



ГАЗИНФОРМСЕРВИС

[www.gaz-is.ru](http://www.gaz-is.ru)

# «Швейцарский нож» для администраторов ИТ и «Всевидящее око» для сотрудников ИБ



# Современные ИТ-инфраструктуры



- ИТ-инфраструктуры огромных размеров
- ИТ-инфраструктуры быстро меняются и усложняются
- Компоненты ИТ-инфраструктур расположены в разных городах
- Управляющему персоналу ИТ-инфраструктур необходимо оперативно реагировать на инциденты ИБ

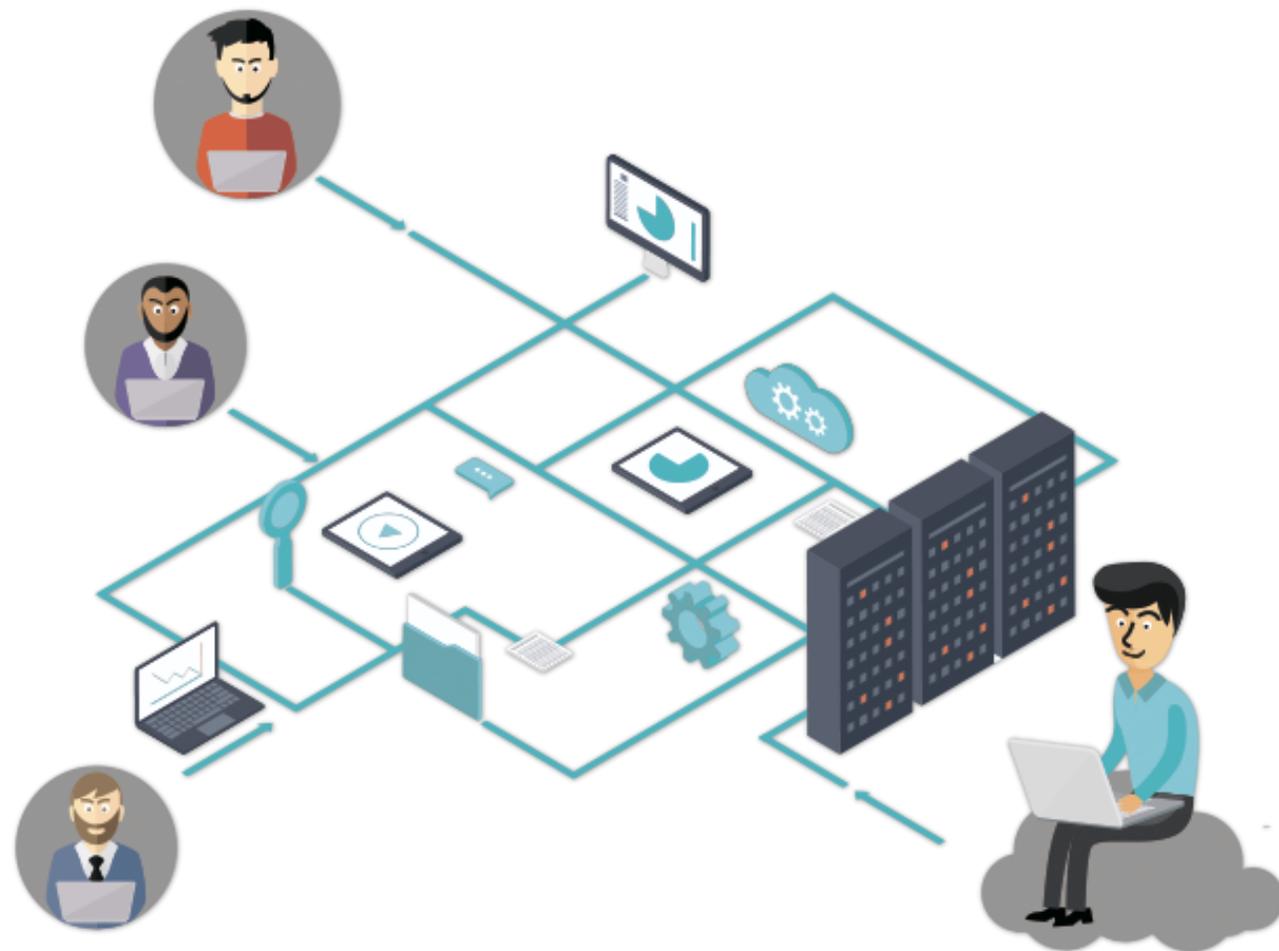
# Проблематика

Нарушение регламента проведения изменений

Длительное согласование изменений со стороны ИБ

Несвоевременное исправление выявленных уязвимостей

Проблемы проверки выполненных предписаний от ИБ в ИТ



# Решаемые задачи

ОТДЕЛ ИБ	ОТДЕЛ ИТ
Обнаружение уязвимостей ИТ-инфраструктуры	Инвентаризация объектов ИТ-инфраструктуры
Проверки соответствия отраслевым стандартам и аудит	Устранение уязвимостей объектов ИТ-инфраструктуры
Контроль целостности файлов серверных и десктопных операционных систем	Контроль обновлений, служб, пользователей серверных операционных систем
Контроль проведения запланированных изменений	
Контроль конфигураций сред виртуализации	
Контроль конфигураций и состояния рабочей среды сетевого оборудования	

