НАУЧНЫЙ ЖУРНАЛ
НАУКА И МИРОВОЗЗРЕНИЕ

УДК-004

КИБЕРБЕЗОПАСНОСТЬ. УСИЛЕНИЕ ЗАЩИТЫ КОМПЬЮТЕРА

Чуриев Максат Меретмухаммедович

Старший преподаватель, кандидат технических наук, Международного университета нефти и газа имени Ягшыгелди Какаева
г. Ашхабад Туркменистан

Сопыева Огульбайрам

Преподаватель, Международного университета нефти и газа имени Ягшыгелди Какаева
г. Ашхабад Туркменистан

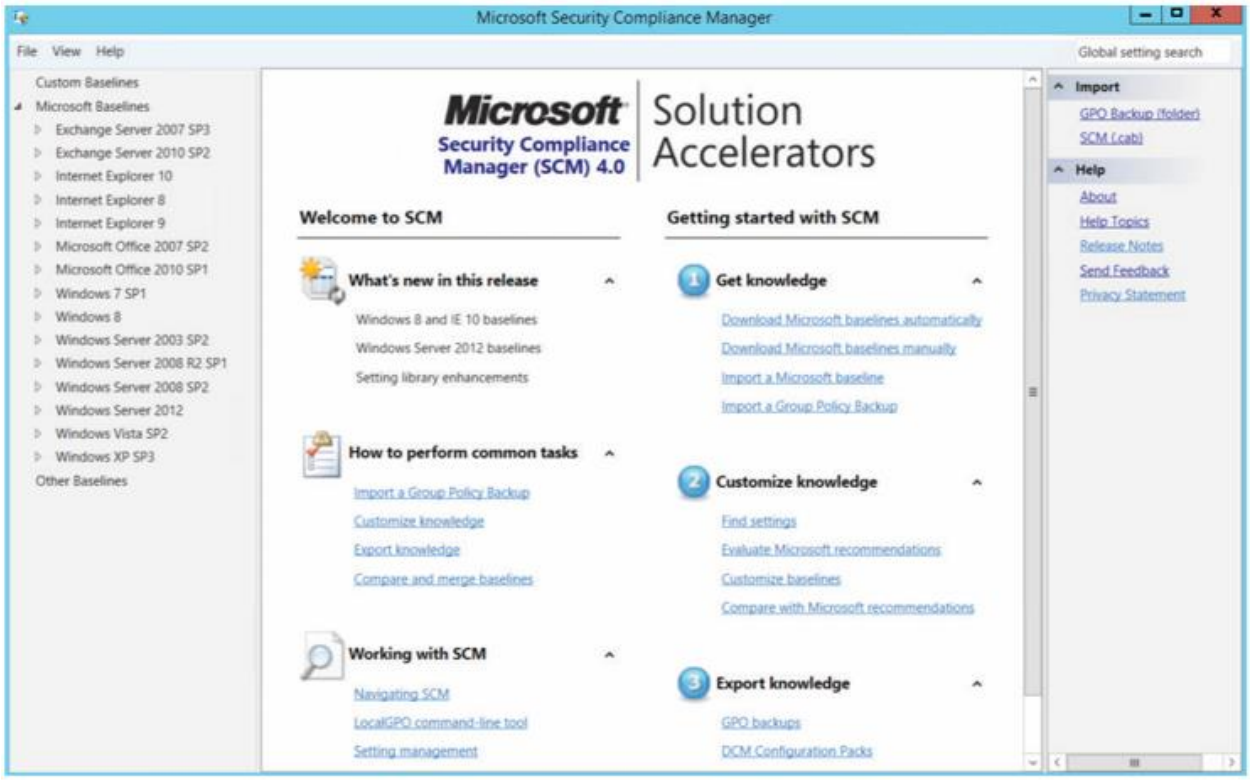
Ишангулыев Гуванч

Студент, Международного университета нефти и газа имени Ягшыгелди Какаева
г. Ашхабад Туркменистан

Когда вы начинаете планировать развертывание своей политики и решать, какие параметры следует изменить, чтобы лучше защитить компьютеры, вы усиливаете их защиту, чтобы уменьшить вектор атаки. Вы можете применять принципы стандарта списка типовых конфигураций (CCE) для своих компьютеров.

