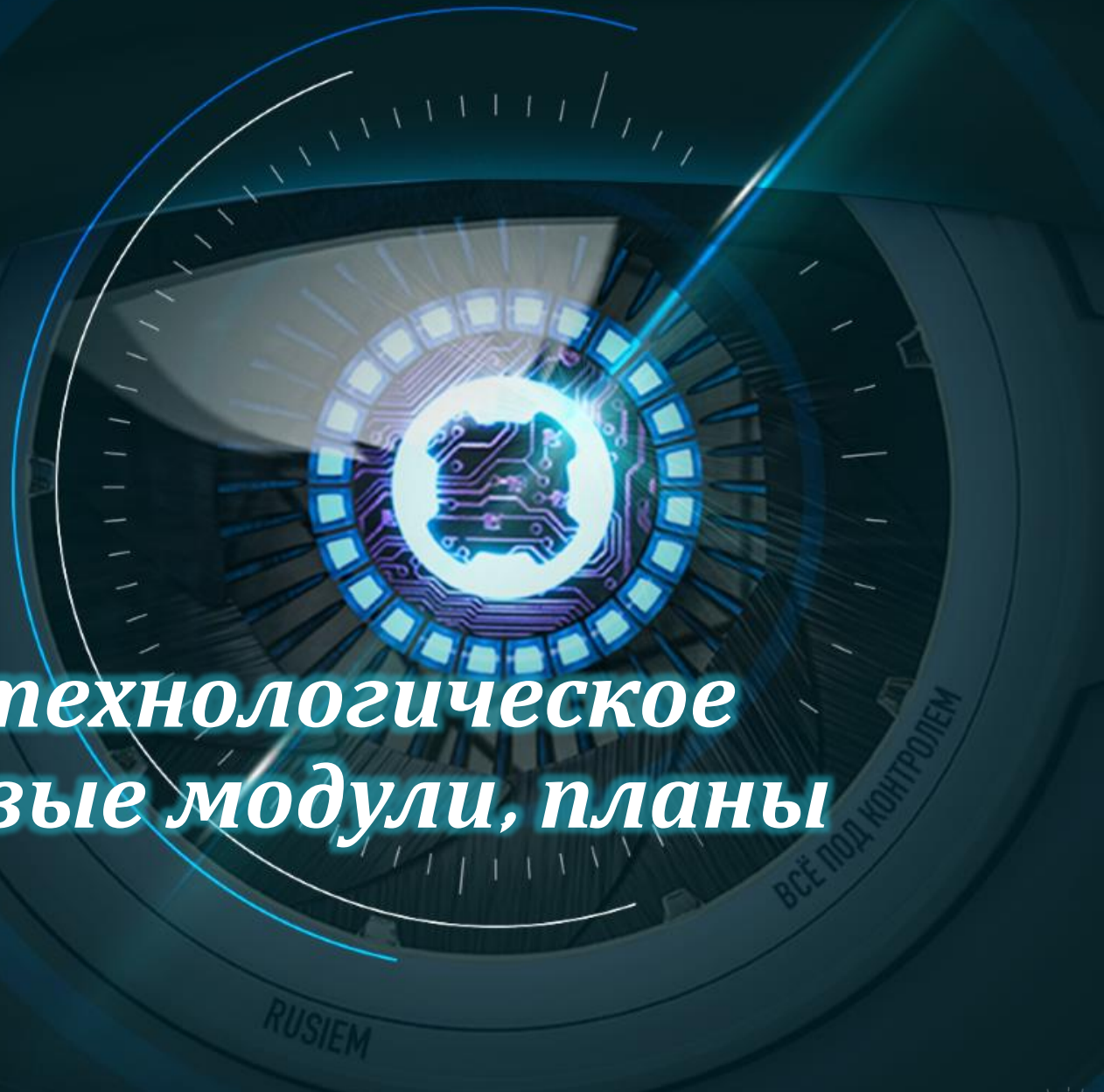
RUSIEM
Всё под контролем




# SIEM-система RuSIEM: технологическое развитие решения, новые модули, планы на 2023 год

***Дмитрий Чеботарев,***
***руководитель отдела предпродажной подготовки***

# RuSIEM – это

Полностью российская разработка (с 2014 года)

Резидент Сколково

> 450

Партнеров в России и странах СНГ

Продукт включен в Единый реестр отечественного ПО

Продукт имеет сертификаты ФСТЭК России (4 УД), ОАЦ (Беларусь)

RUSIEM
Всё под контролем

# Какие задачи решает SIEM

- Оперативное обнаружение, реагирование и контроль обработки инцидентов
- Оперативный контроль состояния инфраструктуры компании
- Создание единого центра мониторинга
- Определение прав, обязанностей и разграничение зон ответственности персонала компании (ИТ- и ИБ-служб)
- Соответствие требованиям регуляторов
  (Федеральные законы № 152-ФЗ, 161-ФЗ, 187-ФЗ, приказы ФСТЭК России № 21, 17 и 31, СТО БР ИББС и РС БР ИББС-2.5-2014, международного стандарта PCI DSS, ISO 27001)

# Соответствие требованиям

**ФЗ РФ**
**от 27 июля 2006 г.**
**№ 152-ФЗ**
«О персональных данных»

**ГОСТ Р 57580.1-2017**
«Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»

**ФЗ РФ**
**от 26 июля 2017 г.**
**№ 187-ФЗ**
«О безопасности критической информационной инфраструктуры РФ»

**ISO/IEC 27001**
«Системы менеджмента информационной безопасности. Требования»

**ГОСТ Р 57580.2-2018**
«Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия»

# Внедрение SIEM


- Access Control, Authentication
- DLP-системы
- IDS/IPS-системы
- Антивирусные приложения

- Журналы событий серверов и рабочих станций
- Межсетевые экраны
- Сетевое активное оборудование
- Сканеры уязвимостей

