

# INFRARED

BY ALPHA SYSTEMS

Reliable IT infrastructure management



# 1

## НЕУЧТЕННЫЕ АКТИВЫ И СЕРВИСЫ В ИТ-ИНФРАСТРУКТУРЕ

Встречаются в 90% компаний. Является причиной 43% инсайд атак.

# 2

## ОТСУТСТВИЕ УПРАВЛЕНИЯ КОНФИГУРАЦИЯМИ И СВЯЗЯМИ ИТ-АКТИВОВ

Более чем в 87% компаний не знают о зависимостях бизнес сервисов и ИТ-Активов.

# 3

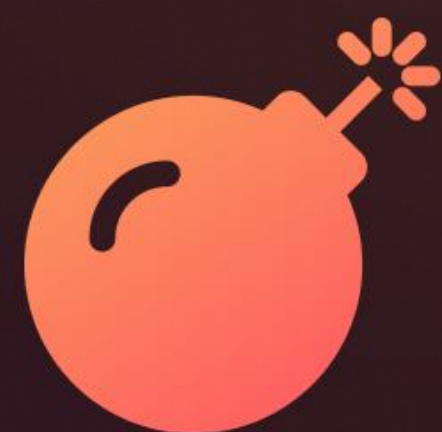
## ОТСУТСТВИЕ РЕГУЛЯРНОГО АНАЛИЗА КОНФИГУРАЦИЙ ИТ-АКТИВОВ

С 2022 года, атаки через ошибки в настройках выросли на 51%.

# 4

## ВЫСОКАЯ СКОРОСТЬ ИЗМЕНЕНИЙ ИТ ЛАНДШАФТА В КОМПАНИЯХ

В развивающихся компаниях ИТ ландшафт меняется более чем на 10% за 1 месяц.



## УМЫШЛЕННОЕ ПОВРЕЖДЕНИЕ КОНФИГУРАЦИЙ

Несанкционированные модификации или вредительские действия. Ущерб оценивается в диапазоне от 5 до 129 млн рублей за инцидент.



## «ДЫРЫ» В ПРАВИЛАХ МЕЖСЕТЕВЫХ ЭКРАНОВ

Ошибки в правилах МСЭ позволили в 2022 году атаковать более чем 21% периметровых средств защиты.



## ЗАБЫТЫЕ ИТ-АКТИВЫ, КОТОРЫЕ НЕ ВЫВЕЛИ ИЗ ЭКСПЛУАТАЦИИ

Угроза атаки и/или заражения ИТ инфраструктуры. Стоимость потерь от 1 – 10 млн руб за инцидент.



## ОШИБКИ В КОНФИГУРАЦИЯХ

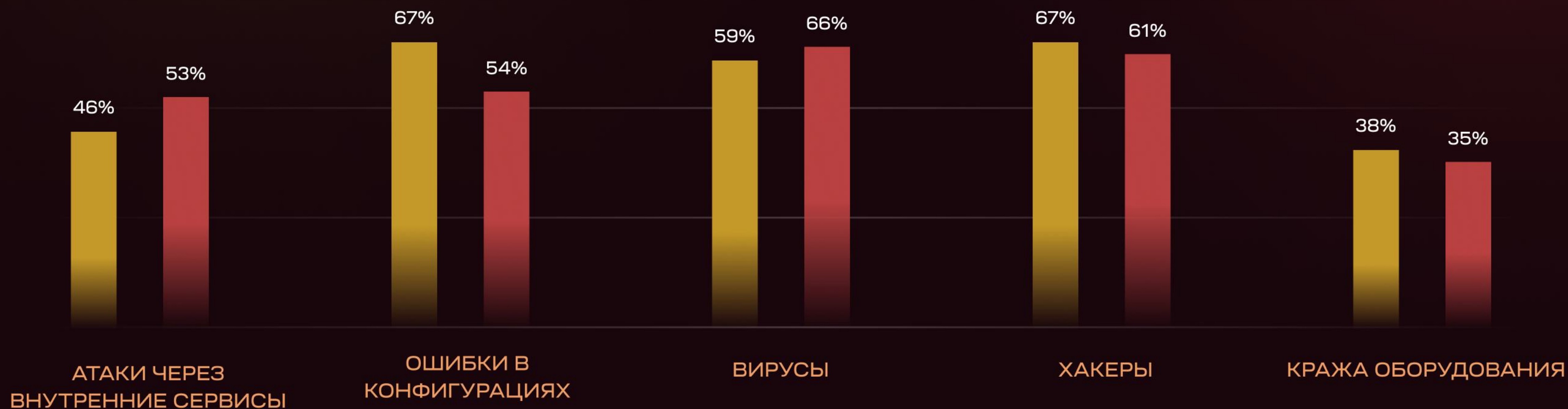
Уязвимости в конфигурациях информационных систем являются главным (составляющим 78%) источником аварийных ситуаций.

