



**RUSIEM**

Всё под контролем

# ***Технологическое развитие 2023 года и планы на 2024 год***

***Владислав Шатохин,  
менеджер по работе с ключевыми заказчиками***

# RuSIEM – это



Полностью  
русская разработка  
(с 2014 года)

Sk Сколково

Резидент  
Сколково

> 550

Партнеров в России и  
странах СНГ



Продукт включен  
в Единый реестр  
отечественного ПО



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

# Линейка продуктов



## RvSIEM (free)

– классическое решение класса LM



## RuSIEM

– коммерческая версия класса SIEM



## RuSIEM Analytics

– модуль для анализа событий, основанный на ML



## RuSIEM IoC

– модуль индикаторов компрометации



## RuSIEM Monitoring

– модуль мониторинга информационных систем, узлов, приложений

# 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»

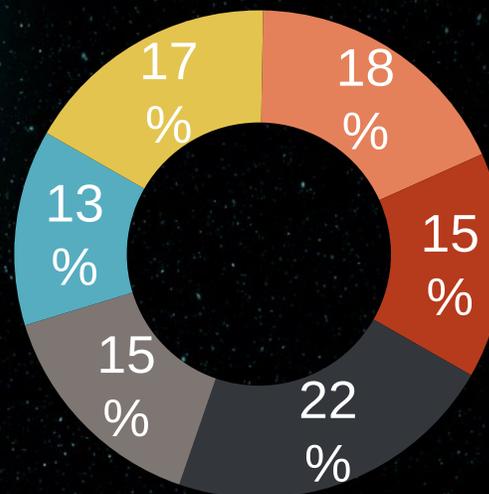
# Особенности RuSIEM



# Аналитика по отрасли (SIEM)

- Активное развитие рынка отечественных SIEM-систем и выход на рынок новых игроков
- Успешная миграция на российские SIEM: сложностей при миграции все меньше, а решения становятся все более технологичными и зрелыми
- SIEM остаётся центральным инструментом выявления компьютерных атак, массовость и сложность которых неуклонно возрастают

## Тенденции развития российских SIEM?



- Предиктивная аналитика (в т.ч. на базе ИИ) (22%)
- Масштабируемость и быстродействие (18%)
- Удобство использования (17%)
- Реагирование на инциденты и киберразведка (15%)
- Нарращивание экспертизы и возможностей «из коробки» (15%)
- Интеграция и экосистемность (13%)

# Стратегические итоги 2023

- Технологическое развитие RuSIEM, выпуск новых модулей
- По предварительным подсчетам рост компании в 2 раза относительно итогов 2022 года (в 2022 году был зафиксирован 3х-кратный рост по отношению к 2021 году)
- 4 мажорных релиза за 2023 год, готовый 5-й релиз с обновленным дизайном системы (дата релиза: 8 февраля 2024 года)
- Усиление экспансии на международной арене (новые рынки)
- Значительный рост партнерской сети и числа заказчиков разных сфер деятельности

# Технологические итоги 2023

1

## НОВЫЙ ФУНКЦИОНАЛ

- Поддержка Ubuntu 22
- Добавлена вкладка «Задачи по инцидентам»
- Обогащение событий активами
- Добавлено множество правил корреляции
- Агрегация событий
- Возможность фильтрации входящих событий
- Telegram-уведомления об инцидентах
- RuAgent оптимизирован под нагрузку
- Разработан модуль сбора событий ODBC

# Технологические итоги 2023

## 2

### ФИЛИАЛЬНАЯ СТРУКТУРА (Multitenancy)

- Добавлена возможность фильтрации по тенантам
- Оптимизирован функционал обмена статическими списками
- Оптимизирован функционал обмена правилами корреляции
- Добавлен функционал контроля статусов лицензий
- Добавлен функционал копирования списков на подчиненные ноды

# Технологические итоги 2023

3

## ИСТОЧНИКИ

- Оптимизирован раздел работы с агентами
- Добавлена функция массового удаления агентов

4

## АГЕНТ

- Оптимизирован модуль RestAPI
- Оптимизирован модуль EventLog
- Оптимизирован модуль FileLog
- Оптимизирован модуль FTP Log
- Доработан модуль АПКШ Континент
- Повышена стабильность модуля postgresql

# Технологические итоги 2023

5

## ОТЧЕТЫ

- Добавлена возможность выбора полей инцидентов
- Генерация отчетов в формате docx
- Доработаны отчеты по задачам инцидентов

6

## МИКРОСЕРВИСЫ

- Оптимизирован коррелятор
- Повышена стабильность нормализатора
- Добавлена возможность удаления конфигураций

# Технологические итоги 2023

7

- Новые правила корреляции – 42
- Новые парсеры – 28
- Доработанные парсеры – 96

Полный перечень доработок, вошедших в состав продукта, доступен на сайте в разделе

**«История обновлений»** -

[https://rusiem.com/ru/products/release\\_notes](https://rusiem.com/ru/products/release_notes)