# Решение

# EFFRDS

## Config Inspector

Повышение  
эффективности  
работы ИБ/ИТ

Оперативный и  
удобный аудит  
конфигураций

Автоматизация  
контроля  
целостности

Повышение  
уровня ИБ

# Функциональные возможности



Операционные  
системы



Сетевые  
устройства



Виртуальная  
среда



Контроль  
Active Directory

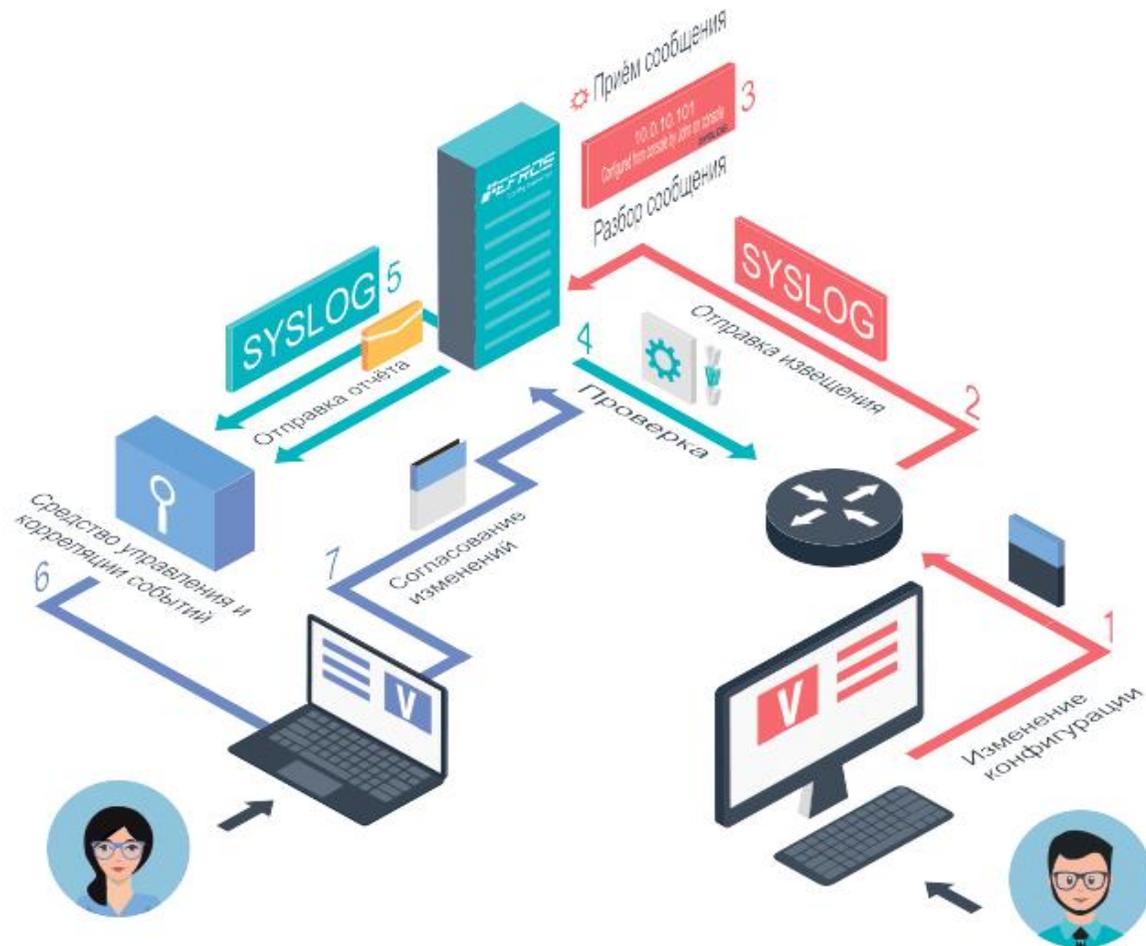