- Система инвентаризации и asset-management (а у некоторых СИЕМ есть даже свой внутренний функционал работы с активами)
- Система веб-фильтрации

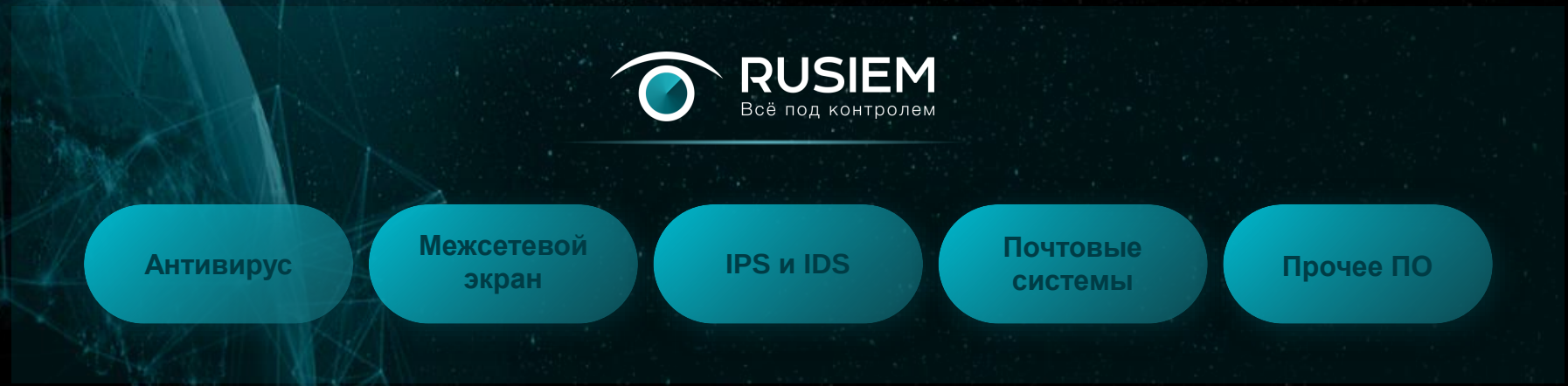
# RuSIEM – это

**Более 350** источников событий «из коробки»

Более **400** правил корреляции **для анализа событий**

**75** Предустановленных шаблонов **отчетов**

**Собственная технология анализа событий**, основанная на лучших практиках и собранном опыте



# Особенности RuSIEM


Интеграция с ГосСОПКА и сертификация ФСТЭК России

RuSIEM MQ – очередь

Приведенная к общем формату объектная нормализация

Встроенная управляемая и редактируемая корреляция

Высокая производительность (Свыше 90000 событий на одну ноду)

Нет ограничений по количеству событий и источников

Вертикальная масштабируемость

Горизонтальная масштабируемость

Разделение нагрузки на несколько серверов или виртуальных машин

Наличие собственных модульных агентов

Real-time и историческая корреляция

Коннекторы от производителя

Нет ограничений по размеру архивного хранилища

Сохранение исходных RAW-событий

# Лицензирование

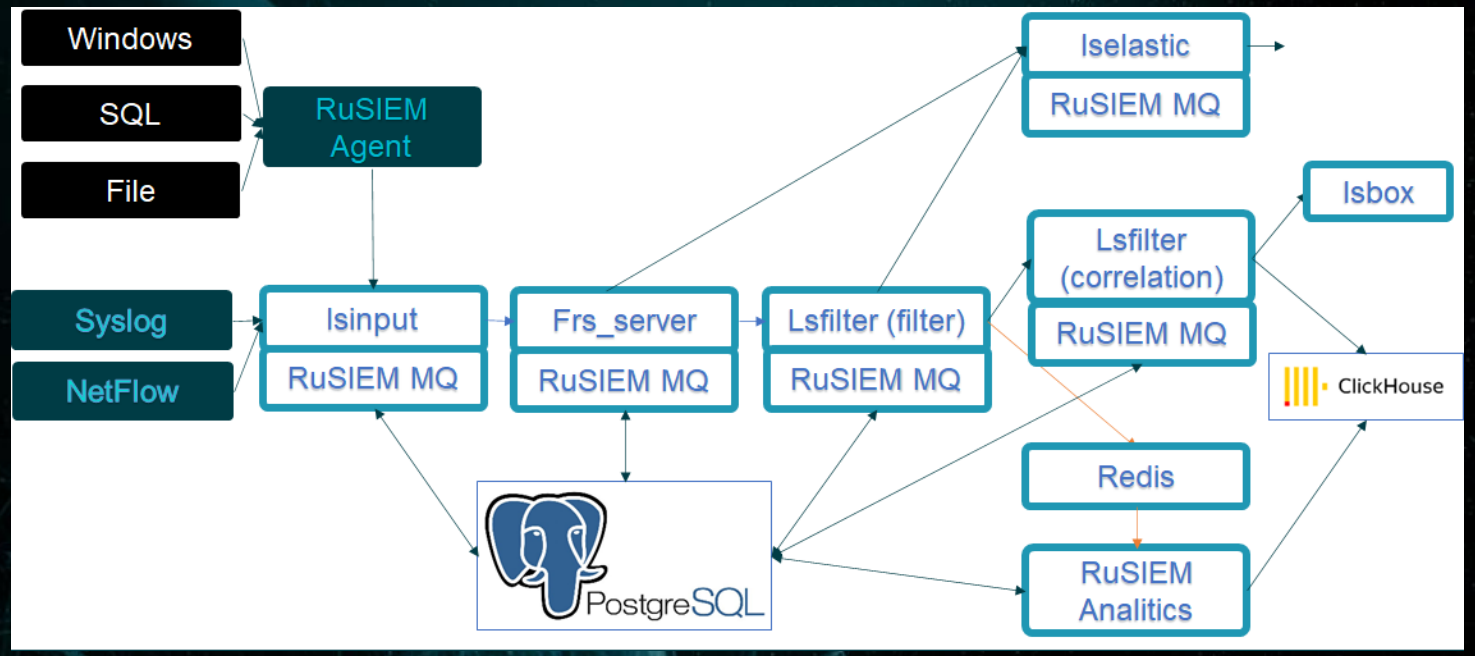
- Проектные цены
- Модульные спецификации
- Бессрочные и срочные лицензии
- Разработка сложных парсеров
- Разработка правил корреляции

**Кол-во событий в секунду (Event per second)**

2000 eps
3000 eps
4000 eps
5000 eps
7500 eps
10000 eps
12500 eps
15000 eps
20000 eps
...

