Многофункциональный комплекс по защите ИТ-инфраструктуры: сетевых и конечных устройств, компонентов сред виртуализации и контейнеризации, системного и прикладного программного обеспечения.

EFROS

DEFENCE OPERATIONS

РЕШАЕТ КЛЮЧЕВЫЕ ЗАДАЧИ:

- Централизованное управление доступом в сеть и ведение журналов событий
- Анализ топологии сети, маршрутов, оптимизация правил брандмауэров
- Оценка рисков ИБ, связанных с эксплуатацией уязвимостей
- Профилактика атак как снаружи, так и изнутри периметра организации

EFROS
DEFENCE OPERATIONS

EDO-IK-1.09-05

Отдел продаж:
+7 (812) 677-20-53
sales@gaz-is.ru

GIS
ГАЗИНФОРМ СЕРВИС

Надежные решения для безопасности бизнеса

EFROS DEFENCE OPERATIONS

Модульная платформа Efros DefOps позволяет подобрать оптимальное решение для обеспечения информационной безопасности ИТ-инфраструктуры. Функциональные модули платформы обеспечивают:

- безопасный, необходимый и достаточный доступ в сеть и к оборудованию;
- контроль действий и изменений в инфраструктуре;
- оптимизацию правил межсетевых экранов;
- своевременное выявление возможных векторов атак;
- соответствие системы внутренним политикам и лучшим мировым практикам безопасных конфигураций.

Архитектура комплекса разработана с учетом требований к отказоустойчивости и производительности и позволяет использовать Efros DefOps на площадках с тысячами контролируемых объектов.

В структуру ПК EFROS Defence Operations входят следующие функциональные модули:

NETWORK ACCESS CONTROL (NAC)

Управление доступом в сеть

Модуль обеспечивает централизованный контроль доступа конечных сетевых устройств по протоколу RADIUS, а также доступ к активному сетевому оборудованию по протоколу TACACS+. Широкий спектр поддерживаемых методов аутентификации позволяет настроить контроль доступа для любого типа оборудования: от принтеров и ip-телефонов до устройств IoT и гостевых ноутбуков.

Модуль поддерживает создание порталов аутентификации для гостевых пользователей и персональных устройств (BYOD).

Предусмотрены механизмы профилирования и проверки состояния конечных устройств на соответствие политикам безопасности. В ходе проверки проводится сбор данных об установленной операционной системе, антивирусных приложениях и базах обновлений, процессах и подключенных USB - устройствах.

Детальное журналирование каждой сессии подключения позволяет оперативно выявлять и анализировать инциденты ИБ, а также оценить правильность настройки политики доступа в сеть.

Возможности защиты протокола DNS позволяют предотвращать незаметную передачу информации злоумышленниками, получение доступа к оборудованию и передачу команд вредоносному ПО. Это осуществляется благодаря заведению черных и белых списков доменов и IP-адресов, анализу запрашиваемых доменов по принадлежности к DGA, а также сигнатурному анализу IDS.

INTEGRITY CHECK COMPLIANCE (ICC)

Контроль целостности и проверки соответствия хостов и конечных точек

Функциональный модуль Integrity Check Compliance осуществляет контроль целостности файлов различных операционных систем (АРМ и серверов), гипервизоров, виртуальных машин и систем управления виртуализацией, серверов SCADA.

Модуль также проводит контроль неизменности конфигураций СУБД, контроль защищенности сред контейнеризации. Расширенные наборы политик безопасности, основанные на лучших мировых практиках, позволяют проводить проверки конечных точек на соответствие требованиям безопасности и рекомендовать изменения для соответствия стандартам безопасности.

FIREWALL ASSURANCE (FA) & CHANGE MANAGER (CM)

Оптимизация и анализ правил межсетевых экранов. Автоматизация процессов управления правилами

Модуль аудита правил МЭ позволяет автоматизировать отслеживание изменений и проверки безопасности. Осуществляет мониторинг неиспользуемых, избыточных и противоречивых правил.

