Семейство SAFEsuite компании ISS

ИНФОРМЗАЩИТА
НАУЧНО-ИНЖЕНЕРНОЕ ПРЕДПРИЯТИЕ

Семейство SAFEsuite

Управление уязвимостями	Управление угрозами
Система	Система
Сеть	Сеть

Семейство SAFEsuite

Семейство SAFEsuite

ИНФОРМЗАЩИТА
НАУЧНО-ИНЖЕНЕРНОЕ ПРЕДПРИЯТИЕ

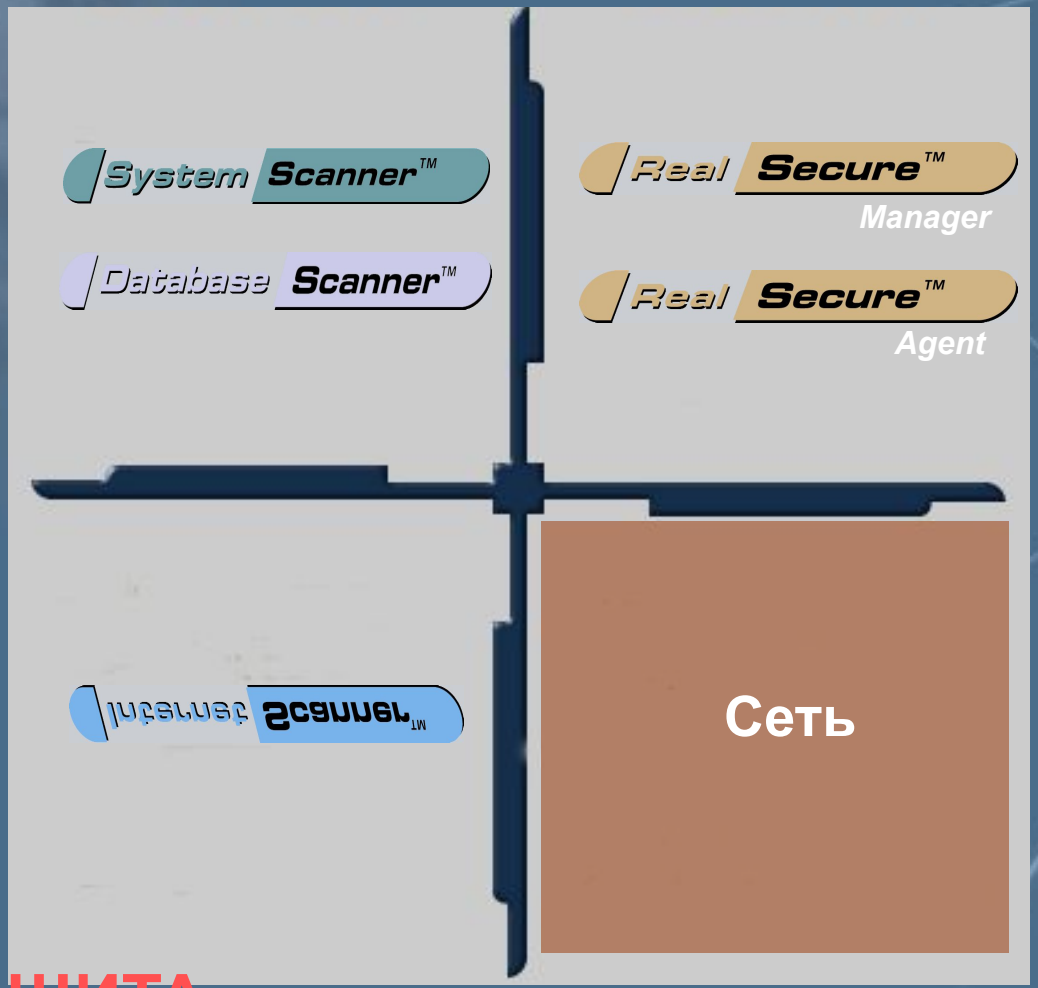
Семейство SAFEsuite

Управление уязвимостями

Управление угрозами

Система

Сеть



Система

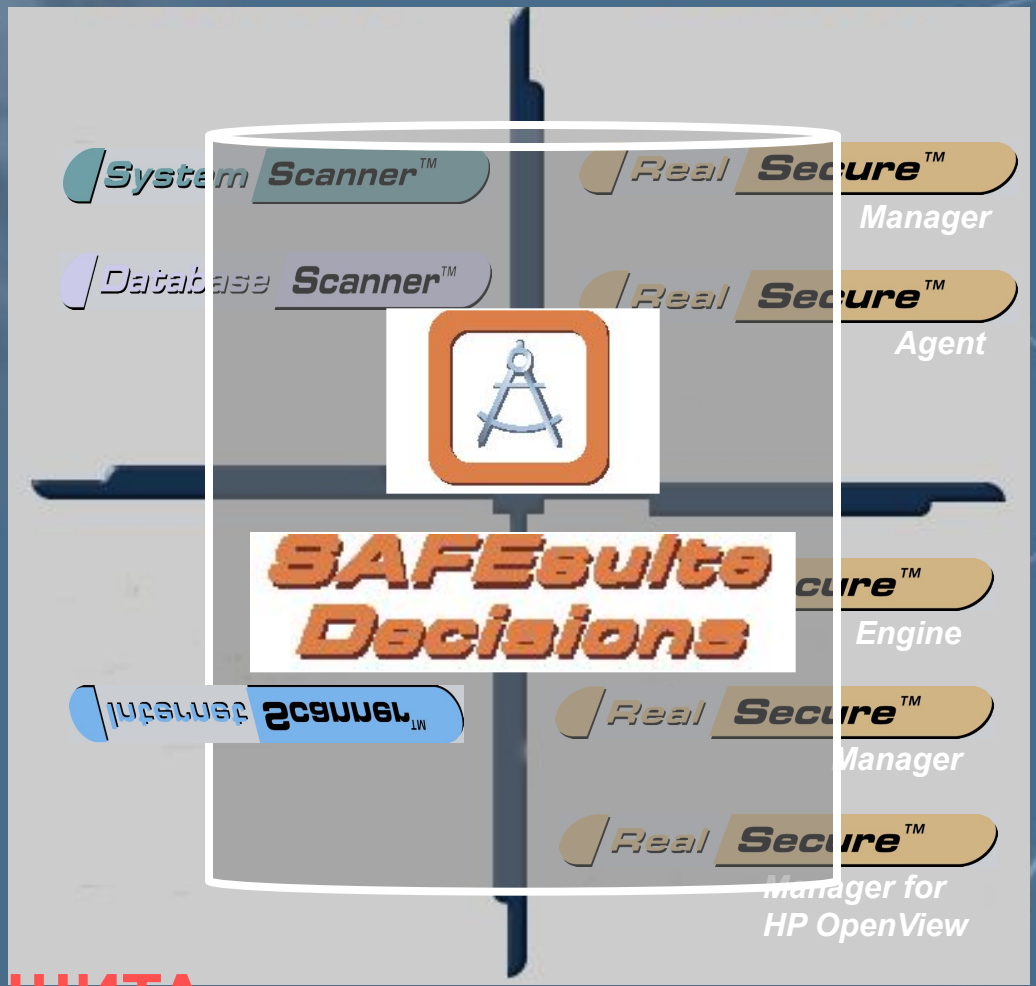
Семейство SAFEsuite

Управление уязвимостями

Управление угрозами

Система

Сеть



Система

Сеть

ИНФОРМЗАЩИТА

НАУЧНО-ИНЖЕНЕРНОЕ ПРЕДПРИЯТИЕ

Обнаружение атак на уровне сети

Анализ сетевого трафика

Поддержка распространенных протоколов (TCP/IP)

Не влияют на производительность сети

Ориентированы на высококритичные системы

Обнаружение атак на уровне сети

Достоинства:

- *низкая стоимость эксплуатации*
- *обнаружение сетевых атак*
- *хакеру трудно «замести следы»*
- *обнаружение в реальном режиме времени*
- *независимость от операционной системы*
- *обнаружение атак до достижения ею цели*

Обнаружение атак на уровне операционной системы

Анализ журналов регистрации и действий сотрудников

Поддержка syslog (Unix) и EventLog (Windows NT)

Автономный анализ и анализ в реальном времени

Ориентированы на конкретные ОС

Обнаружение атак на уровне операционной системы

Достоинства:

- контроль конкретного компьютера

- обнаружение системных атак

- работают в коммутируемых сетях

