ГАЗИНФОРМ СЕРВИС

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

Описание релиза v. 2.10

Санкт-Петербург, 2024

Описание релиза программного комплекса по защите системно-технической инфраструктуры «Efros Defence Operations» v. 2.10

Программный комплекс «Efros Defence Operations» релиз v.2.10 (далее – ПК «Efros DO» или комплекс).

О релизе:

Основные нововведения релиза:

1) Выполнена доработка раздела «Центр задач» (модуль «Efros Change Manager»).
2) Реализован отчет потребления трафика с возможность отправки e-mail уведомлений при превышении объема трафика сети.
3) Реализована проверка и верификация DNS-запросов.
4) Реализован механизм импорта данных из ПК «Efros Config Inspector» (ПК «Efros CI») в ПК «Efros DO».
5) Реализован метод API с аутентификацией, позволяющий получить информацию об устройствах и пользователях.
6) Реализована возможность получения информации с конечных устройств с помощью протоколов CDP и LLDP для более точного профилирования.
7) Реализована поддержка EAP-FAST и TEAP.
8) Реализована возможность отправки уведомлений при формировании кода подтверждения в виде e-mail и/или SMS при входе на гостевой портал.
9) Усовершенствован механизм интеграционного взаимодействия кроссплатформенного приложения агента ПК «Efros DO» с комплексом.
10) Выполнена доработка иерархии серверов по требованиям заказчиков.
11) Выполнена доработка эксплуатационной документации, в том числе разработана документация с описанием REST-интерфейса ПК «Efros DO».
12) Выполнены исследовательские задачи по совместимости комплекса с сетевым оборудованием Extreme X440G2-48t-10G4.
13) Добавлен ряд функциональных улучшений. Выполнены доработки для упрощения работы пользователей и оптимизации системы.

Новые возможности

1 Доработка раздела «Центр задач» (модуль «Efros Change Manager»)

В рамках этапа выполнены следующие доработки раздела «Центр задач»:

- реализован «Динамический маршрут» с автоматическим определением пользователей:
  - в карточке типа заявки «Запрос доступа» добавлен переключатель «Динамический маршрут»;
  - реализована возможность назначать тип ответственности для пользователей в подразделе «Пользователи»;
  - при динамическом маршруте запущенная по маршруту заявка направляется пользователям на каждой стадии маршрута, которые имеют указанный тип ответственности по каждому объекту защиты (ОЗ);
  - в карточке маршрута добавлена валидация: маршрут, в котором выбран тип заявки «Запрос доступа» не может иметь более одной стадии «Согласование» и «Утверждение»;
  - реализован динамический маршрут для заявок на отмену изменений запроса доступа.
- реализована отправка заявки на корректировку от стадии «Согласования»/ «Утверждения» к автору при динамическом маршруте;
- реализована ролевая модель на всех вкладках заявки: каждый пользователь видит на вкладках информацию только по тем ОЗ, по которым у него указан тип ответственности;
- реализована корректировка поведения заявки с типом «Запрос доступа»: в случае, если в результате моделирования все найденные маршруты имеют статус «Построен», то заявке автоматически присваивается статус «Закрыта»;
- реализована группировка правил по политике при выполнении заявки с типом «Отмена изменений».

2 Отчет потребления трафика с возможность отправки e-mail уведомлений при превышении объема трафика сети

В рамках доработки релиза реализованы следующие возможности:

- добавлен новый тип отчета «Доступ в сеть: трафик»;
- реализована отправка уведомлений при превышении трафика в сети в подразделе «Планировщик»;
- реализована возможность игнорирования пустого отчета, отправка пустых отчетов не осуществляется.

3 Проверка и верификация DNS-запросов

В рамках этапа добавлен новый лицензионный модуль «Efros Secure DNS». В комплексе добавлен раздел «Защита DNS», включающий в себя подразделы

- «Черный и белый списки» – позволяет управлять соответствующими списками доменов и IP-адресов для обеспечения безопасности DNS-трафика;
- «Правила IDS/IPS» – позволяет управлять правилами систем обнаружения вторжений и систем предотвращения вторжений;
- «Защита DNS-трафика» – позволяет управлять настройками модулей защиты DNS, используемых при обработке DNS-трафика;
- «Серверы пересылки» – позволяет управлять настройками DNS-сервера в части переадресации DNS-запросов;

Также добавлен подраздел событий защиты DNS.

4 Механизм импорта данных из ПК «Efros CI» в ПК «Efros DO»

Реализован импорт данных из ПК «Efros CI» в ПК «Efros DO» через веб-интерфейс комплекса.

5 Метод API с аутентификацией, позволяющий получить информацию по устройствам и пользователям

Реализован метод API с аутентификацией для предоставления внешней системе информации по устройствам и пользователям из ПК «Efros DO», запрашивающим доступ в сеть и/или на оборудование. Для формирования ответа используются данные из журналов/логов RADIUS и TACACS+.

6 Получение информации с конечных устройств с помощью протоколов CDP и LLDP

Реализована возможность получения информации с конечных устройств с помощью протоколов CDP и LLDP для более точного профилирования. Получение данных производится при настройке задачи по расписанию «Запустить SNMP сканирование».