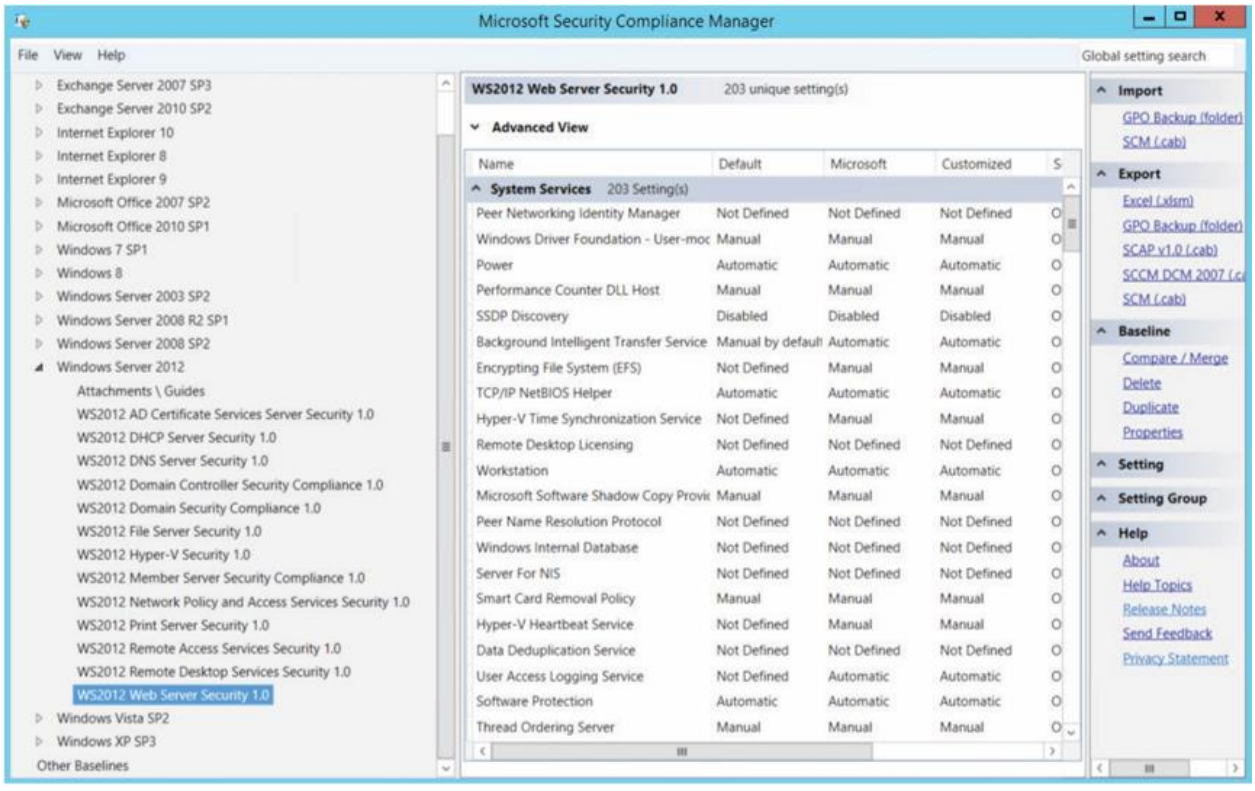
Для оптимизации развертывания вам также следует рассмотреть возможность использования базовых показателей безопасности. Это может помочь вам лучше управлять не только аспектом безопасности компьютера, но и его соответствием политике компании. Для платформы Windows вы можете использовать Microsoft Security Compliance Manager (рис.1).

На панели слева у вас есть все поддерживаемые версии операционной системы и приложения.



