EFROS
DEFENCE OPERATIONS

МНОГОФУНКЦИОНАЛЬНЫЙ КОМПЛЕКС ПО ЗАЩИТЕ СЕТЕВОЙИНФРАСТРУКТУРЫ

EFROS Defence Operations

+7 (812) 677-20-50
sales@gaz-is.ru

Санкт-Петербург, 2025г.
www.gaz-is.ru

GIS ГАЗИНФОРМ СЕРВИС

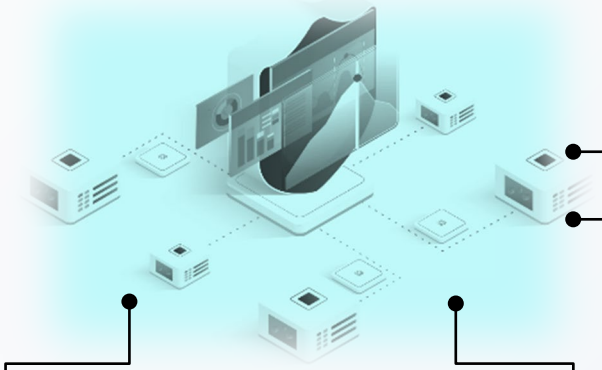
EFROS
DEFENCE OPERATIONS

Решение для мониторинга инцидентов и анализа безопасности ИТ-инфраструктуры, включающее:

- аутентификацию и авторизацию конечных точек,
- аудит топологии и сегментации сети,
- анализ векторов атак,
- контроль целостности и соответствия политикам безопасности системных файлов и параметров прикладного ПО.

ДЕЙСТВИЯ ЗЛОУМЫШЛЕННИКОВ ПО МАТРИЦЕ MITREATT&CK

Проблематика



01 Подключение дополнительных устройств

02 Выявление уязвимостей в клиентском ПО

03 Эксплуатация уязвимостей для повышения привилегий

04 Отключение или перенастройка системного межсетевого экрана

05 Точечный или сетевой отказ в обслуживании

06 Несанкционированное использование ресурсов

ПОДБОР ОПТИМАЛЬНЫХ ИНСТРУМЕНТОВ ЗАЩИТЫ

Цель

01

Автоматизация управления **политиками безопасности**

02

Анализ и визуализация сетевой связности, топологии

03

Интеграция с **облачными и гибридными** средами

04

Соблюдение **нормативных требований**

05

Фокус на пользовательском опыте. Обеспечение процесса безопасной разработки

ПК EFROS«DEFENCE OPERATIONS»

Решение

01 NETWORK ACCESSCONTROL
разграничение и контроль доступа в сети

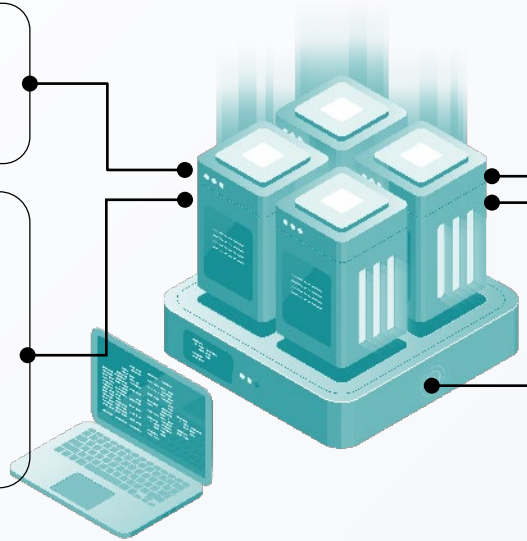
02 NETWORKASSURANCE
контроль конфигураций и топологии сети

VULNERABILITYCONTROL
анализ уязвимостей и построение векторов атак

03 FIREWALLASSURANCE
оптимизация и настройка межсетевых экранов

CHANGEMANAGER
автоматизация процессов управления правилами

04 INTEGRITY CHECK COMPLIANCE
контроль целостности и проверки соответствия



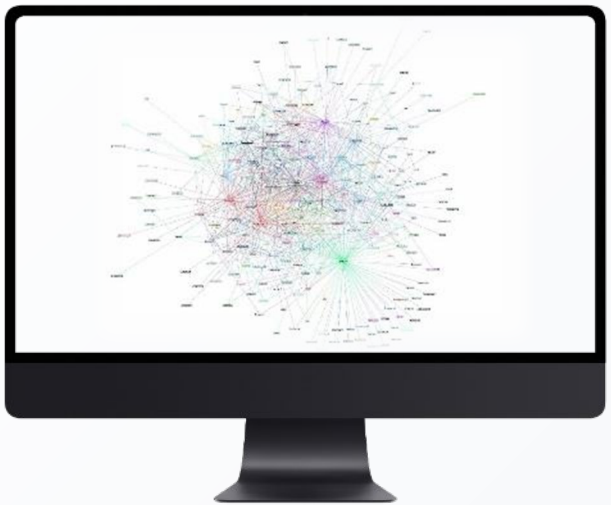
ВЕНДОР РОССИЙСКОГО ПО

О нас

- **130+ пользователей Efros**
- Полностью импортонезависимое решение. Реестр отечественного ПО № 18615
- Реализация требований:
  - Указ Президента РФ № 250, 166 (импортозамещение)
  - Проект Федерального закона N 502104-8 (о введении оборотных штрафов)
  - Приказы ФСТЭК России 17 (Гос. ИС), 21 (ПДн), 31 (АСУТП), 239 (КИИ), 118 (защита контейнеров)
- Сертификация ФСТЭК России УД4