RUSIEM
Всё под контролем

# Очередь событий – RuSIEM MQ




- Недоступность сервиса
- Превышение лицензионных метрик

# Масштабирование горизонтальное, распределение нагрузки


- Производительность
- «Горячее» расширение без остановки сбора
- Поддержка слабых каналов между удаленными объектами
- Корреляция в центральном офисе без необходимости передачи всех событий «наверх»
- Распределенный поиск по событиям без необходимости «единого хранилища»

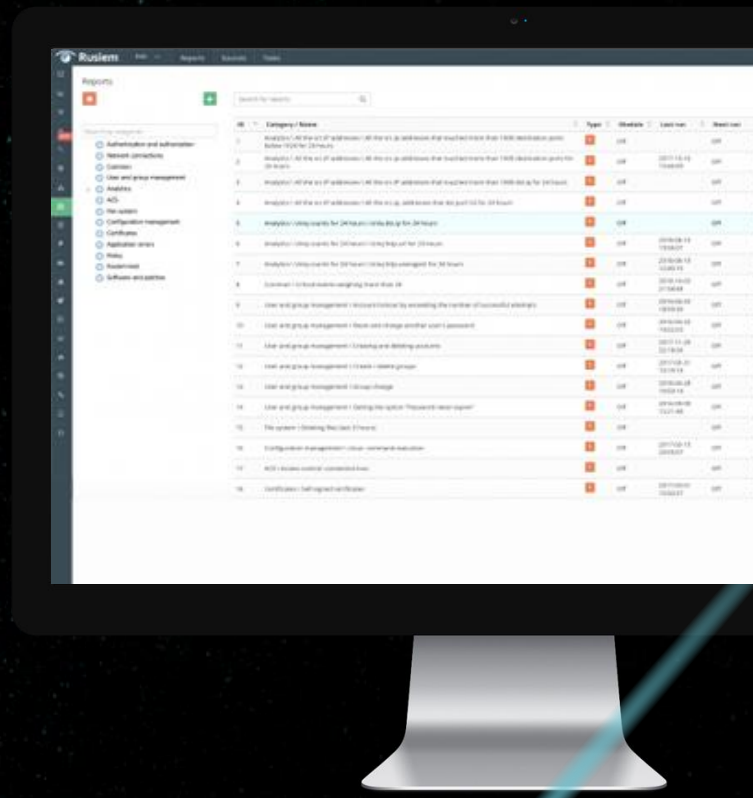
RUSIEM
Всё под контролем

# Масштабирование вертикальное


RUSIEM
Всё под контролем

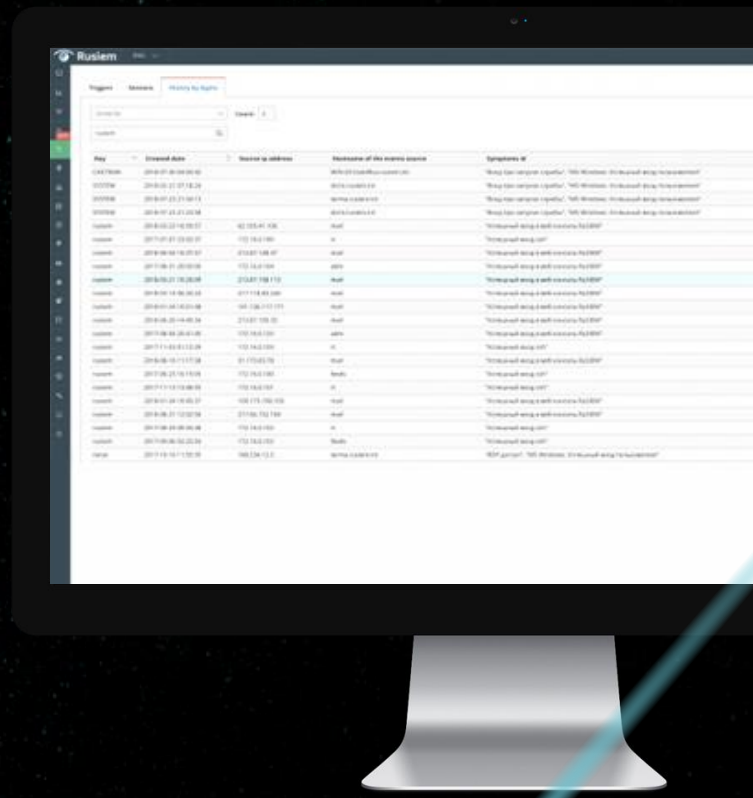
# Ретроспективный анализ

- Пользователь может выполнить **правило корреляции** по уже накопленным событиям в любой момент на всю глубину хранилища



# Динамические списки

- С помощью **правил корреляции** пользователь может создавать динамические списки для дальнейшего анализа



# Конструируй это!

- **Правила корреляции** (создание новых, корректировка имеющихся)
- **Отчеты** + настройка расписания, отправки, форматов
- **Дашборды**
- **Парсеры** (LogStash)

