EFROS
DEFENCE OPERATIONS

Многофункциональный комплекс по защите сетевой инфраструктуры

EFROS Defence Operations

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

Санкт-Петербург. 2024г.
www.gaz-is.ru

GIS
ГАЗИНФОРМ
СЕРВИС

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 MITRE ATT&CK

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

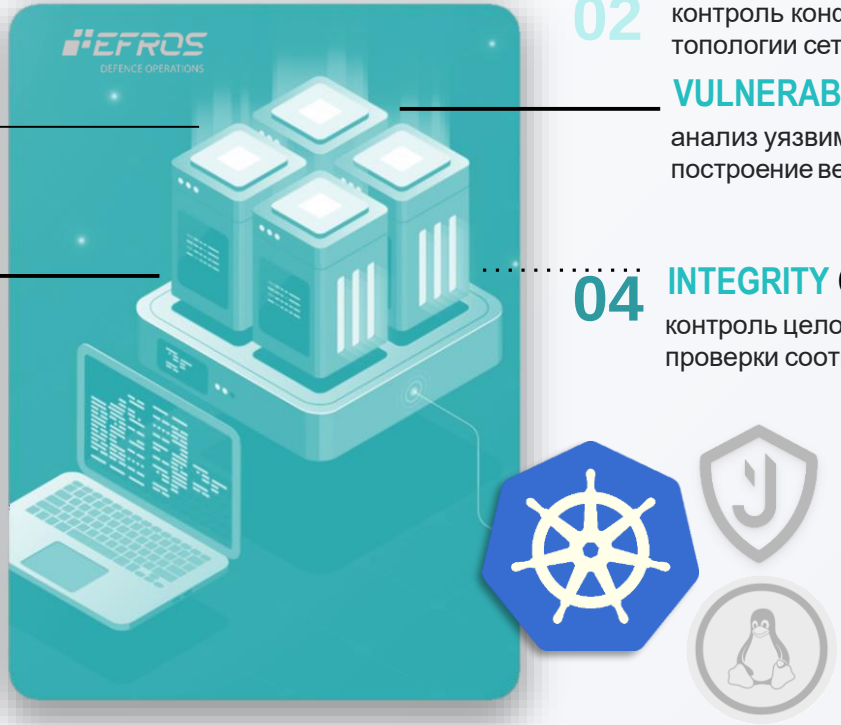
ПК EFROS «DEFENCE OPERATIONS»

01 NETWORK ACCESS CONTROL
разграничение и контроль доступа в сети

FIREWALL ASSURANCE
оптимизация и настройка межсетевых экранов

03 CHANGE MANAGER
автоматизация процессов управления правилами

NETFLOW ANALYZER
статистика по потокам данных в сети

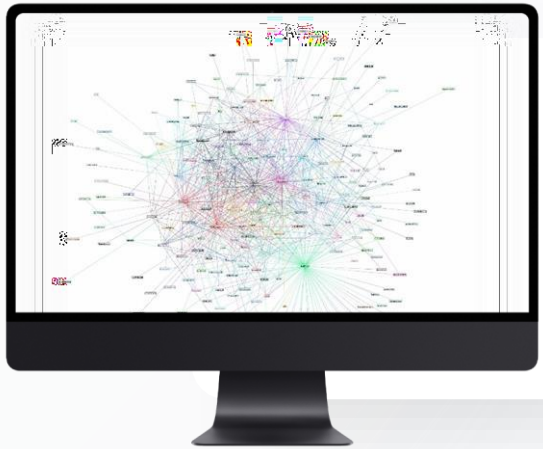


02 NETWORK ASSURANCE
контроль конфигураций и топологии сети

VULNERABILITY CONTROL
анализ уязвимостей и построение векторов атак

04 INTEGRITY CHECK COMPLIANCE
контроль целостности и проверки соответствия

НЕКОНТРОЛИРУЕМОЕ ПОДКЛЮЧЕНИЕ
дополнительных устройств



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

Увеличение количества распределенных сетей и удаленных пользователей. Рост подключений через VPN и доли IoT устройств, в том числе в производстве.

