базы данных ГИБДД
- Кража базы данных сотовых операторов
- Кража базы данных на всех ВИЧ-инфицированных Южного Урала
- Кража базы данных по кредитам россиян из одного из банка по потребительским кредитам
- Утечка информации в Центральном Банке (2004 год)

Итог: появление Интернет-ресурсов, предоставляющих свободный доступ к нелегально полученным базам данных

Цель создания решений семейства REDSecure

Целью совместного проекта группы компаний REDLAB/REDCENTER и факультета ВМиК МГУ является обеспечение надежной комплексной защиты информационно-телекоммуникационных систем предприятия

Класс продуктов - REDSecure

Семейство продуктов REDCLASS *- это решения по обеспечению комплексной защиты распределенных информационно-телекоммуникационных систем уровня предприятия от внешних и внутренних угроз безопасности информации*

Линейка продуктов REDSecure:

- **REDSecure IDS** – система обнаружения атак на информационно-телекоммуникационные системы
- **REDSecure IPS** – система обнаружения и предотвращения атак на информационно-телекоммуникационные системы

REDSecure
Обнаружение и предотвращение атак

Задачи решений семейства REDSecure

- ✔ Предотвращение нарушений целостности и незаконного использования информационных ресурсов
- ✔ Обеспечение своевременного получения пользователями ИТС достоверной и полной информации
- ✔ Защита данных и ресурсов, содержащих секретные данные и данные ограниченного пользования
- ✔ Выявление, оценка и прогнозирование источников угроз информационной безопасности
- ✔ Автоматизация защиты информационной безопасности
- ✔ Обеспечение конфиденциальности, целостности и доступности информации, хранящейся в узлах защищаемой сети

Возможности REDSecure IDS/IPS

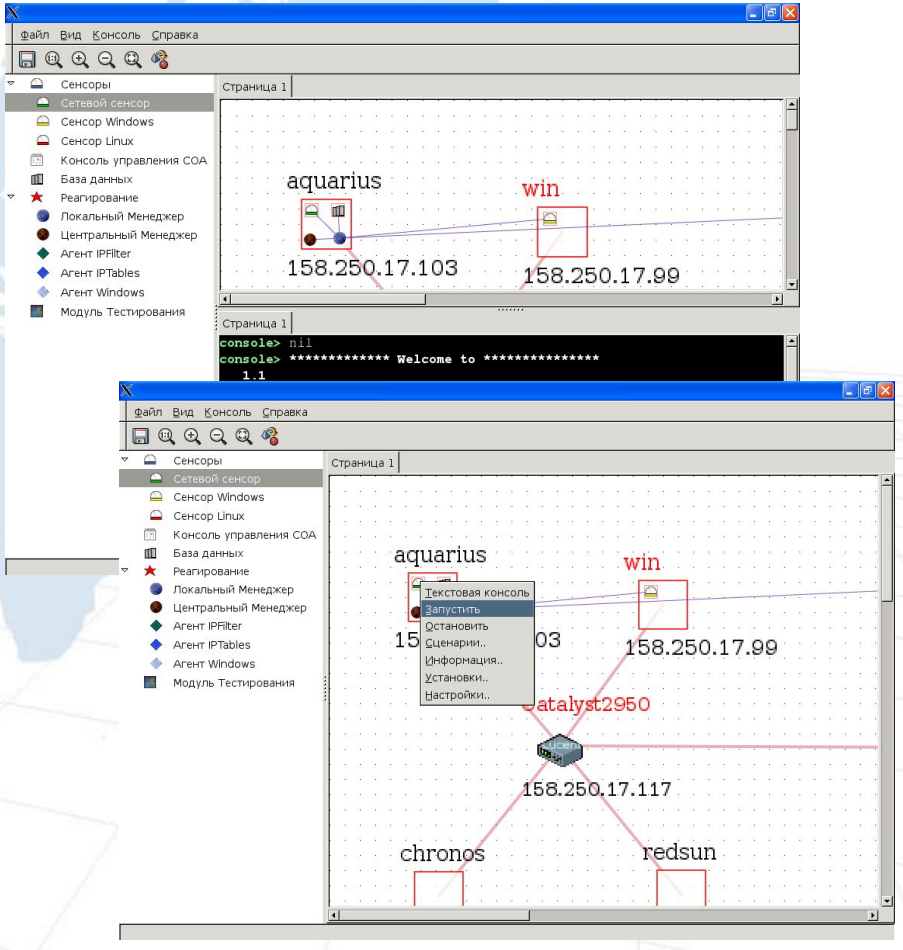
- ✔ Обнаружение компьютерных атак на узлы защищаемой сети
- ✔ Обнаружение аномального поведения внутренних пользователей
- ✔ Обнаружение нарушений политики безопасности на узлах защищаемой сети
- ✔ Поиск уязвимостей на узлах защищаемой сети
- ✔ Автоматическое реагирование на атаки

Особенности REDSecure

- защита гетерогенных сетей, в том числе построенных на базе продуктов компании **Sun Microsystems**
- высокоскоростное ядро анализа, позволяющее анализировать большие потоки данных в реальном времени
- возможность поставки как программных, так и программно-аппаратных комплексов
- возможность адаптации любого продукта под конкретного заказчика в сжатые сроки
- использование сертифицированных криптографических средств

Иерархическая система модулей

- **Сетевой сенсор** – программно-аппаратный комплекс анализа сетевого трафика
- **Узловой сенсор** - агент на узлах сети, контролирующий поведение пользователей и приложений
- **Станция управления** – программно-аппаратный комплекс управления REDSecure



REDLAB
A member of CompuLink Group

REDCENTER
A member of CompuLink Group

Предлагаемые услуги

- ✔ Внедрение и сопровождение комплексных систем защиты сети на базе продуктов REDSecure IDS и REDSecure IPS
- ✔ Обучение персонала работе с предлагаемыми решениями
- ✔ Услуги по адаптации REDSecure IDS и REDSecure IPS под инфраструктуру заказчика, и/или интеграции данных продуктов с существующими средствами защиты информации
- ✔ услуги по детализации базы знаний сетевых и узловых сенсоров REDSecure IDS и REDSecure IPS под конкретную политику безопасности предприятия

Решение на базе Sun UltraSPARC T2

В ближайших планах компании **REDLAB** стоит разработка специализированного программно-аппаратного сенсора на базе серверов компании **Sun Microsystems** с технологией **CoolThreads** и операционной системы Solaris 10, идеально подходящих для задач потоковой обработки и приложений безопасности.

КОНТАКТНАЯ ИНФОРМАЦИЯ

Денис Гамаюнов

Руководитель проекта REDSecure

REDLAB/**REDCENTER**

Тел.: +7 (495) 939-46-71

E-mail: gamajun@redsecure.ru

Веб-сайт: http://www.redsecure.ru/

Москва, Воробьевы горы,

Научный парк МГУ

REDLAB/**REDCENTER**