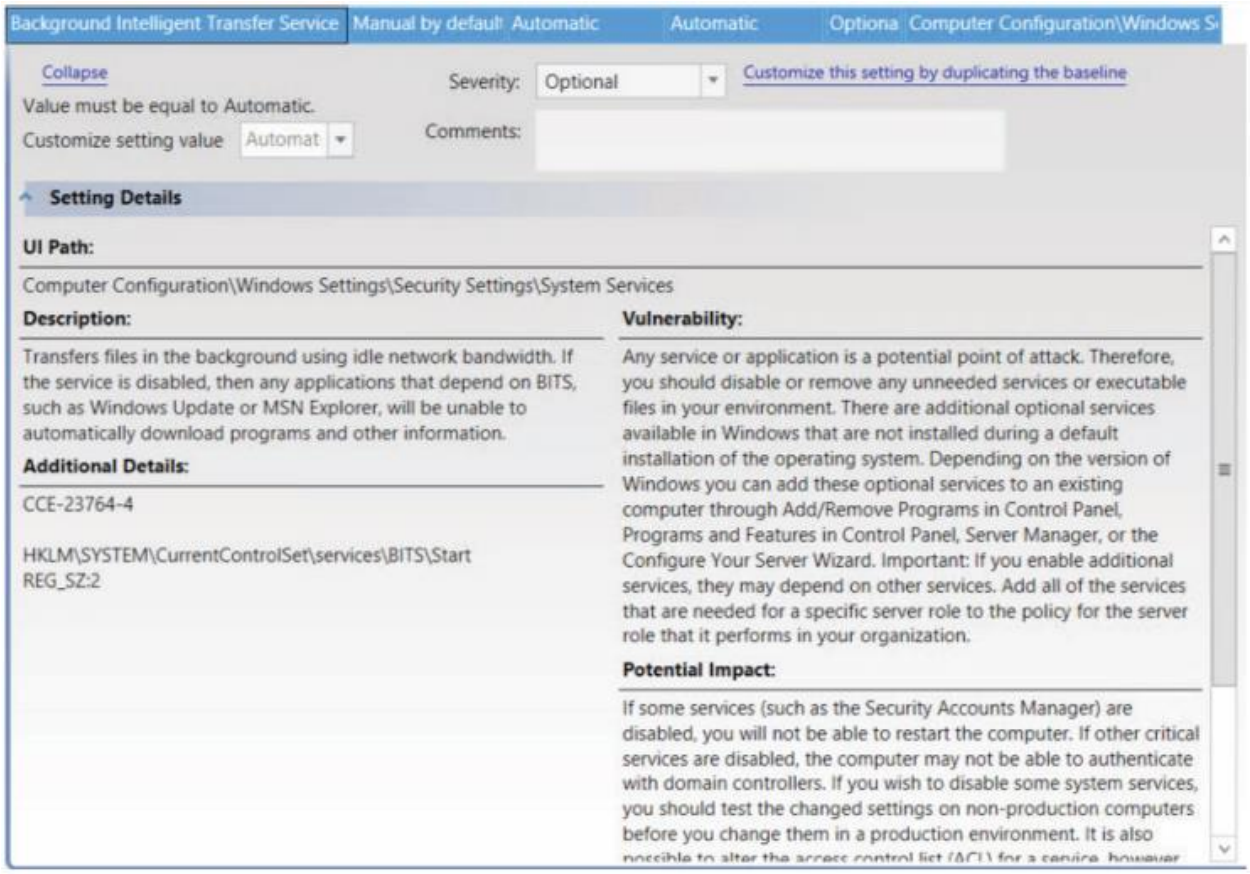
Используем Windows Server 2012 в качестве примера. Как только вы нажмете на опцию с названием этой операционной системы, то вызовете различные роли для этого сервера.

Используя в качестве примера шаблон WS2012 Web Server Security 1.0, вы увидите набор из 203 уникальных настроек, которые улучшат общую безопасность сервера.



Чтобы увидеть более подробную информацию о каждом параметре, вы должны нажать на имя конфигурации в панели справа (рис.3).

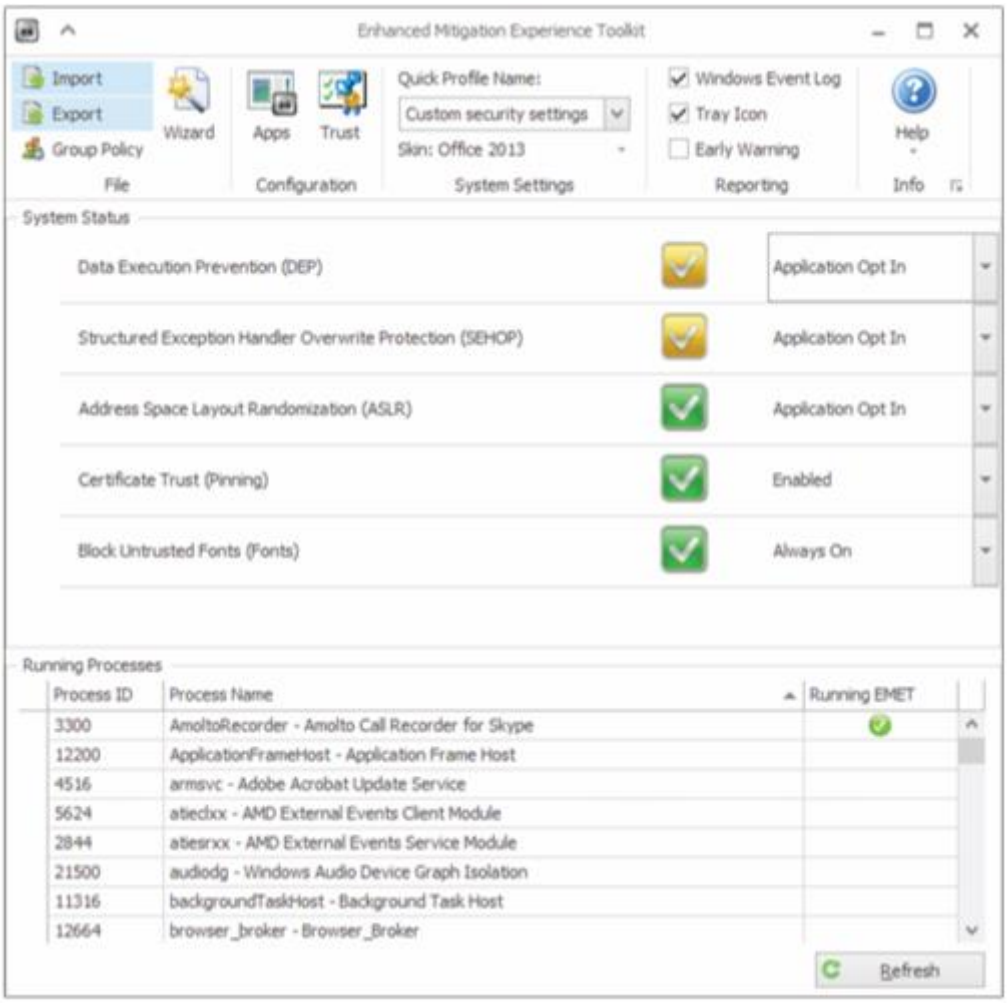
У всех этих параметров будет одинаковая структура: описание, дополнительные сведения, уязвимость, потенциальное воздействие и контрмеры. Эти предложения основаны на стандарте CCE, который является отраслевым стандартом для базовой конфигурации безопасности. После того как вы определили шаблон, который лучше всего подходит для вашего сервера / рабочей станции, вы можете развернуть его через GPO.



