ГАЗИНФОРМ СЕРВИС

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

Описание релиза v. 2.11

Санкт-Петербург, 2024

Описание релиза программного комплекса по защите системно-технической инфраструктуры «Efros Defence Operations» v. 2.11

Программный комплекс «Efros Defence Operations» релиз v.2.11 (далее – ПК «Efros DO» или комплекс).

О релизе:

Основные нововведения релиза:

1) Выполнена доработка раздела «Центр задач» (модуль «Efros Change Manager»).
2) Реализована гибкость и масштабируемость системы в условиях растущей нагрузки (вертикальное и горизонтальное масштабирование).
3) Реализовано ведение журнала событий доступа в сеть для гостевых порталов.
4) Выполнена доработка эксплуатационной документации.
5) Выполнена доработка агента ПК «Efros DO» и реализована возможность управления списками IP-адресов.
6) Реализован экспорт данных для автоматического резервного копирования конфигурации ПК «Efros DO».
7) Реализован импорт групп конечных точек при миграции из Cisco ACS.
8) Реализована синхронизация с доменом для сбора и хранения данных атрибутов LDAP-пользователей.
9) Выполнены исследовательские задачи по развитию возможностей работы с конечными точками.
10) Разработано описание метода API для экспорта списка пользователей из журнала событий TACACS+.
11) Реализована поддержка протокола TLS 1.3.
12) Реализована технология единого входа (SSO) в рамках экосистемы GIS BIOM с использованием протокола Kerberos.
13) Реализована возможность отправки e-mail уведомлений при достижении установленного объема памяти.
14) 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 новый тип заявки «Конфигурирование оборудования»;
- реализована возможность автоматического закрытия заявки типа «Запрос доступа» в случае непрохождения зонного анализа.

2 Гибкость и масштабируемость системы в условиях растущей нагрузки (вертикальное и горизонтальное масштабирование)

В рамках доработки релиза проведено исследование кластерной версии ПК «Efros DO» в условиях растущей нагрузки (вертикальное и горизонтальное масштабирование).

Для кластерной версии комплекса реализовано равномерное распределение нагрузки между всеми нодами кластера при обработке запросов RADIUS или TACACS+ функционального модуля «Efros Network Access Control» («Efros NAC»).

3 Ведение журнала событий доступа в сеть для гостевых порталов

Реализована возможность ведения журнала событий доступа в сеть при работе с гостевыми порталами с взаимосвязью данных: дата события, MAC-адрес, логин и Ф.И.О. гостевого пользователя.

Добавлена возможность перехода к журналу событий со следующих страниц веб-интерфейса комплекса: карточка гостевого портала, карточка пользователя гостевого портала и карточка конечной точки.

4 Доработка эксплуатационной документации

Обновлена эксплуатационная документация на комплекс согласно изменениям релиза. Добавлена информация о протоколах и портах, по которым производится взаимодействие с комплексом.

Улучшена структура документации, изменен порядок описания функциональных возможностей в пяти частях руководства пользователя. Добавлено два отдельных приложения к руководствам пользователя:

- описание возможностей контроля целостности функционального модуля «Efros Integrity Check Compliance» («Efros ICC») оформлено отдельным приложением к части 3 руководства пользователя;
- описание работы с агентом ПК «Efros DO» оформлено отдельным приложением к части 4 руководства пользователя.

5 Доработка агента ПК «Efros DO» и возможность управления списками IP-адресов

В рамках доработки агента ПК «Efros DO» реализованы следующие возможности:

- разработан графический интерфейс агента ПК «Efros DO» для управления с конечной точки супликантом агента и параметрами самого агента;
- реализована возможность выбора режима работы агента под управлением ПК «Efros DO» и без управления ПК «Efros DO»;
- разработана возможность сбора событий с конечной точки для ОС Windows;
- выполнены доработки взаимодействия агента с модулем «Контроль целостности объектов до загрузки операционной системы»;
- добавлена возможность выбора различных политик безопасности для агентов, установленных на ОС одного и того же семейства.