**По данным tadviser.ru Xakep.ru securelist.ru gartner.com*

МОДУЛЬ УПРАВЛЕНИЯ ДОСТУПОМ К СЕТИ

01 NAC

Efros DefOps
«Network Access Control»

- Централизованное управление политиками доступа конечных устройств и администраторов сети
- Управление доступом к сетевым устройствам, поддерживающим протоколы TACACS+, RADIUS
- Авторизация сетевых устройств по MAC адресам, протоколу EAP-PEAP, сертификатам
- Создание порталов аутентификации для гостевых пользователей и персональных устройств
- Ведение журналов событий и формирование отчетов для анализа и предотвращения возможных инцидентов ИБ
- Проверка состояния оконечных устройств на соответствие политикам безопасности с помощью EDO-клиента (ОС, антивирусные приложения, процессы, USB-устройства)

Импортозамещение:

Cisco ISE · aruba ClearPass · portnox · FortiNAC

МОДУЛЬ УПРАВЛЕНИЯ КОНФИГУРАЦИЕЙ СЕТИ

- Инвентаризация всех объектов защиты, сбор конфигураций сетевого оборудования и построение карты сети.
- Анализ соответствия конфигураций сетевых устройств заданным стандартам и лучшим практикам.
- Стандартные и пользовательские проверки соответствия конфигураций
- Анализ сетевых путей, графическая демонстрация подключений и доступа приложений из любого источника и к любому месту назначения.

Визуализация на карте сети возможных маршрутов прохождения заданного типа трафика с демонстрацией разрешающих и запрещающих правил фильтрации.

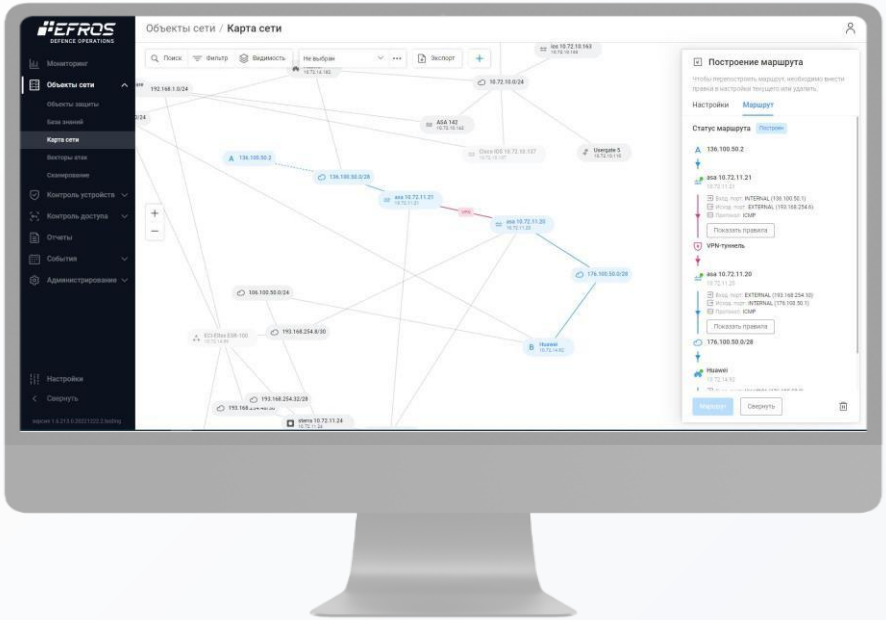
Импортозамещение:

