

ОПЕРЕЖАЯ УГРОЗУ

RedCheck

Оценка соответствия Анализ защищенности

RedCheck – современное средство анализа защищенности, предоставляющее детальные сведения об эффективности мер по защите информации в корпоративной сети и её отдельных элементах.

RedCheck - мощный и эффективный сканер безопасности IT-инфраструктуры предприятия

ВОЗМОЖНОСТИ:

- Проведение детальной инвентаризации программного и аппаратно-программного обеспечения сети организации;
- Аудит уязвимостей на основе контента в формате языка OVAL для современных программных платформ: Microsoft, RedHat, Debian, Ubuntu, Oracle, POCA и др.;
- Оценка соответствия политикам и стандартам, включая PCI DSS, СТО БР, ГОСТ Р ИСО/МЭК 17799, ISO/IEC 27002;
- Контроль целостности на файловом уровне с использованием сертифицированных СЗИ;
- Анализ сетевой активности;
- Детализированные и интегральные отчёты по каждому направлению аудита.

Программа определяет уязвимости ОС и приложений, потенциально опасные настройки, осуществляет оценку соответствия требованиям политик и стандартов, контроль целостности, инвентаризацию оборудования и программ, формирует подробные отчеты.

Сертифицированные решения
ЗАО «АЛТЭК-СОФТ»

Испытательные лаборатории системы
№РОСС RU.0001.01 БИ00



Используется сертифицированное средство
контроля целостности "Фикс-библиотека 1.0"

Детализированный перечень аппаратного
и программного обеспечения целевых хостов

Более 20 000
проверок в репозитории

Международные
экспертные организации



Симуляция реализации угроз
с минимальным набором привилегий



Ежедневная
актуализация критических
обновлений безопасности

Интегральные и дифференциальные отчеты
по всем направлениям оценки и аудита

Проверка соответствия техническим стандартам
безопасности (PCI DSS, СТО БР,
ГОСТ Р ИСО/МЭК 17799, ISO/IEC 27002)

Особенности реализации:

- 6A** - безагентная реализация
- A** - агентная реализация

Совместимое программное обеспечение:

Операционные системы: Microsoft Windows, Debian, Ubuntu, RedHat, Oracle, POCA
СУБД: Microsoft SQL Server
Общие и прикладное ПО: Средства Adobe, Java, браузеры, офисные средства, антивирусные средства и др.

Архитектура RedCheck

RedCheck – 2-х уровневое приложение для использования в составе СМИБ предприятий любого масштаба.

1-ый уровень, «Информационное облако», представляет собой репозиторий OVALDB, развёрнутый в сети интернет, и сервисы работы с ним.

2-ой уровень, Сканер RedCheck разворачивается в контролируемой ИС, состоит из сервера, БД программы и консоли управления.

Основа функционирования и ядро сканера - интерпретаторы OVAL и XCCDF. Интерпретаторы работают с унифицированным SCAP-контентом, получаемым из открытого репозитория OVALDB компании АЛТЭКС-СОФТ. На сегодняшний день репозиторий включает более 20 000 проверок различных программных и аппаратно-программных платформ, полученных из авторитетных экспертных Российских и зарубежных источников. Сканирование хостов может осуществляться в ручном и автоматическом режиме по сформированным на консоли управления заданиям.

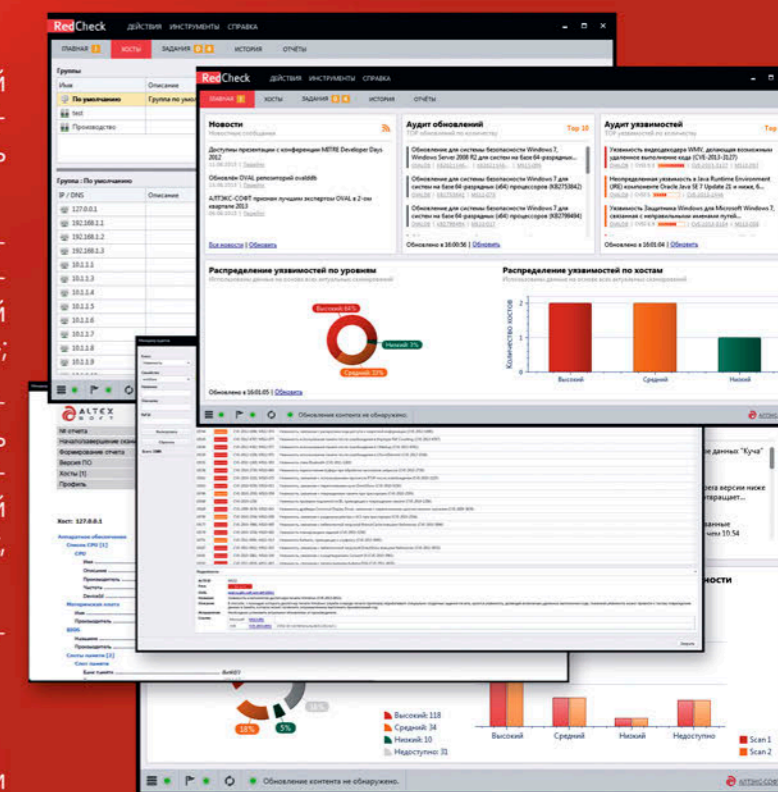
На хостах задания выполняются либо с использованием постоянно работающих управляемых служб-агентов, либо на основе безагентной технологии. По результатам проверок строятся детализированные, интегральные или дифференциальные отчёты, которые могут служить документальным подтверждением уровня защищенности информационных систем. В программе реализован offline-режим работы для закрытых АС, не имеющих подключения к сети Интернет. Функциональные возможности RedCheck постоянно расширяются как в сторону охвата новых платформ и продуктов, так и в глубину анализа объектов оценки. Совершенствуется система документирования данных аудита.