RUSIEM
Всё под контролем

# Основные итоги 2022 года

- Технологическое развитие RuSIEM
- Реализовано обещанное на 2022 год и даже больше
- Выпущены новые модули – RuSIEM Monitoring, RuSIEM IoC
- Выпущено 6 релизов системы
- Выход на международные рынки
- Интересные проекты, обнаружение сложных угроз
- Трехкратный рост партнерской сети
- Новые заказчики

# ЭТАП 1 - ВЫПОЛНЕНО

1

## Динамические таблицы

- возможность использовать табличные списки с функцией автоматического обновления информации внутри них

2

## Филиальная структура (Multitenancy)

- полноценная возможность создавать иерархические структуры SOC-ов с подчиненными SIEM-системами
  - обмен инцидентами
  - управление всеми настройками через интерфейс
  - разграничение прав доступа к информации

# ЭТАП 2 - ВЫПОЛНЕНО

1. Ручная привязка событий к инцидентам
2. Оптимизация нормализации

# ЭТАП 3 - ВЫПОЛНЕНО

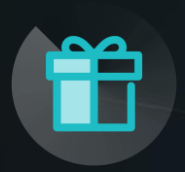
1

- **Модуль мониторинга IT–инфраструктуры**
  - IT Мониторинг представляет собой простой, функциональный набор механизмов получения текущей информации по серверам и сетевым устройствам

2

- **Версия для российских ОС**

# Линейка продуктов



**RvSIEM (free)**
– классическое решение класса LM

**RuSIEM**
– коммерческая версия класса SIEM

**RuSIEM Analytics**
– модуль для анализа событий, основанный на ML

New!!!

**RuSIEM IoC**
– модуль индикаторов компрометации

New!!!

**RuSIEM Monitoring**
– модуль мониторинга информационных систем, узлов, приложений

RUSIEM
Всё под контролем

# RuSIEM Monitoring

***система мониторинга ИТ-инфраструктуры с возможностью удаленного администрирования и встроенной системой HelpDesk***

# Назначение

*RuSIEM Monitoring позволяет контролировать работу ИТ-решений, входящих в периметр комплексной ИТ-инфраструктуры*

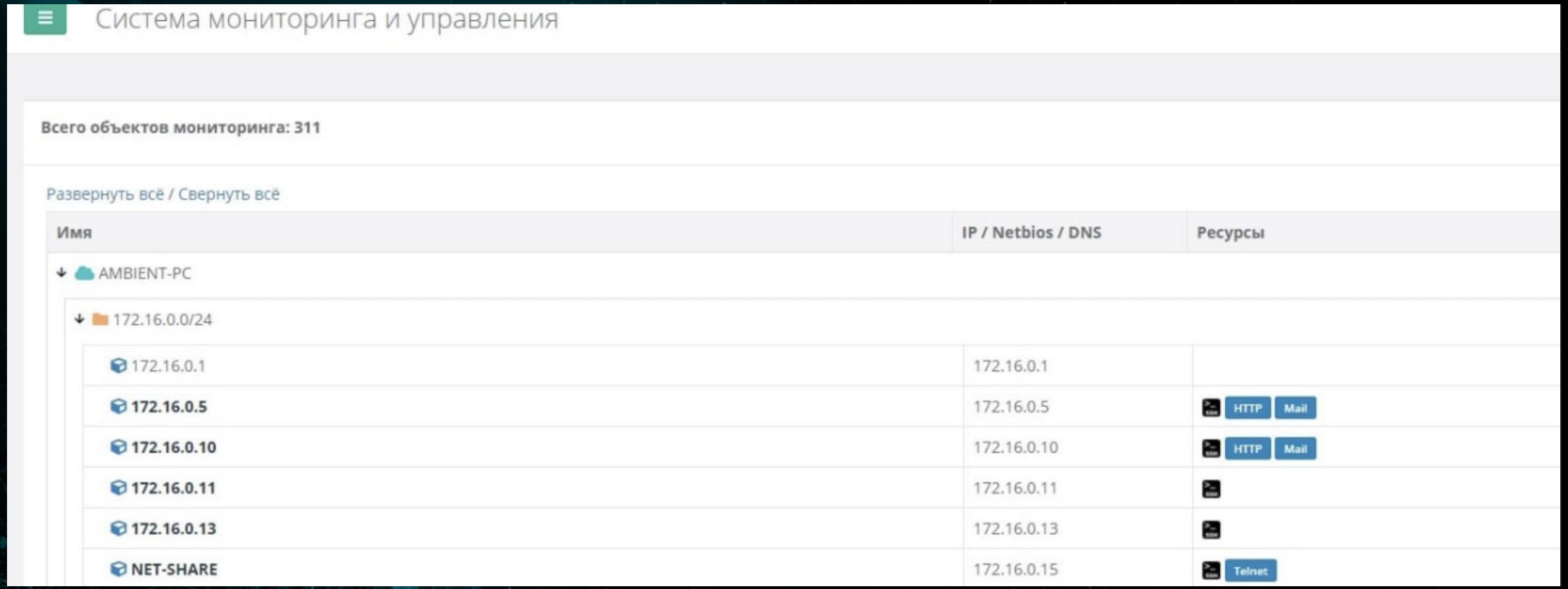
- Мониторинг параметров всех компонентов
- Оповещение специалистов, если значения оказываются вне заданных рамок
- Детальный анализ производительности оборудования
- Оперативное устранение и предотвращение сбоев в работе