# ТОП ВНУТРЕННИХ ИНЦИДЕНТОВ

ALPHASYSTEMS.GROUP

8-800-505-64-54

■ 2022 ■ 2023



# INFRARED

## МУЛЬТИ СЕРВИСНОЕ РЕШЕНИЕ ДЛЯ УПРАВЛЕНИЯ, УЧЕТА И АНАЛИЗА, ИТ-АКТИВОВ И КОНФИГУРАЦИЙ

Система управления конфигурациями представляет из себя систему сбора и учета конфигураций активов ИТ-инфраструктуры. Помимо конфигураций хранятся и собираются метаданные, на основе которых в дальнейшем может быть сформирована карточка сервиса.



Решение класса Assets Auditor

# ЭФФЕКТИВНЫЕ МЕТОДЫ INFRARED

ALPHASYSTEMS.GROUP

8-800-505-64-54



## DISCOVERING

Адаптивное обнаружение и классификация



## VISUALIZATION

Построение схем и связей



## SCAN

Сканирование и сравнение



## REPORT

Конструктор отчетов

UNIX

FORTINET



Linux



MikroTik

vmware

aruba

MOTOROLA

Windows



HUAWEI

CISCO

D-Link



05

06

07

## 01

### МАКСИМАЛЬНЫЙ УРОВЕНЬ ИНВЕНТАРИЗАЦИИ ИТ-АКТИВОВ

- Агентские и безагентские методы сбора данных
- Регулярные автоматизированные аудиты и обновления данных
- Классификация ИТ-активов по уровню критичностью и ценности
- Определение приоритетности управления ИТ-активами

## 02

### АВТОМАТИЗИРОВАННОЕ ОБНАРУЖЕНИЕ УЯЗВИМОСТЕЙ НА СЕТЕВОМ УРОВНЕ

- Проверка и улучшение конфигураций ИТ-активов
- Обнаружение уязвимостей и ошибок в ОС, СУБД и сетевом оборудовании
- Автоматизированные рекомендации по устранению обнаруженных уязвимостей