Преимущества:

- Эффективная комбинация агентной и безагентной технологий сканирования сети, позволяющая существенно сократить время проверок и обеспечить требуемый уровень безопасности;
- Минимизированные временные и финансовые затраты на развертывание систем аудита и управления безопасностью за счет использования решений на базе открытого протокола SCAP и «Best practice»;
- Встроенные полнофункциональные интерпретаторы OVAL и XCCDF, позволяющие осуществлять аудит соответствия произвольных требований безопасности, а также использовать унифицированный SCAP-контент других вендоров: Microsoft, RedHat, McAfee, eEye и др.;
- Быстрое построение интегральных и дифференциальных отчётов по результатам сканирования.

Сценарии применения:

- Внутренний аудит информационной безопасности предприятия;
- Контроль (мониторинг) уровня защищённости информационных систем;
- Оценка соответствия требованиям политик, международных, национальных и отраслевых стандартов;



- Проведение испытаний средств и систем защиты АС (ГИС), в том числе в рамках подготовки и проведения аттестации объектов информатизации;
- Оценка эффективности реализованных ИСПДн мер по обеспечению безопасности.

Ведется сертификация по требованиям безопасности ФСТЭК России

RedCheck при реализации и оценке эффективности мер защиты информации в ГИС¹ и ИСПДн²

- Выявление, анализ и оперативное устранение обнаруженных уязвимостей;
- Контроль установки обновлений ПО, включая обновления СЗИ;
- Контроль работоспособности, параметров настройки и правильности функционирования ПО и СЗИ;
- Контроль состава технических средств, ПО и СЗИ;
- Управление изменениями конфигурации ИС и СЗИ;
- Обнаружение фактов несанкционированного нарушения целостности информационной системы.

¹ Требования по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (Приказ ФСТЭК России от 11 февраля 2013 г. N 17);

² Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (Приказ ФСТЭК России от 18 февраля 2013 г. N 21).

О Репозитории OVALDB

Первоначально репозиторий OVALDB задумывался компанией АЛТЭКС-СОФТ как база данных обновлений сертифицированного по требованиям безопасности ПО Microsoft. Однако, в конечном итоге, он вырос в полноценный банк контента, описывающего множество аспектов безопасности ИС для различных платформ, технологий и решений. Сегодня, помимо обновлений, в репозитории содержатся: описания известных уязвимостей, определения (описания) программных и аппаратных средств, используемых для задач инвентаризации; широкий выбор базовых конфигураций параметров безопасности, соответствующих требованиям международных стандартов и рекомендациям вендоров, а также другой смежный контент.

Репозиторий обладает удобным функционалом по поиску нужных определений и имеет возможность их выгрузки во внешние файлы.

Ресурс OVALDB поддерживается квалифицированной командой экспертов, тесно сотрудничающих с широким кругом партнеров по международному проекту SCAP. Репозиторий получил официальный статус OVAL Adopter. Компания АЛТЭКС-СОФТ за активную деятельность в проекте по описанию и публикации уязвимостей неоднократно была удостоена статуса «OVAL Repository Contributor» от международной некоммерческой организации MITRE Corporation.



СДЕЛАНО В РОССИИ.
2008-2013 © АЛТЭКС-СОФТ.

RedCheck – зарегистрированная товарная марка «АЛТЭКС-СОФТ». Прочие встречающиеся названия и логотипы могут быть торговыми марками соответствующих владельцев.

Наша миссия в международном «проекте SCAP»:

- Содействовать внедрению и популяризации SCAP в России;
- Формировать отечественную базу уязвимостей, в том числе и для Российских продуктов и СЗИ;
- Разрабатывать простые и доступные унифицированные инструменты для работы с международными базами уязвимостей и конфигурациями безопасности;
- Принимать участие в развитии отечественных и международных стандартов управления безопасностью.



Адрес: 141067, Московская обл., г. Королев, мкр-н Болшево, ул. Маяковского, д.10А, пом. VII

Телефоны: (495) 543 31 01
(498) 601 49 38

Факс: (498) 720 89 14

E-mail: info@altx-soft.ru