НЕКОНТРОЛИРУЕМОЕ ПОДКЛЮЧЕНИЕ
дополнительных устройств

Проблематика



Увеличение количества распределенных сетей и удаленных пользователей. Рост доли IoT устройств в производстве.

Предотвращение атак через учетную запись в отсутствии гранулярных прав доступа администраторов.

Приоритет к подходам, **предотвращающим атаки через доверенных партнеров** (поставщиков услуг и сервисов, имеющим доступ во внутреннюю сеть)

МОДУЛЬ УПРАВЛЕНИЯ ДОСТУПОМ К СЕТИ

01 NAC

Efros DefOps
«Network Access Control»

- Централизованное управление политиками доступа конечных устройств и администраторов сети
- Контроль проводных, беспроводных и удаленных (VPN) подключений
- Поддержка разных методов и протоколов аутентификации: 802.1X, MAB, сертификаты
- Гибкие политики авторизации: RADIUS CoA, загружаемые ACL, назначение VLAN и др
- EDO-агент для проверки подключаемых устройств на соответствие политикам безопасности
- Разграничение доступа администраторов к активному сетевому оборудованию (TACACS)

Импортозамещение:

Cisco ISE, aruba ClearPass, pormox, FortiNAC

МОДУЛЬ АНАЛИЗА МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ

02 FA

Efros DefOps
«Firewall Assurance»

- Оптимизация и анализ действующих настроек межсетевого экранирования.
- Упрощение конфигурации и уменьшение нагрузки на межсетевой экран за счет выявления дублирующих, «теневых» и неиспользуемых правил.
- Контроль политики сетевого доступа на уровне зон безопасности межсетевых экранов.

Импортозамещение:

ManageEngine Firewall Analyzer

SKYBOX Firewall Assurance

algosec Firewall Analyzer

tufin SecureTrack

МОДУЛЬ УПРАВЛЕНИЯ МЕЖСЕТЕВЫМИ ЭКРАНАМИ

03 CM
Efros DefOps
«Change Manager»

- Создание workflow на изменение сетевого доступа за счет встроенной системы заявок или интеграции с внешними системами.
- Формирование рекомендаций по оптимизации настроек МЭ перед изменением конфигураций межсетевых экранов при изменении сетевых доступов.
- Автоматическое применение планируемых изменений.
- Ведение журнала произведенных изменений и исполнителей.

Импортозамещение:

ManageEngine Firewall Analyzer
SKYBOX Firewall Assurance
algosec Firewall Analyzer
tufin SecureTrack

ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ

Повышение привилегий

Проблематика

- Контроль **неизменных параметров системы.**
- Инвентаризация, **анализ влияния изменений.**
- **Проактивное управление уязвимостями** , оценка реальной защищенности инфраструктуры.

МОДУЛЬ УПРАВЛЕНИЯ КОНФИГУРАЦИЕЙ СЕТИ

04 NA

Efros DefOps
«Network Assurance»

- Инвентаризация всех объектов защиты, сбор конфигураций сетевого оборудования и построение карты сети.
- Моделирование топологии, анализ влияния изменений на «цифровом двойнике».
- Стандартные и пользовательские проверки соответствия конфигураций
- Анализ сетевых путей, графическая демонстрация подключений и доступа приложений из любого источника и к любому месту назначения.
- Анализ соответствия конфигураций сетевых устройств заданным стандартам и лучшим практикам.

Импортозамещение:

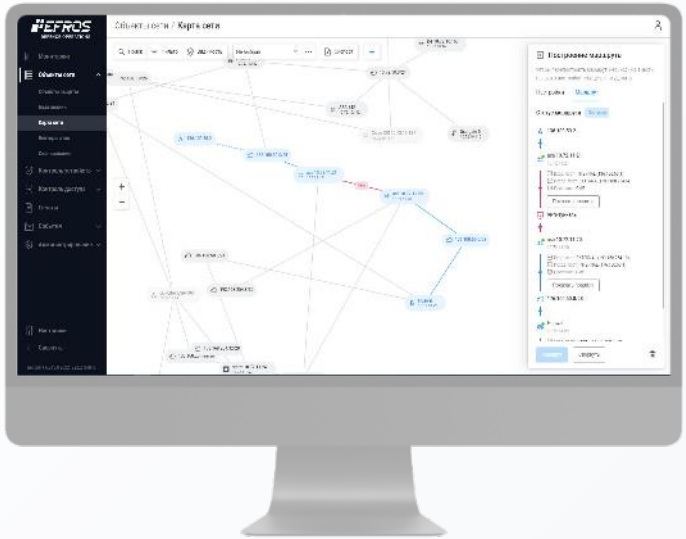
ManageEngine Network Configuration Manager