## 03

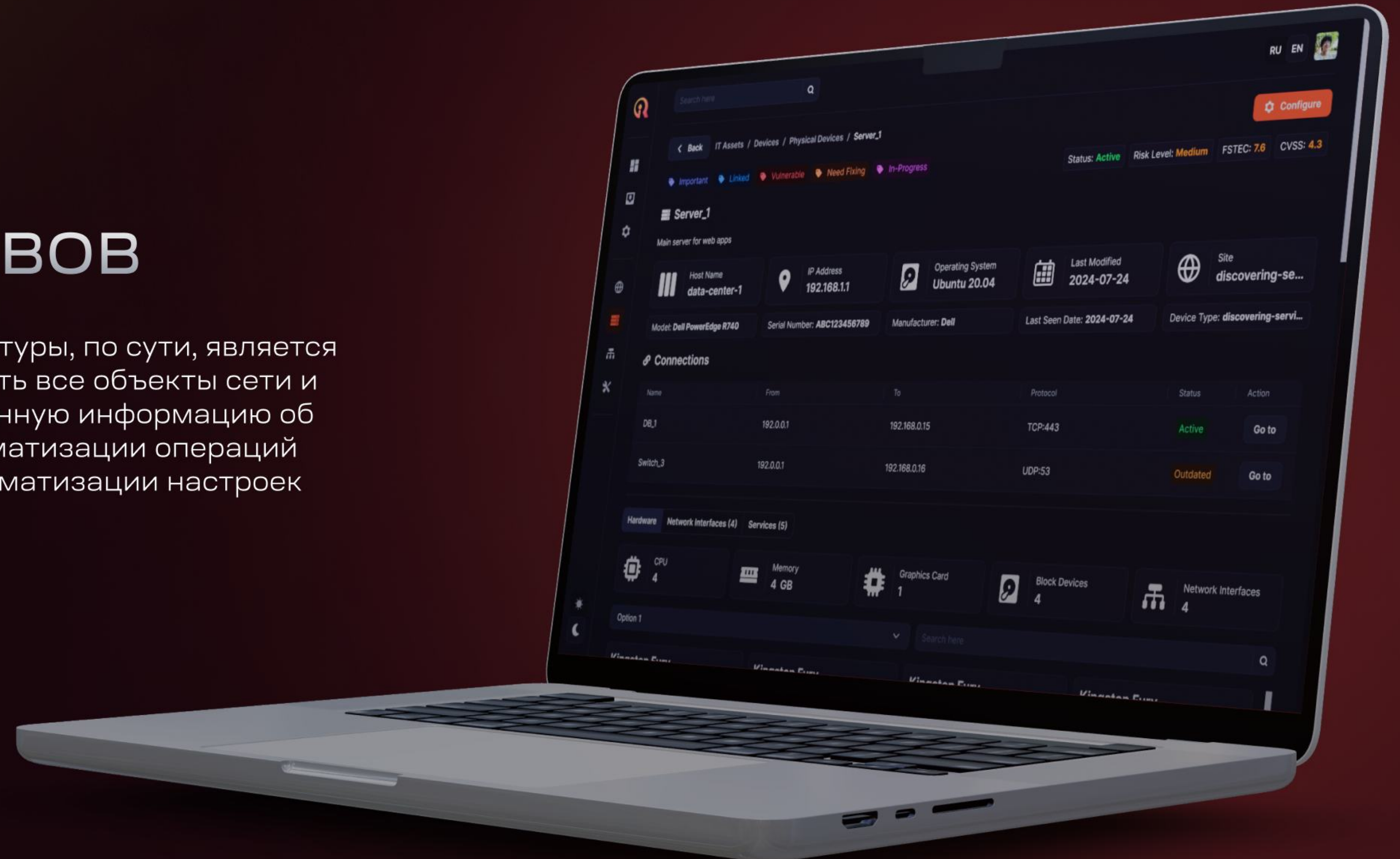
### ОПТИМИЗАЦИЯ РАЗВЕРТЫВАНИЯ ИТ-ИНФРАСТРУКТУРЫ

- InfraRed - центральный репозиторий конфигураций
- Интеграция с ведущими инструментами автоматизации (Ansible, Terraform, др.)
- InfraRed позволяет развернуть промышленную ИТ-инфраструктуру всего за 10-15 минут



# ОБНАРУЖЕНИЕ И УЧЕТ ИТ-АКТИВОВ

Система учета активов ИТ-инфраструктуры, по сути, является базой данных, где можно смоделировать все объекты сети и хранить всю информацию о них. Собранную информацию об активах можно использовать для автоматизации операций развертывания инфраструктуры и автоматизации настроек сети.







# СБОР И АУДИТ КОНФИГУРАЦИЙ ОПЕРАЦИОННЫХ СИСТЕМ И СУБД

Учет и анализ конфигурационных единиц позволит оперативно получать информацию о валидности конфигурации ИТ-актива, а также вести централизованный репозиторий конфигураций, для средств автоматизации развертывания инфраструктуры.