Также реализована возможность управления списками IP-адресов для формирования гео-ограничений (в том числе, запрет на удаленное подключение пользователей с IP-адресов за пределами заданного перечня стран).

6 Реализован экспорт данных для автоматического резервного копирования конфигурации ПК «Efros DO»

Реализована возможность экспорта данных для автоматического резервного копирования конфигураций «Контроль устройств», что позволяет восстановить данные контроля устройств ПК «Efros DO» с помощью доработанной возможности импорта данных.

7 Реализован импорт групп конечных точек при миграции из Cisco ACS

Реализована возможность импорта групп конечных точек при миграции из Cisco ACS для сокращения времени формирования списка устройств.

8 Синхронизация с доменом для сбора и хранения данных атрибутов LDAP-пользователей

Реализована возможность синхронизации с доменом для сбора и хранения данных атрибутов LDAP-пользователей в подразделе «Конечные точки».

9 Исследовательские задачи по развитию возможностей работы с конечными точками

В рамках данного этапа были проведены следующие исследовательские работы по расширению возможностей комплекса:

- помещение конечных точек в карантин до утверждения политик безопасности администратором ИБ по результатам профилирования. Разработано несколько вариантов реализации задачи, одно из которых не требует доработок комплекса;
- поддержка настройки режима ограничения портов, по которым подключаются конечные точки, и контроль перемещений конечных точек между портами локальной вычислительной сети (ЛВС). Разработано решение, которое добавлено в план график выполнения работ первого квартала 2025 года.

Также выполнены исследовательские задачи по гарантийному письму от «Газпромбанк» (Акционерное общество).

10 Экспорт списка пользователей из журнала событий TACACS+

Для метода API с аутентификацией для предоставления внешней системе информации по пользователям из ПК «Efros DO», запрашивающим доступ на оборудование, разработано описание экспорта списка пользователей из журнала событий TACACS+.

11 Поддержка протокола TLS 1.3

Реализована поддержка протокола TLS 1.3 для доступа в сеть. Данная версия протокола доступна для выбора в полях «Минимальная версия TLS» и «Максимальная версия TLS» при настройке конфигурации TLS в веб-интерфейсе комплекса.

12 Технология единого входа (SSO) в рамках экосистемы GIS BIOM с использованием протокола Kerberos

Реализована технология единого входа (Single Sign-On) для выполнения аутентификации пользователя в ПК «Efros DO» по имени доменной учетной записи в рамках экосистемы GIS BIOM с использованием протокола Kerberos.

13 Отправка e-mail уведомлений при достижении установленного объема

Для контроля объема хранилища выполнены следующие доработки:

- в веб-интерфейсе комплекса добавлены параметры для задания объема памяти, выделенной для хранения локальных журналов регистрации событий информационной безопасности модулей «Контроль устройств» и «Контроль доступа»;

– добавлена возможность отправки уведомлений при превышении % от объема хранения в подразделе «Планировщик».

14 Функциональные улучшения

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

– реализован перенос профилей SNMP на уровень ОЗ:
  - подраздел «SNMP профили» перемещен в раздел «Объекты сети»;
  - на форме объекта защиты добавлен блок настроек «Подключение по SNMP»;
  - доработаны настройки запуска SNMP сканирования в подразделе «Планировщик»;
  - реализована утилита для миграции данных профилей SNMP. Утилита запускается автоматически при обновлении комплекса.

– реализована поддержка аутентификации и авторизации сетевого оборудования типа Juniper;

– доработано представление отчета «Правила МЭ». Реализовано разделение страницы отчета на две части: список набора правил и отображение колонок по выбранному правилу;

– доработки возможностей иерархии серверов, также реализовано ведение системных событий подчиненных серверов;

– произведено обновление модуля DGA и корректировка правил IPS лицензионного модуля «Efros Secure DNS»;

– реализована возможность создания кратковременного доступа на гостевой портал с саморегистрацией;

– реализована переработка групп пользователей ПК «Efros DO»;

– доработки возможностей карты сети:
  - реализована имитация проходимости трафика;
  - реализовано отображение полного списка всех сработавших правил (VPN, NAT) при построении маршрута;
  - добавлена вложенность по интерфейсам.