# Технологические планы на 2024 год

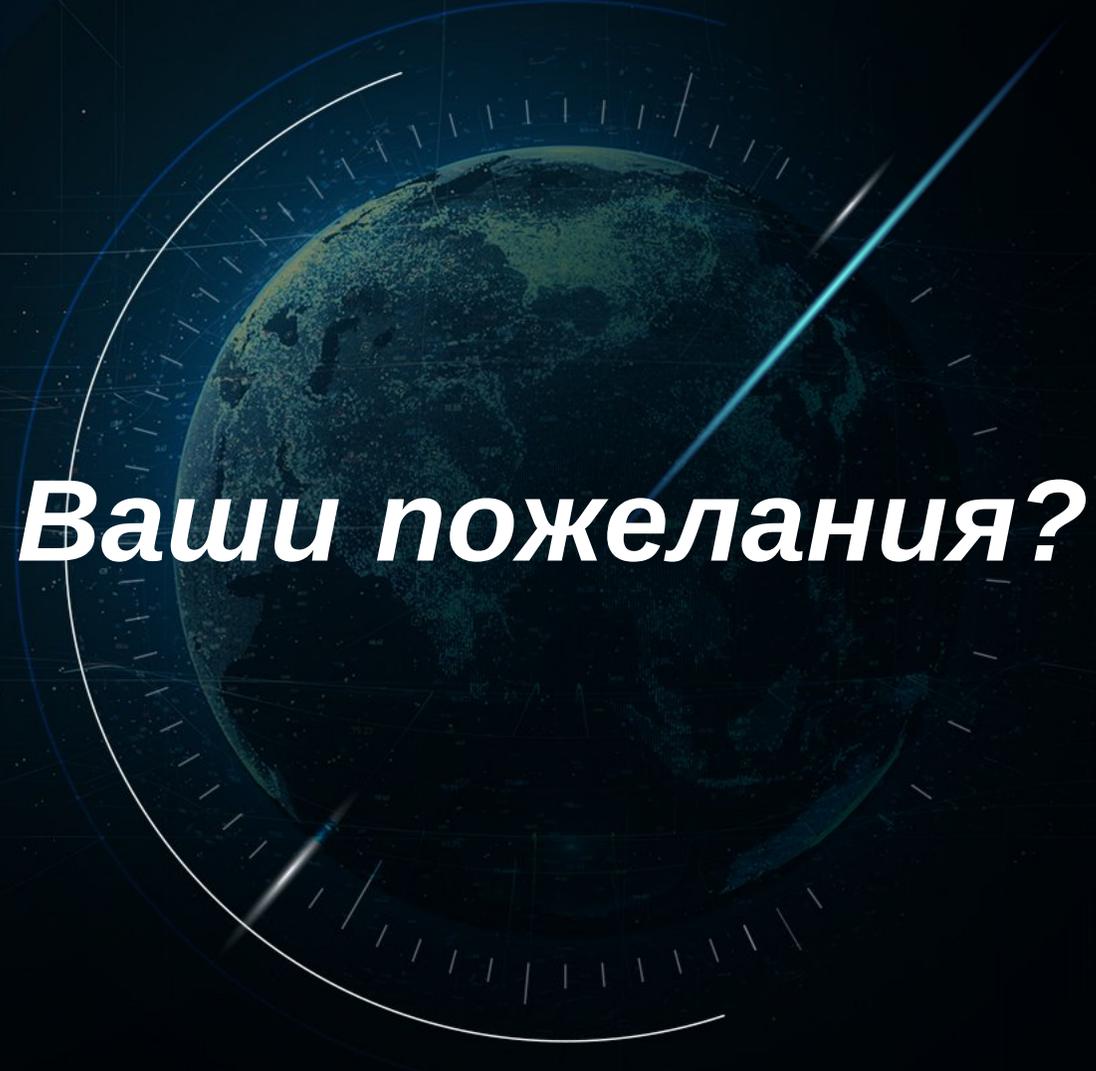
- Новый интерфейс
- Sigma конвертер
- Мониторинг источников (начало года – syslog, после – доработка по всем)
- SNMP trap
- Оптимизация работы коррелятора и нормализатора
- Создание модели для выявления вредоносного кода
- Поиск аномалий в запущенных процессах Windows/Linux/macOS пользователей

# Технологические планы на 2024 год

- Обновленные и оптимизированные baseline в аналитике
- Новые операторы для коррелятора
- Обновление базы корреляций
- Реагирование на отсутствие событий
- Обновленная система оповещения через Telegram
- Статические таблицы
- Обогащение событий из статических таблиц
- Новые виджеты в дашбордах
- Агент на Linux

# Стратегические планы на 2024 год

- Дальнейшее технологическое развитие решения
- Выпуск новых модулей
- Укрепление позиций в России и СНГ
- Открытие локальных представительств в отдельных странах СНГ
- Укрепление партнерской сети
- Новые проекты и довольные заказчики
- Развитие международных активностей
- Внутреннее укрепление и развитие команды



***Ваши пожелания?***

# Telegram-каналы RuSIEM

<https://t.me/rusiem>

*последние новости, важные события*



<https://t.me/rusiemsupport>

*возможность быстро связаться с технической поддержкой*



**Спасибо за внимание!**

Владислав Шатохин

✉ [v.shatohin@rusiem.com](mailto:v.shatohin@rusiem.com)

☎ **+7(915)776-27-31**