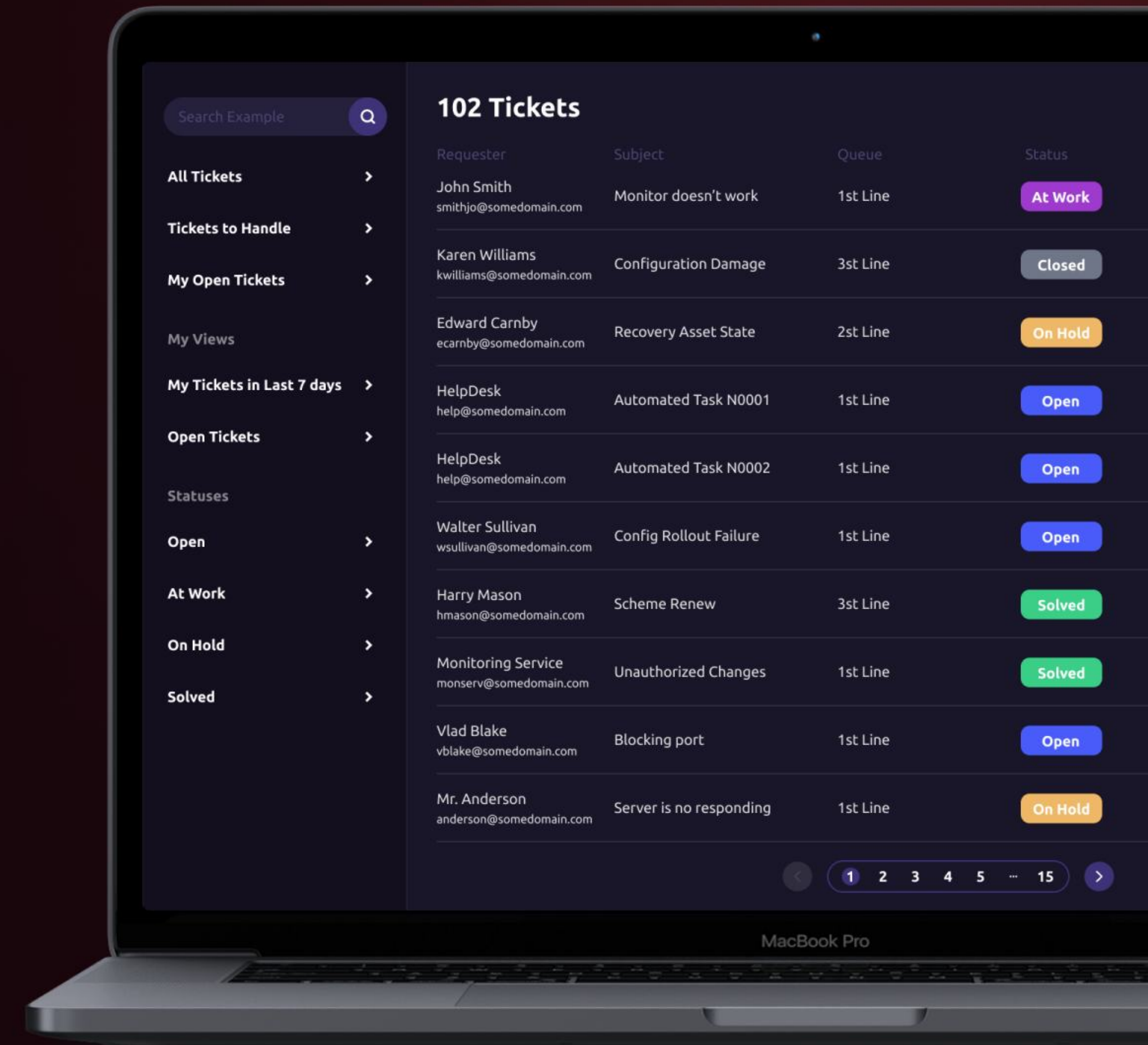




# ИНТЕГРАЦИЯ С ТИКЕТ СИСТЕМАМИ

Полнота учета ИТ-активов делает InfraRed одним из основных источников мониторинга состояния соответствия и защищенности ИТ-инфраструктуры.

- Настройка интеграций для управления ИТ-активами через тикет-системы
- Автоматизация процесса создания → закрытия замечаний





# АВТОМАТИЧЕСКИЕ ОБНОВЛЕНИЯ КОМПОНЕНТОВ И ВЕРСИЙ ПРОДУКТА

Система обновления компонентов и версий продукта, позволяет осуществлять поставку новых функций «на лету», без переустановки и дополнительных настроек.

Пока вы пользуетесь существующими возможностями, в InfraRed появляются новые.





# ОТЧЁТЫ ОБ УЯЗВИМОСТЯХ И КОНФИГУРАЦИЯХ

InfraRed формирует базу знаний об ИТ-активах и конфигурациях. Отчеты информационной безопасности с обнаруженными замечаниями могут быть оперативно переданы в профильное подразделение автоматически, для проведения работ по устранению уязвимостей.

Данный подход позволяет обеспечивать высокий уровень соответствия и защищенности инфраструктуры, легко вводить и выводить из эксплуатации узлы и компоненты информационных систем, а также быстро подключать к обслуживанию инфраструктуры новых специалистов.