Проверка на  
уязвимости



Соответствие политикам  
безопасности

# Сценарий работы

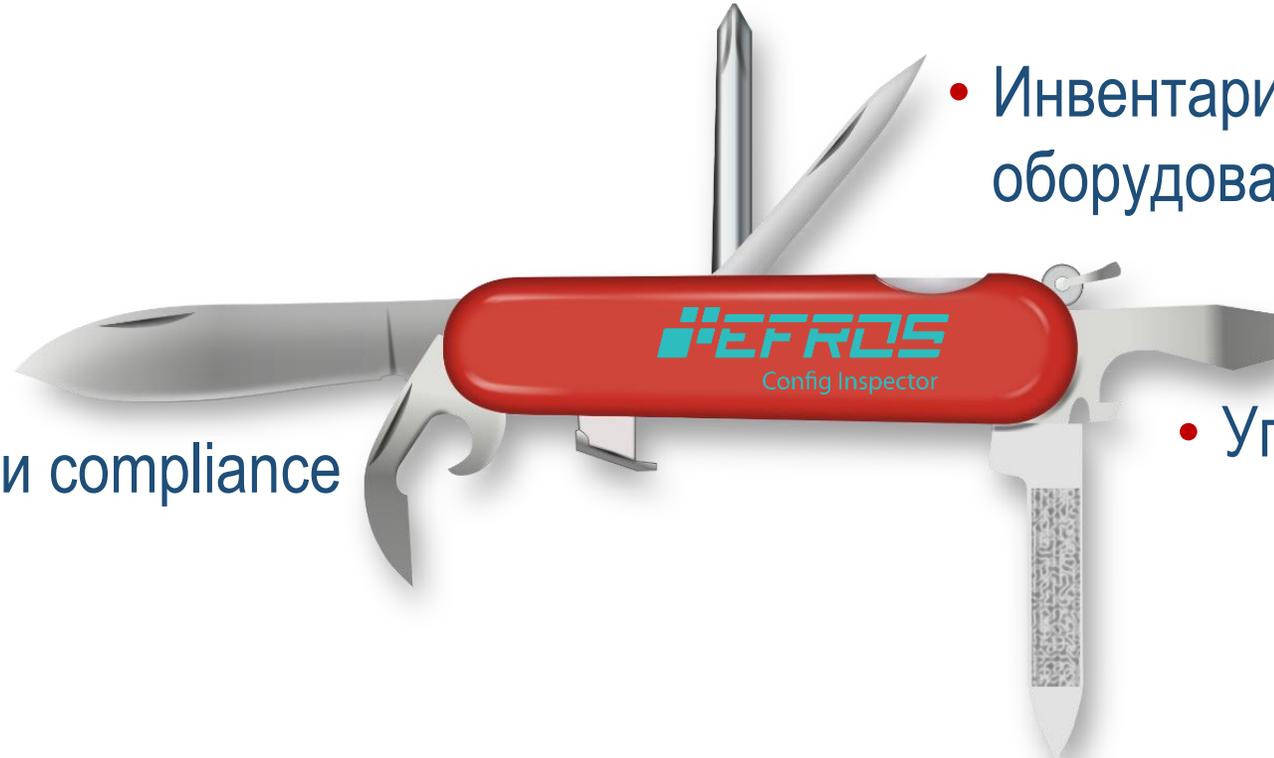


- Efos CI запускает проверки по расписанию, проводя полный анализ на соответствие заданным параметрам
- Efos CI принимает и анализирует syslog сообщения от устройств и по результатам анализа запускает проверку