SKYBOX Network Assurance

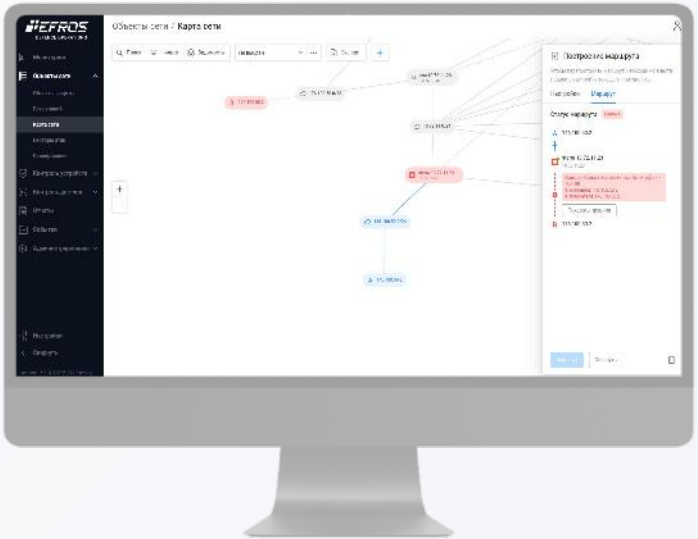
Network Configuration Manager

АНАЛИЗ МАРШРУТА

Efros DefOps
«Network Assurance»



- Учитываем маршрутизацию, VPN, NAT
- VRF, MPLS*



*доступно для ряда вендоров

МОДУЛЬ КОНТРОЛЯ УЯЗВИМОСТЕЙ

05 VC

Efros DefOps
«Vulnerability Control »

- Автоматический сбор информации об ИТ-активах из сканеров, систем инвентаризации и патч-менеджмента.
- Выявление вновь появляющихся уязвимостей в период до/между сканированиями.
- Проверка инфраструктуры с целью выявления известных уязвимостей в соответствии с БДУ ФСТЭК, CVE, OVAL и др.
- Расчет возможных векторов атак с учетом модели нарушителя. Визуализация вектора на интерактивной карте.

Аналоги:

Qualys. tripwire positive technologies

МОДУЛЬ КОНТРОЛЯ ЦЕЛОСТНОСТИ

06 ICC

Efros DefOps
«Integrity Check Compliance»

- Контроль целостности файлов в различных ОС.
- Контроль целостности таблиц в СУБД.
- Предоставление рекомендаций по внесению изменений для соответствия требованиям регуляторов.
- Стандартные и пользовательские проверки соответствия объектов защиты.

Аналоги:

tripwire

РАЗРАБОТКИ 2025

Дорожная карта

NA

Анализ изменения сети, **развитие возможностей моделирования** , группировка активов и др.

FA

Консолидация правил, **работа с объектами правил** (Cisco, Check Point, Fortinet).

CM

Создание новых типов заявок на добавление, удаление, изменение правил. Ресертификация правил

NAC

Интеграции с отечественными продуктами ИБ (в первую очередь, VPN). **Развитие возможностей EDO-агента** и безагентские профилирование

ICC

Развитие встроенной библиотеки проверок PCI DSS, патч-менеджмент.

О НАС

8
Филиалов в РФ

Более 130 компаний пользователей Efros

3 мажорных релиза в год

20 лет
Разработки решений для рынка ИБ

Программа обучения

4 УД
В соответствии с сертификацией ФСТЭК России

Полностью импортонезависимое решение

24/7
Техподдержка

ПОДДЕРЖИВАЕМОЕ ОБОРУДОВАНИЕ

infotecs
ФАКТОР-ТС
ELTEX
UserGate
КОД БЕЗОПАСНОСТИ
Linux
vmware
cisco
s•terra
HUAWEI
AVAYA
JUNIPER NETWORKS
Lenovo
FORTINET
Check Point SOFTWARE TECHNOLOGIES LTD.
hp
Microsoft Windows
HIRSCHMANN A BELDEN BRAND
...

*Полный перечень на сайте ГИС и в технической документации

EFROS
DEFENCE OPERATIONS

GIS ГАЗИНФОРМ СЕРВИС
gaz-is.ru

Следующие шаги

ДЕМО ВЕРСИЯ

ПИЛОТНОЕ ВНЕДРЕНИЕ

РАСЧЕТ СПЕЦИФИКАЦИИ

+7 (812) 677-20-50
sales@gaz-is.ru