The screenshot shows a report titled "Configuration Audit Report - alphasystems.group". It includes metadata such as start and end times, scan type, benchmark ID, and URL. It lists IP addresses (IPv4 and IPv6) and MAC address. The CPE platform is identified as "cpe:/o:debian:debian\_linux:12". Chained audits are listed as "1. alphasense.a-s.group" and "2. test.audit.a-s.group". The audit summary shows 107 Not Matched, 26 Matched, and 107 Unavailable. The score is 42.08% / 100%. The host misconfigurations brief for 192.188.1.168 shows 2 High, 10 Medium, 5 Low, and 20 Info issues.

**Report** HTML Version

### Configuration Audit Report - alphasystems.group

Start time: 16 May 2024 at 12:41  
End time: 17 May 2024 at 10:01  
Scan Type: Auto  
Benchmark ID: xccdf\_org.ssgproject.content\_benchmark\_DEBIAN-12  
Benchmark URL: /usr/share/xml/scap/ssg/content/ssg-debian12-xccdf.xml  
Benchmark version: 0.1.71

**Addressess**

IPv4: 127.0.0.1; 192.168.1.49  
IPv6: 0:0:0:0:0:0:1; fe80:0:0:0:c97e:6058:2c78:ed15  
MAC: 00:00:00:00:00:00; 08:00:27:3B:62:40

**CPE Platforms**

cpe:/o:debian:debian\_linux:12

**Chained Audits:**

1. alphasense.a-s.group
2. test.audit.a-s.group

**Audit Summary: 256**

- 107 Not Matched
- 26 Matched
- 107 Unavailable

**Score:**

42.08% / 100%

**Host Misconfigurations Brief - 192.188.1.168**

- 2 High
- 10 Medium
- 5 Low
- 20 Info

**Audit Overview**

### Q4 2024

- Расширение возможностей по аудиту конфигураций (Docker, K8S, сетевое оборудование)
- Сбор и версионирование конфигураций
- Модульные отчеты

### Q1 2025

- Автоматизация работы с патчами и рекомендациями
- Аудит баз данных
- Расширенные возможности уведомлений (Telegram, вебхуки)
- Выгрузка отчетов (CSV, JSON)

### Q2 2025

- Конструктор отчетов
- Интеграции с тикет-системами
- Аудит МСЭ

## НАМ ДОВЕРЯЮТ



ВАОН

ТРИНФИКО

BIDZAAR

ЕАПТЕКА



## НАШИ ПАРТНЁРЫ



GROUP-IB

R-Vision



МГУ

SEARCHINFORM  
INFORMATION SECURITY



uncom

ANGARA  
SECURITY

КРОСС  
ТЕХНОЛОДЖИС

UserGate

КОД  
безопасности

Ангара  
lab

RUSIEM

IT TASK  
системный интегратор

FORTIS



# КОМАНДА

ALPHASYSTEMS.GROUP

8-800-505-64-54

КОМАНДА ALPHA SYSTEMS СОСТОИТ ИЗ ЭКСПЕРТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ОБЪЕДИНЕННЫХ ОБЩИМ ВИДЕНИЕМ И ЦЕЛЯМИ

## EXPERIENCE

Более 10 лет работы в кибербезопасности

## MISSION

Делаем компьютерные технологии более простыми и надежными для бизнеса

## PRODUCTS

Инновационные подходы и простота реализации



# КИБЕРБЕЗОПАСНОСТЬ С ALPHA SYSTEMS

ALPHASYSTEMS.GROUP

8-800-505-64-54

Alpha Systems - активно развивающаяся российская инновационная компания в сфере информационной и кибербезопасности. Эксперты компании обладают самым передовыми знаниями и незаменимым опытом, которые способствуют созданию безопасной цифровой среды для бизнеса.

КОНСАЛТИНГ

ВНЕДРЕНИЕ

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА



## ПРОДУКТОВЫЙ ПОРТФЕЛЬ:

### AlphaSense

Комплексное автоматизированное решение для поиска и дальнейшей эксплуатации известных уязвимостей.

### Symbiote

Связующий элемент для решений, анализа и поддержания высокого уровня защищённости информации компании

### InfraRed

Мульти сервисное решение для управления и анализа конфигураций, учета активов ИТ инфраструктуры.



# КОНТАКТЫ



**ALPHASYSTEMS.GROUP**



**8-800-505-64-54**

**Агаев Р. Г.**



**+7-915-318-12-99**



**ra@alphasystems.group**

**Смирнов И. В.**



**+7-905-575-33-22**



**ismirnov@alphasystems.group**