RUSIEM
Всё под контролем

# Задачи

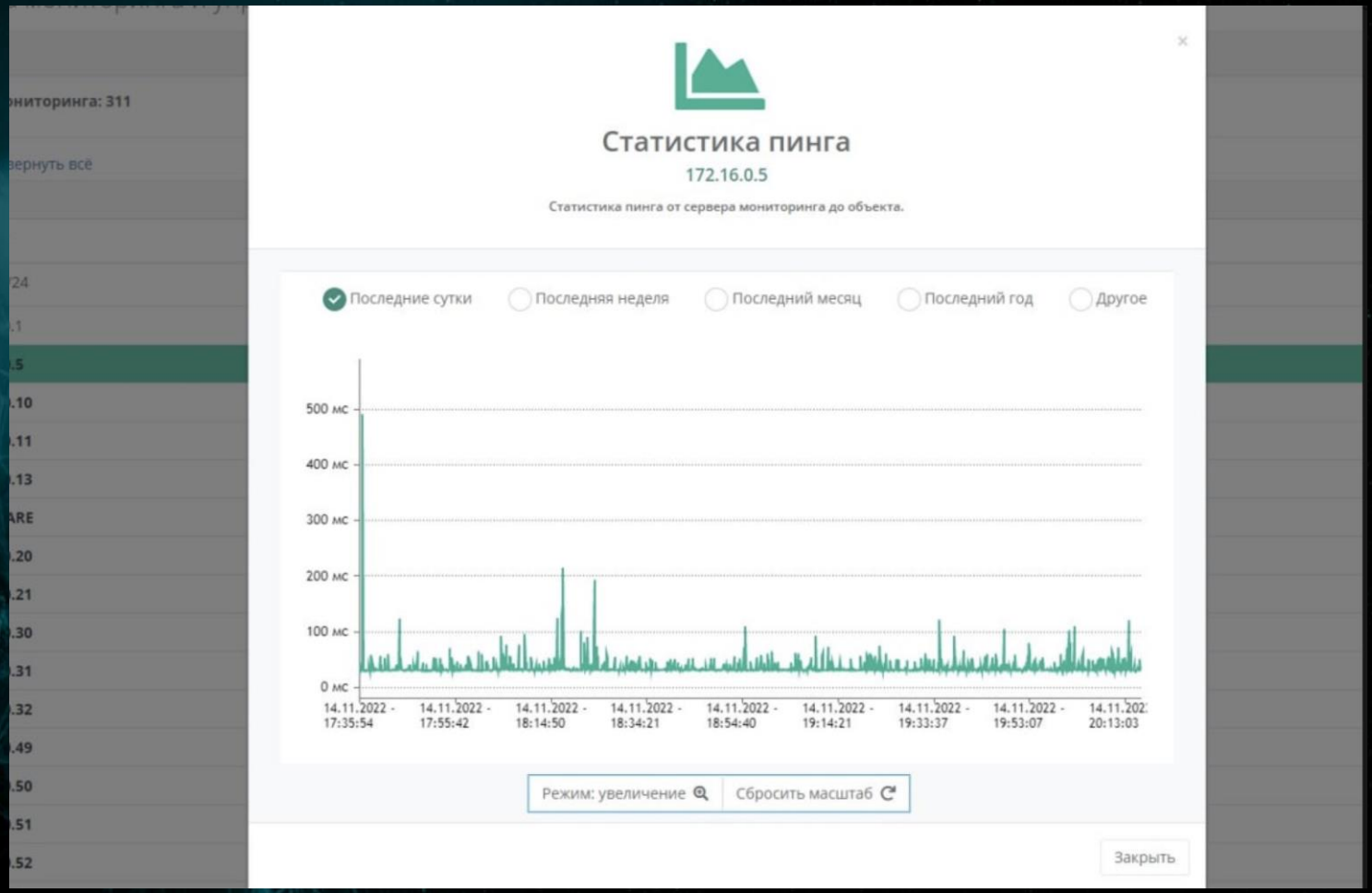
- Мониторинг и устранение неполадок узлов ИТ-инфраструктуры, включая серверы, сетевое оборудование и рабочие станции
- Мониторинг приложений, работающих в режиме реального времени для обеспечения бесперебойной работы
- Мониторинг информационных систем и бизнес-критичных серверов
- Улучшение процесса управления ИТ-инфраструктурой за счет упрощения выявления узких мест, пропускной способности и других потенциальных проблемных точек в сетевой среде
- Удаленный и защищенный доступ к управлению ИТ-инфраструктурой и, как результат, снижение затрат
- Простое и удобное администрирование рабочих станций пользователей и серверов, включая удаленные, что стало очень актуальным в нынешнее время