# Швейцарский нож для IT

- Восстановление после сбоев

- Инвентаризация сетевого оборудования

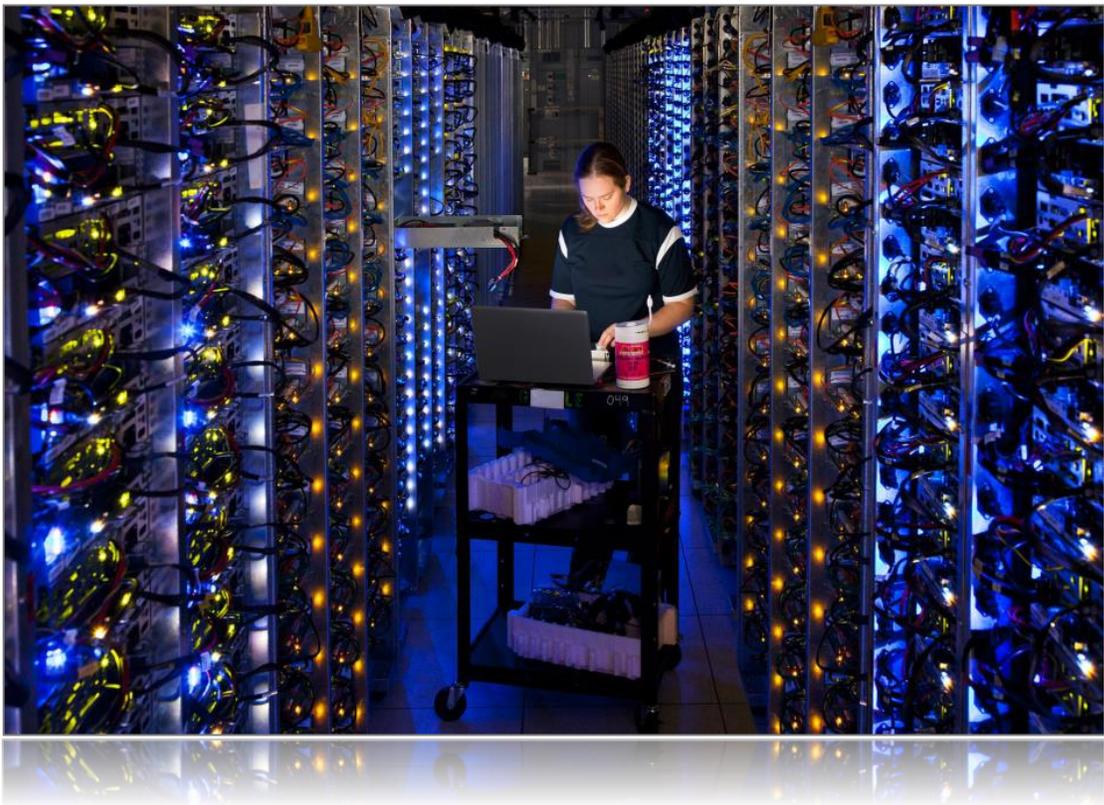


- Лучшие практики и compliance

- Управление изменениями

- Управление конфигурациями

# Выгоды для отдела ИТ



- Оперативная диагностика и восстановление после сбоев
- Автоматизированное ведение базы данных конфигураций
- Контроль проведения запланированных изменений
- Удобные механизмы поиска и сравнения

# «Всевидящее око ИБ»



- Контроль за изменениями конфигурационной информации
- Контроль соответствия проводимых изменений политике безопасности предприятия
- Контроль текущих конфигураций на наличие уязвимостей
- Организация ролевой модели доступа

# Выгоды для отдела ИБ



- Предотвращение несанкционированного изменения конфигурационной информации
- Контроль соответствия проводимых изменений политике безопасности предприятия
- Поиск уязвимостей в текущих конфигурациях
- Рекомендации по устранению уязвимостей

# Мониторинг изменений

Config Inspector 3.1.6

← → Мониторинг

root

Статус | Устройства | Уведомления

## КОНТРОЛЬ ИЗМЕНЕНИЙ



27 из 81  
отчетов с нарушениями

Статистика за месяц



## ПОСЛЕДНИЕ НАРУШЕНИЯ

Дата и время	Устройство	Тип нарушения
17.03.2017 15:14	ASA	Cisco ASA 'show version'
17.03.2017 15:16	Cisco ASA 10.72.10.119	Cisco ASA 'show version'
17.03.2017 15:19	CheckPoint R77.30	Check Point GAiA отсортированный 'show configuration'
17.03.2017 15:19	CheckPoint R77.30	Check Point GAiA 'ifconfig'
17.03.2017 15:20	CheckPoint R77.20	Check Point GAiA отсортированный 'show configuration'
17.03.2017 15:20	CheckPoint R77.20	Check Point GAiA 'ifconfig'
17.03.2017 15:21	windows 10.72.10.27	Журнал регистрации неуспешных попыток входа
17.03.2017 15:23	Cisco 10.127.255.252	Cisco IOS 'show version'
18.03.2017 3:21	vSphere	VMware vSphere Дерево иерархии
20.03.2017 9:16	CheckPoint SPLAT	Check Point SecurePlatform 'ifconfig'