ManageEngine Network Configuration Manager

SKYBOX Network Assurance

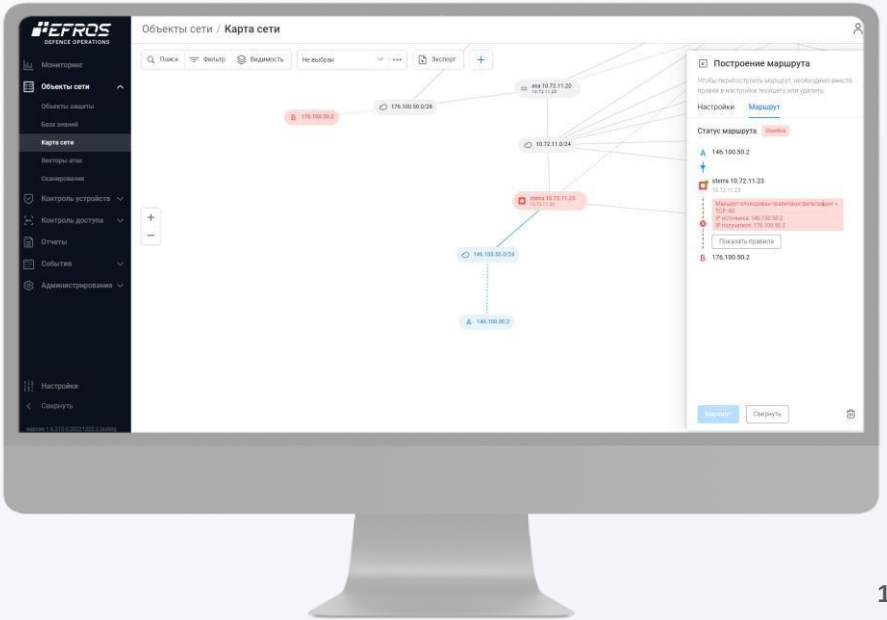
solarwinds Network Configuration Manager

АНАЛИЗ МАРШРУТА



Учитываем маршрутизацию, VPN, NAT

'24 VRF, MPLS



МОДУЛЬ АНАЛИЗА МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ

- 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

- 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

Проактивное управление уязвимостями, оценка реальной защищенности инфраструктуры.

Виртуализация и контейнеризация – победа над дефицитом IT инфраструктуры. Увеличение количества контейнеров как объектов защиты в корпоративной сети.

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.
- Оценка и приоритезация уязвимостей в соответствии с БД CVSS 4, EPSS, CISA KEV.
- Расчет возможных векторов атак с учетом модели нарушителя. Визуализация вектора на интерактивной карте.

Аналоги:

Qualys. tripwire positive technologies

МОДУЛЬ КОНТРОЛЯ ЦЕЛОСТНОСТИ

- Контроль целостности файлов ОС на базе Windows и Linux, SCADA-систем
- Контроль неизменности конфигураций СУБД, сред контейнеризации и виртуализации
- Compliance-проверки на соответствие стандартам безопасности
- Предоставление рекомендаций по внесению изменений для соответствия требованиям безопасности

Аналоги:

tripwire

positive technologies MaxPatrol HCC

Kaspersky Container Security

positive technologies PT CS

РАЗРАБОТКИ 2024

NA

Анализ изменения сети путем сравнения текущей модели с сохраненной на определенный момент времени моделью.

FA

Аудит просроченных правил, консолидация правил, **работа с объектами правил** (Cisco, Check Point, Fortinet).

CM

Создание новых типов заявок на добавление, удаление, изменение правил и объектов правил МЭ.

NAC

Реализация функций профилирования CDP/LLDP и **развитие возможностей EDO-агента.**

ICC

Расширение функциональных возможностей по **защите сред контейнеризации, увеличение библиотеки** коробочных compliance-проверок

МОДУЛЬ АУДИТА ПОТОКОВ ДАННЫХ В СЕТИ

MVP NFA

Efros DefOps
«Netflow Analyzer»

- Отслеживание пропускной способности сети и типовых паттернов трафика на уровне интерфейсов. Мониторинг производительности сетевого оборудования.
- Сопоставление сложных шаблонов и корреляция событий.
- Поддержка различных форматов NetFlow, sFlow, cflow, J-Flow , FNF, IPFIX, NetStream, Appflow.

Аналоги:

ManageEngine NetFlow Analyzer

Cisco Stealthwatch

EFROS
DEFENCE OPERATIONS

О НАС

8
Филиалов в РФ

Более **120** компаний пользователей Efros

Ежеквартальное обновление

20 лет
Разработки решений для рынка ИБ

4 уд
В соответствии с сертификацией ФСТЭК России

Программа обучения

Полностью импортонезависимое решение

24/7
Техподдержка

ПОДДЕРЖИВАЕМОЕ ОБОРУДОВАНИЕ

** Полный перечень на сайте ГИС и в технической документации*

Следующие шаги

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

ДЕМО ВЕРСИЯ

ПИЛОТНОЕ ВНЕДРЕНИЕ

РАСЧЕТ СПЕЦИФИКАЦИИ