# Мониторинг и управление узлами инфраструктуры



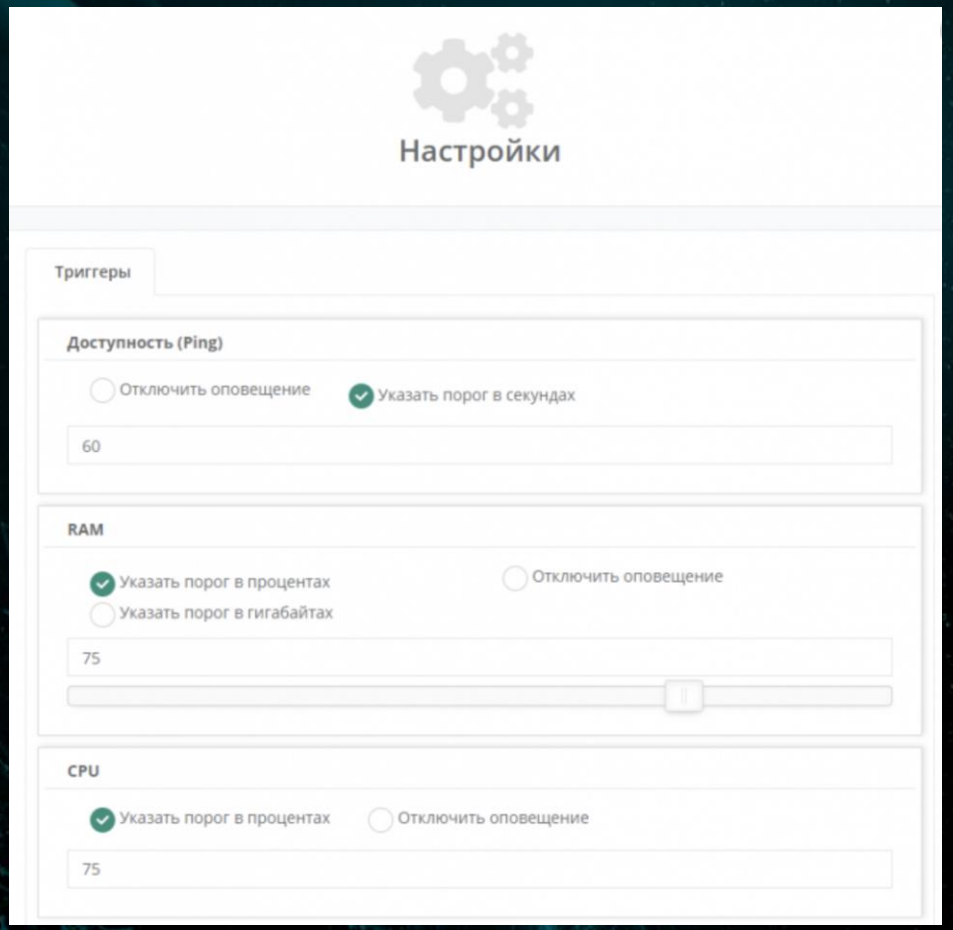

RUSIEM
Всё под контролем

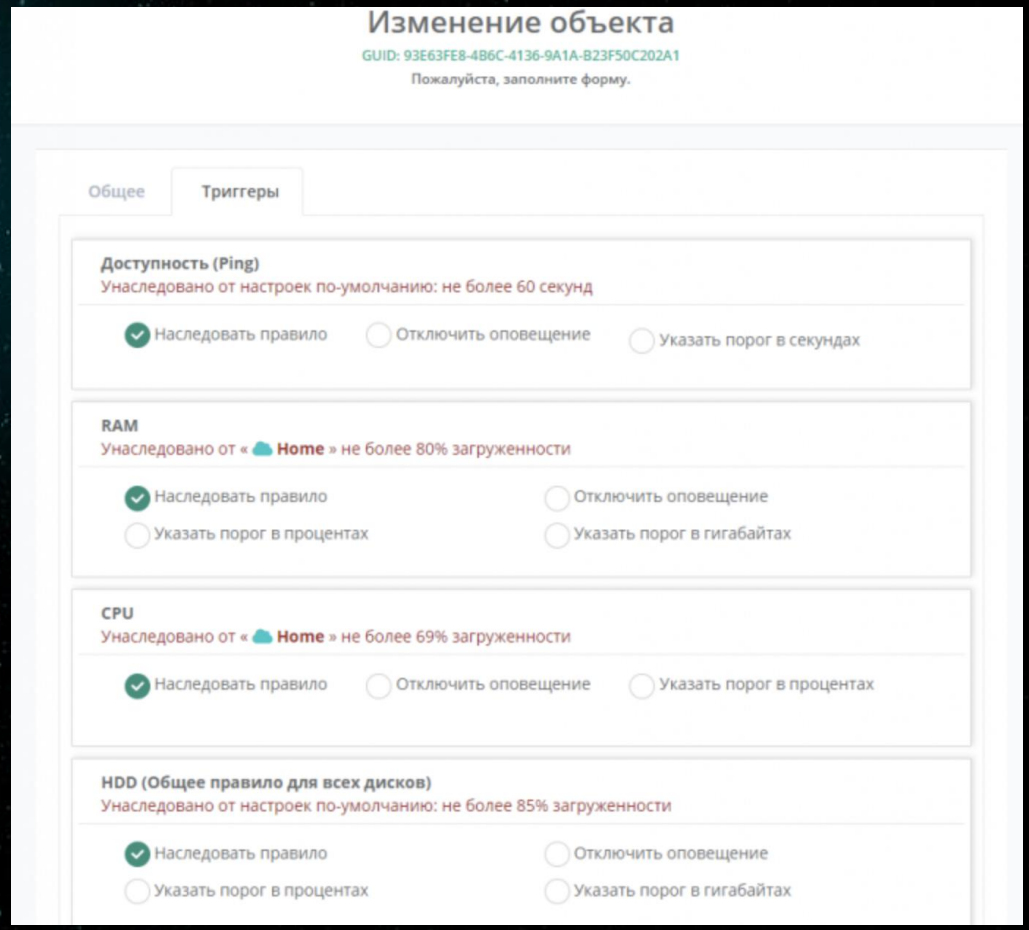
# Проверка целостности и качества соединений в сети