Регулярная проверка соответствия правил доступа корпоративной политике предотвращает возникновение критичных нарушений в фильтрации трафика, таких как появление доступа в запрещенный сегмент сети или пропажа доступа к важным ресурсам, нарушение при взаимодействии бизнес приложений.

При создании стандартов безопасности, для анализа используется матрица взаимодействия зон друг к другу. Данный механизм аудита текущих правил экранирования упрощает настройку/создание новых правил.

Возможность автоматического управления изменениями списков доступа межсетевых экранов, реализуемая с помощью модуля Change Manager, делает процесс настройки и обновления более удобным и эффективным. Журналирование событий, связанных с изменениями доступа, позволяет просматривать информацию о причинах создания/изменения тех или иных правил, а также их исполнителях.

VULNERABILITY CONTROL

Анализ уязвимостей и построение векторов атак

Модуль Vulnerability Control позволяет проводить проверки инфраструктуры на наличие уязвимостей в режиме аудита. Проводится проверка уязвимостей для объекта с использованием информации из различных баз данных, включая БДУ ФСТЭК России; также в качестве источников информации могут подключаться сканеры и ITSM-системы.

Следующий шаг – визуализация возможных векторов атак на интерактивной карте. Выявление пути и способа, с помощью которого злоумышленник может проникнуть в целевую систему. В построении векторов атаки учитываются как возможные действия и инструменты злоумышленников извне, так и человеческий фактор или уязвимые технологии в контролируемой инфраструктуре.

Таким образом, в модуле Vulnerability Control реализован комплекс мер по выявлению уязвимостей, ассоциации их с активами, градация и приоритизация выявленных уязвимостей к устранению.

NETWORK ASSURANCE (NA)

Контроль конфигураций, моделирование, визуализация топологии сети, аудит уязвимостей

Функциональный модуль Efros DefOps NA предназначен для отслеживания изменений сетевой топологии и конфигураций активного сетевого оборудования. Ведется база данных эталонных конфигураций для быстрого восстановления состояния инфраструктуры после сбоев.

Используя интерактивную карту сети, администратор может анализировать связность и достижимость подсетей, выявлять маршруты распространения трафика. Моделирование в виртулизированной среде, в режиме изолированной программной среды позволяет анализировать возможные последствия изменений топологии.

Оценка защищенности сетевого оборудования осуществляется на основе данных из БДУ ФСТЭК, а также баз данных вендоров, содержащих описания в форматах CVE, OVAL и др. Для устранения выявленных уязвимостей предоставляются рекомендации экспертов.

Каждый функциональный модуль Efros DefOps отвечает за реализацию определенного набора функций и может приобретаться и работать отдельно.

Efros DefOps может применяться

- для защиты объектов критической информационной инфраструктуры;
- для работы с персональными данными;
- для защиты государственных информационных систем (не содержащих государственную тайну).

Сертификация ФСТЭК России по уровню доверия 4

Решение включено в реестр отечественного ПО №18615

НАМ ДОВЕРЯЮТ

госорганы · ТЭК · металлургия · финсектор · химия · туризм · машиностроение · и другие

ПОДДЕРЖИВАЕМЫЕ СИСТЕМЫ И ОБОРУДОВАНИЕ:

S-Terra	NME-RVPN, VPN Gate	**Astra Linux**	
Infotecs	VipNet Coordinator	**Alt Linux**	
«Фактор-ТС»	Dionis LX и NX	**«РЕД ОС»**	
«Код безопасности»	АПКШ «Континент»	**«Скала-Р»**	
Fortinet		**zVir**	
Huawei	Quidway	**UserGate**	
Check Point	SecurePlatform, Gaia, SmartCenter	**CISCO**	IOS, PIX, ASA, FWSM, WLC,
VMware	ESXI, vCenter	**ELTEX**	Eltex ESR, MES, WOP/WEP **и другие**
DOCKER		**Kubernetes**	