7 Поддержка EAP-FAST и TEAP

Реализована возможность гибкой аутентификации EAP-FAST через защищенный туннель. Также была реализована возможность управления списком методов аутентификации EAP на основе сертификатов защищенного расширяемого протокола аутентификации TEAP.

8 Отправка уведомлений при формировании кода подтверждения в виде e-mail и/или SMS при входе на гостевой портал

Реализован метод отправки кода подтверждения в виде e-mail и/или SMS на номер телефона, указанный пользователем на странице входа на гостевой портал. Также в комплекс добавлена возможность настройки внешней системы «SMS-провайдеры».

9 Механизм интеграционного взаимодействия кроссплатформенного приложения агента ПК «Efros DO» с комплексом

Усовершенствован механизм интеграционного взаимодействия кроссплатформенного приложения агента ПК «Efros DO» с комплексом. Реализованы следующие возможности:

- механизм формирования инсталляционного пакета, в состав которого входят:
  - дистрибутив агента ПК «Efros DO»;
  - дистрибутив суппликанта ПК «Efros DO»;
  - дистрибутив модуля «Контроль целостности до загрузки ОС»;
  - защищенный файл с данными: версии пакета и операционной системы, список изменений версий агентов, эталонные контрольные суммы отдельных компонентов и всего инсталляционного пакета.
- интеграция с подсистемой MinIO для хранения инсталляционных пакетов;
- добавлен новый подраздел «Установка и Обновление», позволяющий загружать на сервер инсталляционные пакеты и настраивать централизованное обновление агентов, установленных на конечных устройствах по расписанию или вручную. Для поддержки успешного обновления данную функцию должен

поддерживать, как сам комплекс, так и агент, установленный на конечном устройстве;

– проверка целостности агента, который реализован на основе механизма сбора контрольных сумм, их отправке на сервер и сравнении полученных на агенте контрольных сумм с эталонными значениями;

– интеграция агента ПК «Efros DO» и модуля «Контроль целостности до загрузки ОС» (в режиме аудита) для конфигурирования политики контроля целостности объектов до загрузки операционной системы.

10 Доработка иерархии серверов

Реализованы следующие возможности иерархии серверов:

– доработано логирование событий аудита действий пользователя головного сервера на подчиненном;

– реализованы проверки при добавлении новых подчиненных серверов:

  • проверка на подчиненном сервере токена подключения, который использует головной сервер при добавлении подчиненного сервера;

  • проверка на наличие зацикленности в иерархии при добавлении новых подчиненных серверов.

– добавлена вкладка «Вышестоящие серверы», на которой отображаются вышестоящие серверы, к которым текущий сервер подключен как подчиненный;

– реализован набор системных событий, связанных с иерархией серверов;

– добавлено оповещение пользователя (всплывающее окно) об успешном или неуспешном переключении между серверами иерархии;

– реализована возможность формировать отчет об уязвимостях на ОЗ по подчиненным серверам.

11 Доработка эксплуатационной документации

Обновлена эксплуатационная документация на комплекс, описаны новые функциональные возможности в пяти частях руководства пользователя.

Разработано руководство, которое содержит описание REST-интерфейса ПК «Efros DO». Для методов API описаны: атрибуты запроса/ответа, примеры запроса/ответа.

12 Исследовательские задачи по совместимости комплекса с сетевым оборудованием Extreme X440G2-48t-10G4

Проведена проверка совместимости комплекса с сетевым оборудованием Extreme X440G2-48t-10G4. Основные результаты проверки:

- комплекс поддерживает организацию доступа на оборудование с использованием протоколов RADIUS и TACACS+;
- комплекс поддерживает авторизацию команд только по протоколу RADIUS.

13 Функциональные улучшения

Добавлен ряд функциональных улучшений и выполнены следующие доработки для оптимизации работы пользователей и системы:

- для системных заявок выполнена доработка скрипта конфигурирования Cisco ASA, Cisco FMC и Check Point для добавления нескольких объектов;
- для отчета «Правила МЭ» добавлен поиск по политикам и правилам;
- для проверок МЭ заменено значение «Другой протокол» на вывод актуального списка протоколов;
- выполнена доработка построения множественных маршрутов в карте сети;
- добавлены новые поля в карточку трассировки событий доступа в сеть, вкладка «Аутентификация»;
- добавлен учет нового типа отчёта по PBR для устройств Check Point Gateway;
- реализован клиент-pathfinder для построения маршрута на карте сети;
- реализовано сохранение профиля виртуального объекта (ВО) на карте сети без кнопки «Сохранить», при изменении профиля ВО сохранение производится автоматически;
- реализовано расширение модели системных событий, добавлено отдельное логирование общих системных событий;
- доработана форма выбора отчета устройств для сравнения. Убрано дерево элементов в форме выбора отчета, сравнение производится в рамках одного типа устройства;
- расширена функциональность привилегии управления при назначении прав доступа на ОЗ (группа «Администрирование»);
- реализовано автоматическое формирование имени файла при экспорте событий;
- расширен лицензионный модуль «Контроль целостности и проверки соответствия», добавлены «Ноды контейнеризации»;

- изменено отображение списка сетевых пользователей для групп LDAP;
- для проверок МЭ добавлено отображение списка зависимостей редактируемой зоны и добавлены правила при редактировании параметров зоны на соответствие основным правилам;
- разработан API метод для блокировки учетных записей администраторов RADIUS и TACACS+ извне.