RUSIEM
Всё под контролем

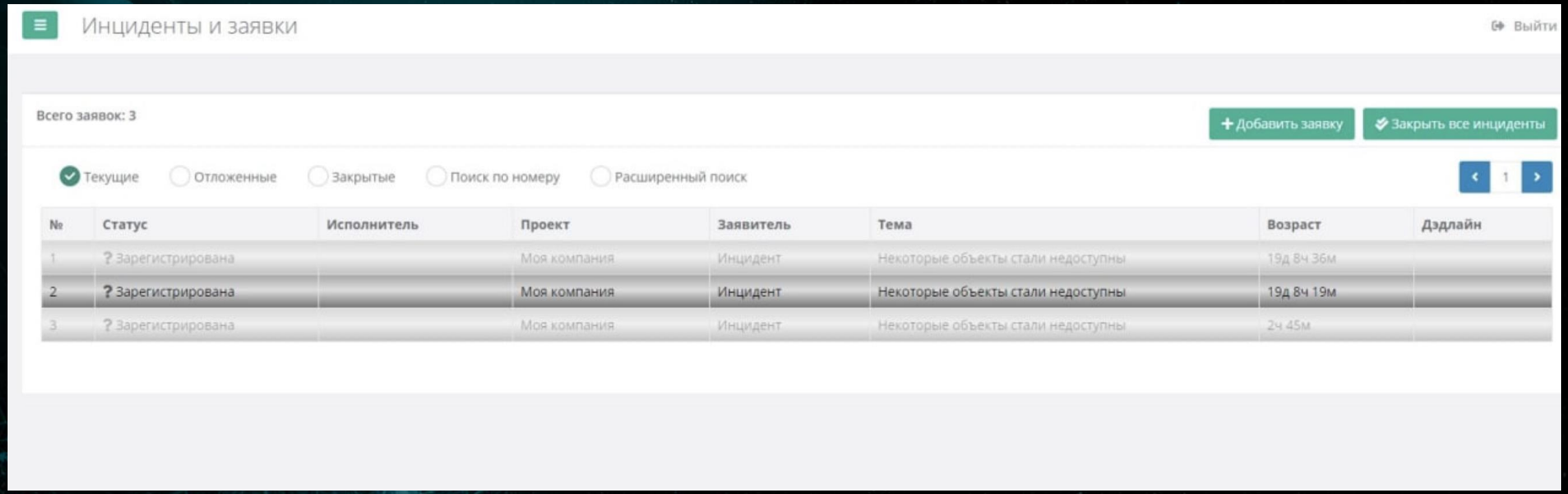
# Отслеживание изменения состояний объектов ИТ-инфраструктуры