Когда защита объекта усиливается, необходимо убедиться, что вы используете все возможности операционной системы для значительного повышения уровня безопасности компьютера. Для систем Windows вам следует рассмотреть возможность использования набора инструментов Enhanced Mitigation Experience Toolkit (EMET).

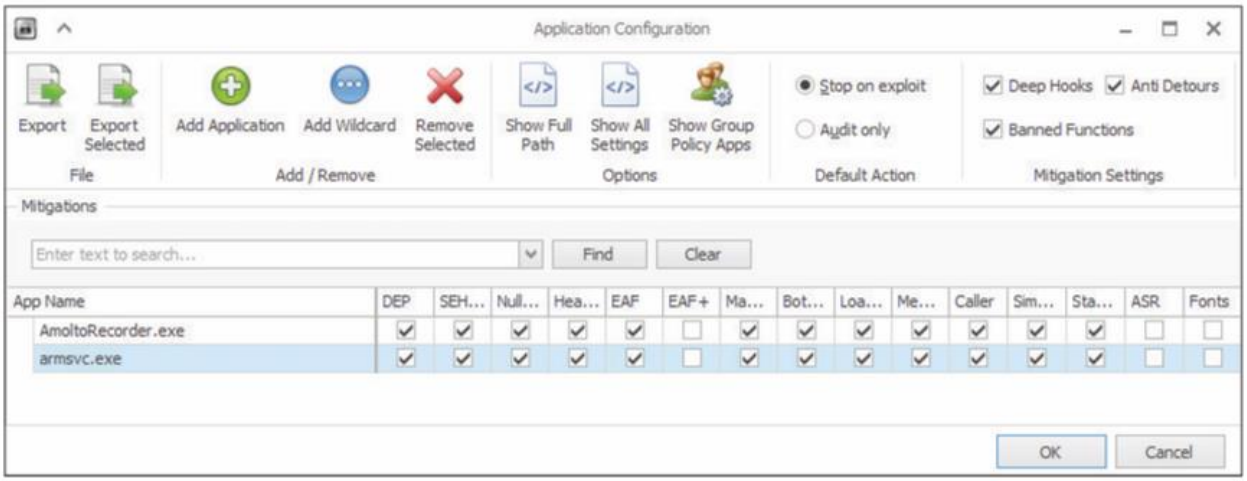
EMET помогает предотвратить доступ злоумышленников к вашим компьютерам, предвидя и предотвращая наиболее распространенные методы, используемые ими для эксплуатации уязвимостей в системах Windows. Это не только инструмент обнаружения.

Он осуществляет защиту путем перенаправления, прекращения, блокировки и аннулирования действий злоумышленника. Одним из преимуществ использования EMET для защиты компьютеров является возможность блокировать новые и неизвестные угрозы.



В разделе System Status (Состояние системы) показаны настроенные решения проблем безопасности. Хотя идеальный сценарий – это включение их всех, данная конфигурация может варьироваться в зависимости от потребностей каждого компьютера. В нижней части экрана показано, какие процессы были включены. В предыдущем примере только 1 приложение поддерживало EMET. EMET работает путем внедрения DLL в пространство памяти исполняемого файла, поэтому при настройке нового процесса для защиты с помощью EMET вам нужно будет закрыть приложение и открыть его снова (то же самое относится и к службам).

Чтобы защитить еще 1 приложение из списка, щелкните по нему правой кнопкой мыши и выберите Configure Process (Настроить процесс).



В окне Application Configuration (Конфигурация приложения) вы выбираете меры, которые хотите включить для этого приложения.