## УЯЗВИМОСТИ

Категория	Количество
критичные	10
важные	1
информационные	0
без уязвимостей	1

## САМЫЕ УЯЗВИМЫЕ УСТРОЙСТВА

Устройство	Критично	Важно	Информация
10.72.10.187	21	19	5
ASA	13	13	0
Cisco ASA 10.72.10.119	13	13	0
Cisco 10.72.14.181	10	12	5
Cisco 10.72.14.181	10	12	5

## СОСТОЯНИЕ УСТРОЙСТВ



ВСЕГО УСТРОЙСТВ: 33  
● НЕТ СВЯЗИ 9  
● КРИТИЧНО 15  
● ВАЖНО 3  
● ИНФОРМАЦИЯ 0  
● БЕЗ УВЕДОМЛЕНИЙ 6

## ПРОВЕРКИ БЕЗОПАСНОСТИ



357 из 634  
выполнено правил

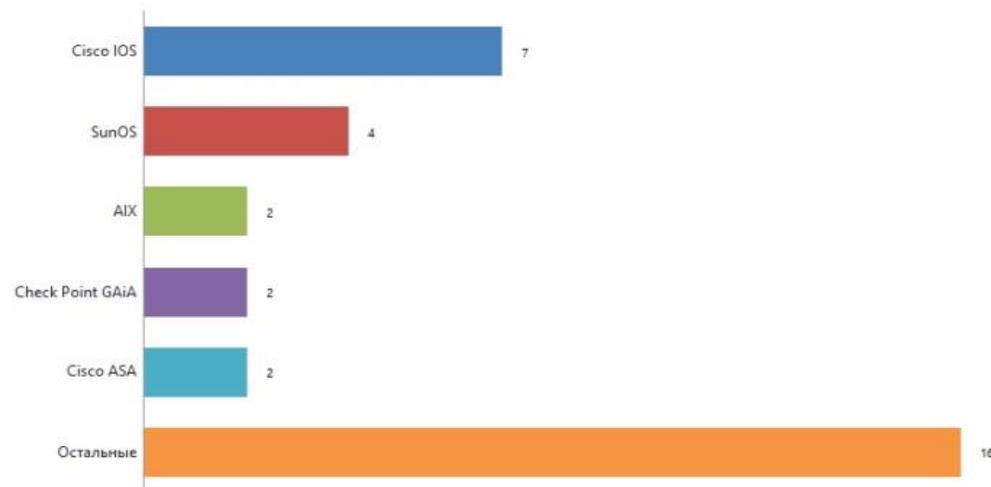
Статистика за месяц



## САМЫЕ НЕЗАЩИЩЕННЫЕ

Устройство	Процент незащищенности
S-Terra	18%
10.72.10.187	38%
Cisco 10.127.255.252	40%
Cisco 10.72.14.189	44%
Cisco 10.72.14.181	47%

## УСТРОЙСТВА



Мониторинг

Устройства

События

Настройки

# Пример сравнения конфигураций

Config Inspector 3.1.23

Устройства > Корневая группа > Сетевые устройства > Cisco > Cisco 2650

Администратор ИБ [Администратор]

Отчет Cisco IOS 'show running'