- последующий анализ данных

Обнаружение атак в реальном режиме времени на уровне сети и уровне операционной системы

Реагирование на атаки в реальном режиме времени

Поддержка протокола NetBIOS и стека протоколов TCP/IP (IP, TCP, UDP, ICMP и других на их основе)

RealSecure™

Компоненты

RealSecure Detector

– *сетевой модуль слежения (Network Engine)*

– *системный агент (System Agent)*

RealSecure Manager

RealSecure Manager HP Open View
RealSecure Manager Plus Tivoli

Возможности

Более 600 контролируемых событий

Задание шаблонов для контроля трафика

Централизованное управление

Различные варианты реагирования на атаки

Распределенная архитектура

RealSecure™

Варианты реагирования на атаки

- Регистрация события в базе данных
- Уведомления по e-mail, пейджеру и т.п.
- Генерация SNMP для систем сетевого управления
- Аварийное завершение соединения
- Управление маршрутизаторами и firewall
- Блокировка учетной записи атакующего
- Запись атаки для дальнейшего анализа
- Задание собственных сценариев обработки атак


Real Secure
ISS
www.iss.net
CA-Unicenter TNG
Tivoli
HP OpenView
ALERT
ALERT
ALERT!
ОБНАРУЖЕНА
АТАКА
Корпоративная
сеть
Human Resources
ЗАПИСЬ СЕССИИ
ПОСЫЛКА EMAIL
РЕГИСТРАЦИЯ
СЕССИИ
ВНУТРЕННЯЯ
АТАКА
DMZ
Engineering
EMAIL/
LOG/
ОТЧЕТ
РЕКОНФИГУРАЦИЯ
FIREWALL/
МАРШРУТИЗАТОРА
Firewall
Manufacturing
Router
ALERT!
ОБНАРУЖЕНА
АТАКА
ЗАВЕРШЕНИЕ
СЕССИИ
ЗАПИСЬ СЕССИИ
ВНЕШНЯЯ
АТАКА