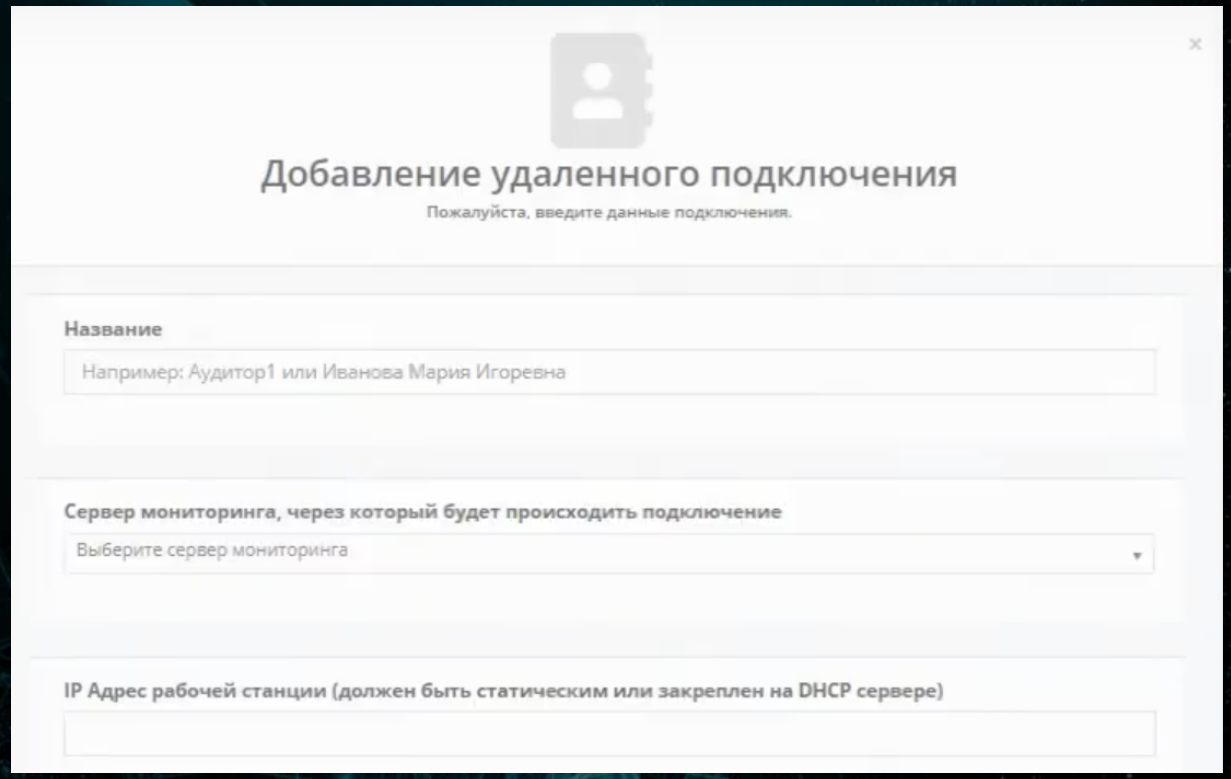

RUSIEM
Всё под контролем

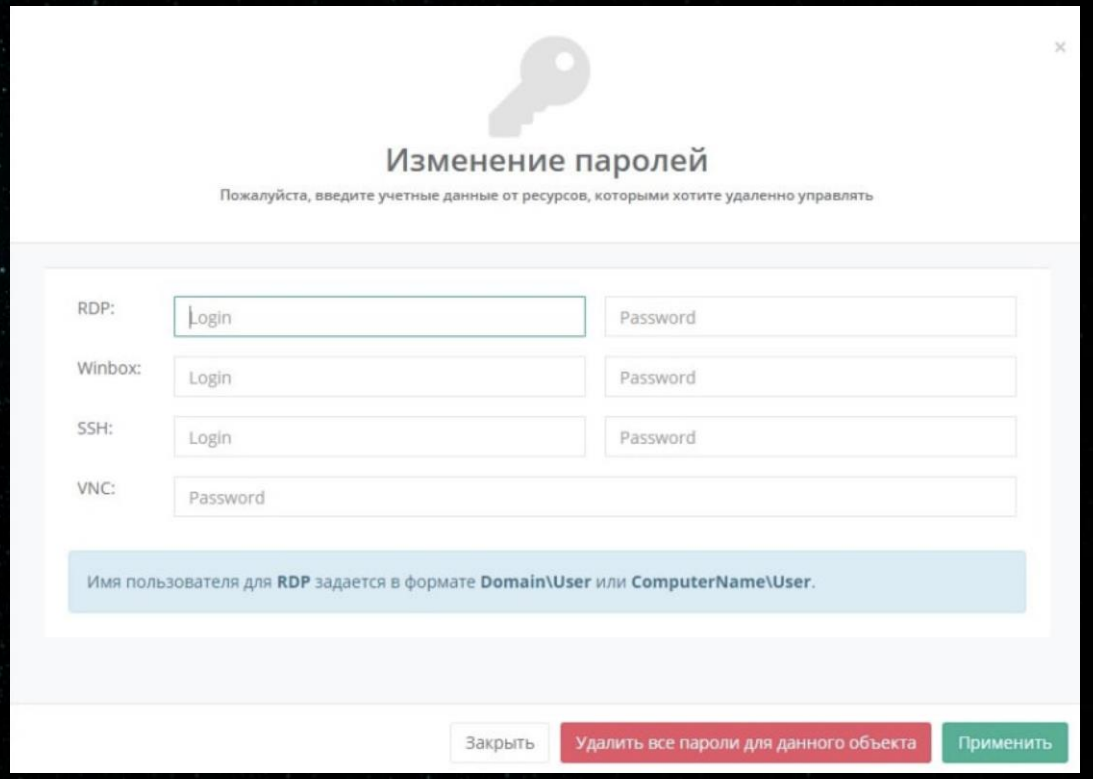
# Выявление инцидентов и создание заявок




RUSIEM
Всё под контролем

# Удаленное подключение и администрирование




RUSIEM
Всё под контролем

# Показатели

RuSIEM Monitoring позволяет оценивать в моменте нижеследующие параметры, а также большое количество других показателей, доступных через WMI, SSH, SNMP

## Информация об узле

- Нагрузка на CPU
- Нагрузка на оперативную память
- Занятость логических дисков

## Информация аппаратной части

- Процессоры
- Оперативная память
- Жесткие диски
- Сетевые адаптеры

## Информация из операционной системы (Microsoft Windows)

- Список локальных пользователей
- Доступные сетевые папки
- Установленное ПО
- Установленные роли сервера
- Остановленные службы
- История входов пользователей

# Преимущества

- Мониторинг не требует установки агентов на серверы
- Запуск системы в работу осуществляется за 10 минут: подключение к серверам и сетевому оборудованию в один клик
- Удаленная поддержка: наличие внутренней системы HelpDesk с доменной авторизацией и подключение к пользователю в один клик из тикета

RUSIEM
Всё под контролем

# RuSIEM IoC

***модуль выявления угроз для корпоративных устройств на основе индикаторов компрометации***

# IoC (Indicators of Compromise)

*Признаки, позволяющие выявлять вредоносную активность, происходящую с корпоративных устройств организации*

Срабатывают, когда

- злоумышленники используют устройство ИТ-инфраструктуры (рабочая станция, оргтехника или иное оборудование, имеющее выход в Интернет) в качестве элементов botnet-сетей
- устройство устанавливает связь с сайтами или командными серверами преступников

# Назначение

**RuSIEM IoC** – модуль SIEM-системы RuSIEM, позволяющий выявить угрозу для корпоративных устройств в виде попыток связаться с вредоносной инфраструктурой злоумышленника

- ✓ Модуль подгружает в систему информацию об IP-адресах, доменах, url, хэшах вредоносного ПО (ВПО)
- ✓ Как только SIEM-система фиксирует в сетевом потоке или хостовой активности обращение к ресурсам, которые есть в базе, она сообщает об этом оператору, указывая, какой конкретно элемент ИТ-инфраструктуры скомпрометирован и требует «лечения»

# Выявляемые угрозы

- Загрузка вредоносных файлов с зараженных ресурсов сети Интернет
- Автоматические запросы с компьютеров к инфраструктуре злоумышленников
- Обращение компонентов клиентской инфраструктуры на вредоносные узлы
- Запросы и обращения с инфраструктуры злоумышленников либо зараженных узлов
- Идентификация конкретного ВПО либо хакерской группировки

# Потребность в IOC

- Покупают SIEM/SOAR/TIP
- Уже есть внедренный SIEM и его активно используют
- Уже есть TIP и его используют
- Ищут замену для подписки от зарубежного вендора
- Активно используют NGFW
- MSSP

# Преимущества RuSIEM IoC

- Автоматическая настройка
- Анализ данных из более чем **260** открытых источников
- Сбор индикаторов из социальных сетей (Telegram, Twitter), репозиториев Github, данных публичных TI-отчетов
- **Более 250 тысяч** уникальных индикаторов в сутки, **30 тысяч** из которых имеют **наивысший уровень опасности**
- Интеллектуальная нормализация, очистка, обогащение индикаторов
- Определение степени опасности каждого индикатора на базе уникальной математической модели ранжирования

Согласно результатам исследования SANS 2021/2022 Cyber Threat Intelligence Survey, интерес к TI, собираемого из открытых источников, растет из года в год

В 2021 году **66,3%** опрошенных использовали открытый TI, а в 2022 году – **71,7%**

# В планах на 2023 год

- Дальнейшее технологическое развитие решения
- Новые проекты и довольные заказчики
- Укрепление партнерской сети
- Развитие международных активностей
- Внутреннее укрепление и развитие команды

RUSIEM
Всё под контролем

# Telegram-каналы RuSIEM

*https://t.me/**rusiem***

*последние новости, важные события*

*https://t.me/**rusiemsupport***

*возможность быстро связаться с технической поддержкой*

RUSIEM
Всё под контролем

RUSIEM
Всё под контролем

# *Спасибо за внимание!*

Дмитрий Чеботарев
d.chebotarev@rusiem.com
+7(916) 824-65-00