Устройство Cisco 2650

Исходный Эталон

Итоговый Текущий

Сравнение отчетов История изменений

Экспорт  Только отличия

Предыдущее Следующее

```
1 Building configuration...
2
3 Current configuration : 6708 bytes
4 !
5 version 12.1
6 no service pad
7 service tcp-keepalives-in
8 service tcp-keepalives-out
9 service timestamps debug datetime msec localtime show-timezone
10 service timestamps log datetime msec show-timezone
11 service password-encryption
12 !
13 hostname C2950
14 !
15 logging buffered 8096 debugging
16 logging console critical
17 no logging monitor
18 aaa new-model
19 aaa authentication login default local
20 aaa authorization exec default local
21 aaa authorization commands 14 default group tacacs+
22 aaa authorization commands 15 default group tacacs+ local
23 enable secret 5 $1$Qdz0$ZO4L5ZgMiVs1CrbeIqmSy.
24 enable password 7 06070B2C45400A1016141D
25 !
26 username admin privilege 15 password 7 06070B2C45400A1016141D
27 username admin1 privilege 15 password 7 14161606050A7B
28 username priv1 password 7 03235A11161D2E411E50
29 username kkk
30 username hacker
31 username 111
32 username red password 7 0134071E4B19090271150E
33 username redcheck privilege 15 password 7 08064D54190B0A1A4252
34 username 999
35 clock timezone MSK 3
36 ip subnet-zero
37 !
38 ip dhcp snooping vlan 1
39 ip domain-name ois
```

```
1 Building configuration...
2
3 Current configuration : 6722 bytes
4 !
5 version 12.1
6 no service pad
7 service tcp-keepalives-in
8 service tcp-keepalives-out
9 service timestamps debug datetime msec localtime show-timezone
10 service timestamps log datetime msec show-timezone
11 service password-encryption
12 !
13 hostname C2950
14 !
15 logging buffered 8096 debugging
16 logging console critical
17 no logging monitor
18 aaa new-model
19 aaa authentication login default local
20 aaa authorization exec default local
21 aaa authorization commands 14 default group tacacs+
22 aaa authorization commands 15 default group tacacs+ local
23 enable secret 5 $1$Qdz0$ZO4L5ZgMiVs1CrbeIqmSy.
24 enable password 7 06070B2C45400A1016141D
25 !
26 username admin privilege 15 password 7 06070B2C45400A1016141D
27 username admin1 privilege 15 password 7 14161606050A7B
28 username priv1 password 7 03235A11161D2E411E50
29 username kkk
30 username hacker
31 username 111
32 username red password 7 0134071E4B19090271150E
33 username redcheck privilege 15 password 7 08064D54190B0A1A4252
34 username 999
35 username Petr
36 clock timezone MSK 3
37 ip subnet-zero
38 !
39 ip dhcp snooping vlan 1
40 ip domain-name ois
```

# Уведомления на электронную почту



Входящие - efros@gis.demo - Microsoft Outlook (безопасный режим)

Файл Главная Отправка и получение Папка Вид Что вы хотите сделать?

Изменить представление, Настройка представления, Восстановить представление по умолчанию

Показывать как беседы, Параметры беседы

Просмотр сообщения

Дата (беседы), Категории, От, Кому, Пометка: дата начала, Пометка: дата выполнения

Обратный порядок сортировки, Добавить столбцы, Развернуть или свернуть

Область папок, Область чтения, Список дел, Макет

- Избранное
- Входящие
- Отправленные
- Черновики
- efros@gis.demo
- Входящие
- Черновики
- Отправленные
- Удаленные
- RSS-каналы
- Исходящие
- Нежелательная почта
- Папки поиска

Поиск в папке "из текущего почтового ящика"

Дата Предмет

Все Непрочитанные Новые

Сегодня

admin@mail.demo	Cisco 2650, Отчет "Cisco IOS 'sh... Отчет "Cisco IOS 'show version'"	9:45
admin@mail.demo	Cisco 2650, Отчет "Cisco IOS 'sh... Отчет "Cisco IOS 'show version'"	9:40
admin@mail.demo	Cisco 2650, Отчет "Cisco IOS ru... Отчет "Cisco IOS running-startup	9:40
admin@mail.demo	Cisco 2650, Отчет "Cisco IOS Раз... Отчет "Cisco IOS Разница	9:40

Ответить Ответить всем Переслать

admin@mail.demo EFROS

Cisco 2650, Отчет "Cisco IOS running-startup difference" изменен и помещен в архив. Уведомления на почту

Отчет "Cisco IOS running-startup difference" изменен и помещен в архив

## Сводка события

Устройство: Cisco 2650 [открыть в консоли](#)  
Размещение: Сетевые устройства\Cisco  
Профиль: Сетевые устройства Cisco  
Время: 05.04.2018 09:39:57  
Триггер: Уведомления на почту  
Тип события: Изменение отчета

Отчет "Cisco IOS running-startup difference" изменен и помещен в архив.

