ГАЗИНФОРМ СЕРВИС

Программный комплекс по защите системно-технической инфраструктуры «Efros Defence Operations»

Описание релиза v. 2.7

Санкт-Петербург, 2023

Описание релиза программного комплекса по защите системно-технической инфраструктуры «Efros Defence Operations» v. 2.7

Программный комплекс «Efros Defence Operations» релиз v.2.7 (далее – ПК «Efros DO» или комплекс).

О релизе:

Основные нововведения релиза:

- реализовано автоматическое выделение устройств, на которых необходимо произвести изменения с учетом распространения трафика (модуль «Efros Change Manager»);
- реализован сценарий самостоятельной регистрации пользователей в гостевом портале;
- разработан механизм формирования и отображения справочной информации в ПК «Efros DO»;
- реализована централизованная система управления MAC-адресами;
- разработан клиент, реализующий функции Posturing и Supplicant.
- проведено тестирование на совместимость и работоспособность с СУБД Jatoba (4.8.2);
- осуществлено развитие модуля анализа межсетевых экранов: добавление устройств, функций, поддержка на карте сети.

Новые возможности

1 Реализация автоматического выделения устройств, на которых необходимо произвести изменения с учетом распространения трафика (модуль «Efros Change Manager)

В рамках этапа была выполнена следующая работа:

- реализована связь типов заявок с модулями лицензии;
- реализовано моделирование по запросу доступа - имитация проходимости трафика от точки А до В;
- реализовано отображение результатов моделирования в разделе «Центр задач» при работе с заявками.
- реализована возможность выбора определенных маршрутов для последующего их утверждения и выполнения;
- реализовано автоматическое выделение устройств, на которых необходимо произвести изменения с учетом распространения трафика.

В рамках моделирования было реализовано следующее:

- поиск всех маршрутов;
- поиск всех промежуточных устройств на маршрутах;
- поиск всех правил межсетевых экранов по каждому устройству, а также цветовая индикация блокирующих правил межсетевых экранов.

2 Реализация сценария самостоятельной регистрации пользователей в гостевом портале

В рамках этапа был реализован новый тип гостевого портала. Данный тип гостевого портала позволяет пользователям создавать собственные учетные записи для получения доступа к ресурсам.

Основные функции нового типа гостевого портала:

- администрирование и настройка рабочего процесса подключения для пользователей в ПК «Efros DO» – «самостоятельной регистрации» портала с возможностью задания политики безопасности (парольной политики) для каждого портала;
- настройка атрибутов, которые необходимо получить от пользователя при регистрации на портале;
- предоставление пользователю возможность заполнить форму для создания учетной записи;

– создание учетной записи;

– функция подтверждения, что регистрацию осуществляет живой пользователь, а не робот;

– возможность проверки учетной записи, созданной пользователем;

– предоставление доступа к ресурсам после успешной регистрации.

3 Разработка механизма формирования и отображения справочной информации в ПК «Efros DO»

В рамках этапа был реализован механизм формирования справочного онлайн-портала ПК «Efros DO», с возможностью перехода из комплекса ко всему справочному онлайн-порталу, так и перехода из определенного раздела комплекса в нужный раздел справочного онлайн-портала. Основанием для формирования справочного онлайн-портала является документация в формате .docx.

4 Реализация централизованной системы управления MAC-адресами

В рамках этапа для работы функциональности MAB (аутентификации по MAC-адресу) в ПК «Efros DO» была реализована возможность вести список разрешенных MAC-адресов. Также было проведено исследование по интеграции с AD при работе MAB.

5 Разработка клиента, реализующего функции Posturing и Supplicant

В рамках этапа был разработан клиент, который позволяет проверить состояние конечных точек, подключающихся к сети, на соответствие требованиям политик безопасности и использовать эти данные для управления доступом к ресурсам организации.

Выполняется проверка следующих данных:

– об операционной системе;

– об антивирусных приложениях (Kaspersky Internet Security);

– о процессах;

– о подключенных USB устройствах.

Управление политиками безопасности осуществляется из ПК «Efros DO» при наличии лицензии «Efros NAC».

6 Поддержка СУБД Jatoba (релиз Jatoba 4.8.2, включающий исправления последних уязвимостей.)

В рамках этапа было проведено тестирование на совместимость и работоспособность с «СУБД Jatoba» (v.4.8.2).

7 Развитие модуля анализа межсетевых экранов: добавление устройств, функций, поддержка на карте сети

В рамках этапа была добавлена возможность поддержки следующих типов оборудования:

- сетевое оборудование «Phoenix Contact»;
- виртуализация «РЕД Виртуализации»;
- прикладное программное обеспечение «Primo RPA Orchestrator»;
- сетевое оборудование «VipNet Prime»;
- сетевое оборудование «H3C».