## Изменения:

4 -username Petr

## Детали события

Тип отчета: Cisco IOS running-startup difference  
Оповещение при изменении: Нет  
Контроль целостности: Отключен

Все значения времени указаны в следующем часовом поясе: (UTC+03:00) Russian Standard Time

Сообщение отправлено [Efros@ Config Inspector](#)

# Карта контролируемых устройств

Config Inspector 3.1.5

Настройки

Мониторинг

Устройства

События

Настройки

```
graph TD; ESXi[ESXi] --> ESXi_1072452[vm ESXi 10.72.4.52]; ESXi --> ESXi_1072451[vm ESXi 10.72.4.51]; MПУР[MПУР] --> ESXi; Linux[Linux] --> Solaris_1010812[Solaris 10.10.8.12]; Linux --> Solaris_101086[Solaris 10.10.8.6]; Linux --> Solaris_101085[Solaris 10.10.8.5]; Linux --> AIX_10101136[AIX AIX 10.10.1.136]; Linux --> AIX_10101134[AIX AIX 10.10.1.134]; Suse[Suse 10.72.10.132] --> MПУР; Ядро_сети[Ядро сети] --> Cisco_10127255251[Cisco 10.127.255.251]; Ядро_сети --> Cisco_10127255252[Cisco 10.127.255.252]; Main_devices[Main_devices] --> MПУР; Main_devices --> Cisco_107214181[Cisco 10.72.14.181]; Main_devices --> Cisco_уязвимости[Cisco - уязвимости]; Main_devices --> WLC[WLC]; Cisco_уязвимости --> Cisco_107214181; Cisco_уязвимости --> WLC;
```

GroupDev

Перейти Загрузить все

**Cisco 2650**  
10.72.14.189

● Устройство доступно

модель, версия  
WS-C2950-24, 12.1(22)EA13

профиль  
Сетевые устройства Cisco

Защищенность  49%

Уязвимости ! 0 ! 11 i 3

Контроль изменений  
0 нарушений

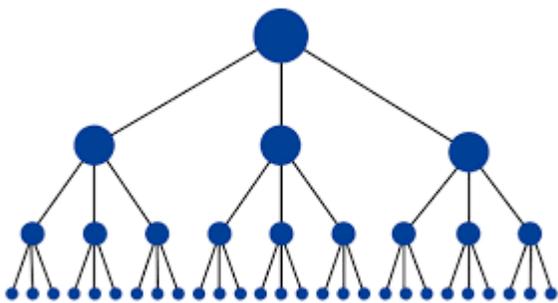
Уведомления ! 1

# ГЕТЕРОГЕННАЯ ИТ-ИНФРАСТРУКТУРА

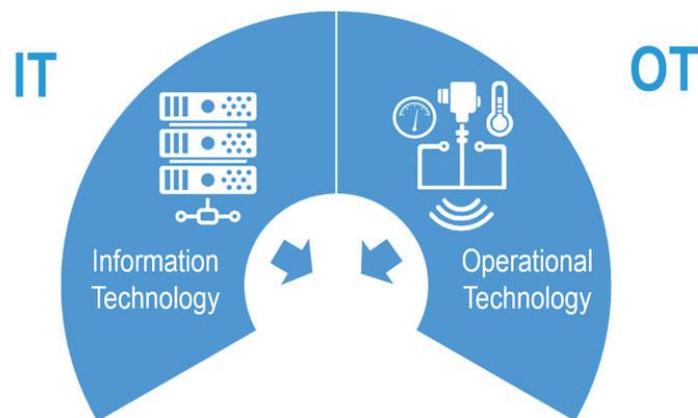
	IOS, PIX, ASA, FWSM, WLC, CatOS, AsyncOS, UCM		ISCOM
	SecurePlatform, Gaia, SmartCenter		JetNet
	Comware Switch, Virtual Connect		Zynos
	ESXI, vCenter		QSW
	NME-RVPN, VPN Gate		DES
	RSOS9000, RS7750, RSOA700		Quidway
	Unix/Linux, Windows		Dionis LX и NX
	Eltex ESR, MES, WOP/WEP		JUNOS
	3Com OS		Active Directory
	XOS v.9		EDS
	Арлан, Инзер		PanOS
	XenServer		VipNet Coordinator



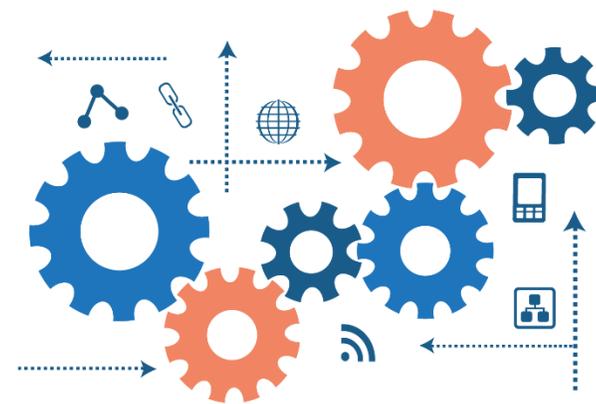
# РАЗВИТИЕ ПРОДУКТА



**РАЗВИТИЕ ИЕРАРХИЧНОЙ  
АРХИТЕКТУРЫ ПРОДУКТА**



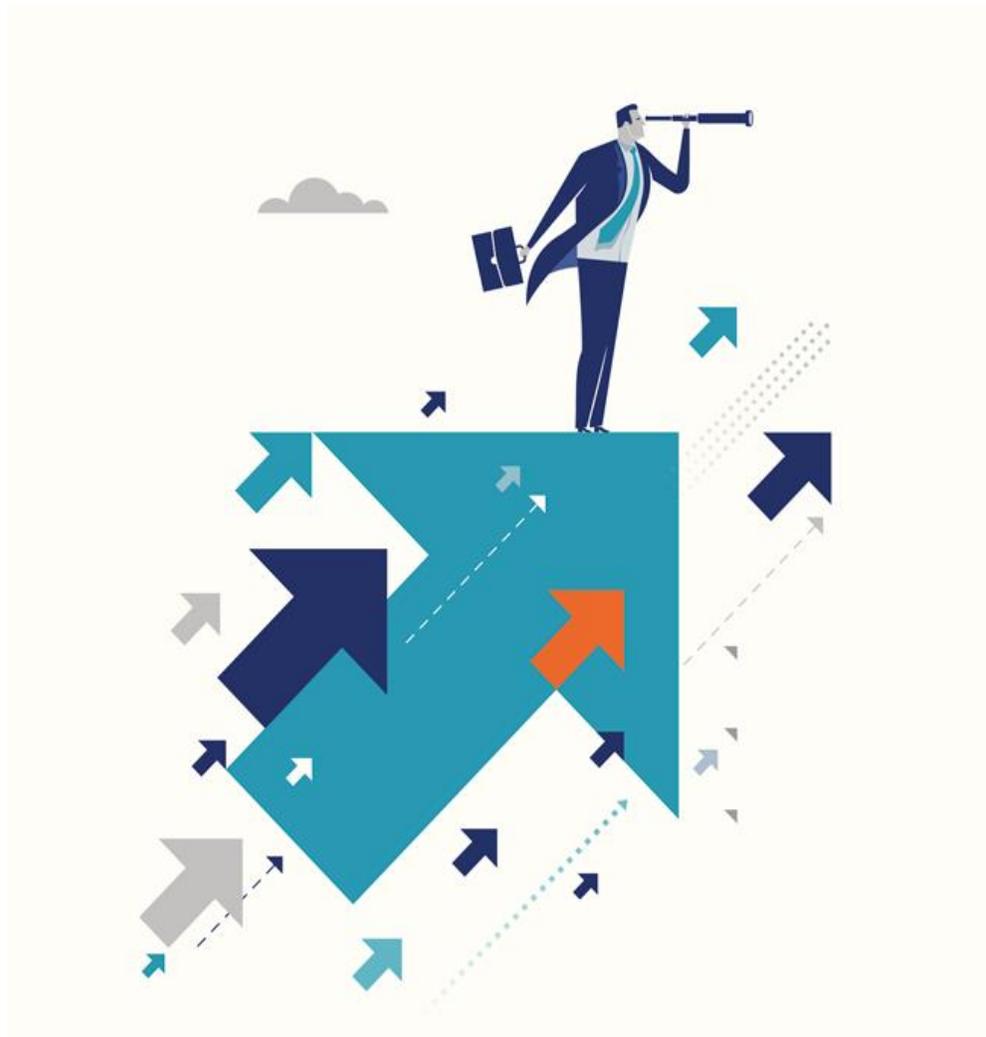
**ИНФОРМАЦИОННАЯ  
БЕЗОПАСНОСТЬ АСУ ТП**



**ИНТЕГРАЦИЯ С СИСТЕМАМИ  
ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ**



# ДЕЙСТВУЙТЕ



- ✓ Скачать демо-версию и попробовать все возможности в течении 90 дней.

[www.gaz-is.ru](http://www.gaz-is.ru)

- ✓ Оформить запрос на проведение пилотного решения.
- ✓ Запросить коммерческое предложение.



Менеджер по развитию бизнеса

**Штубов Никита Александрович**

Тел: +7 (812) 677-20-50, доб. 1662

Моб: 8-981-844-60-86