RUSIEM
Всё под контролем

Выявление киберугроз и реагирование на инциденты информационной безопасности

Даниил Вылегжанин,
Менеджер по техническому сопровождению продаж

1

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

Задачи 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)

SIEM-система RuSIEM

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

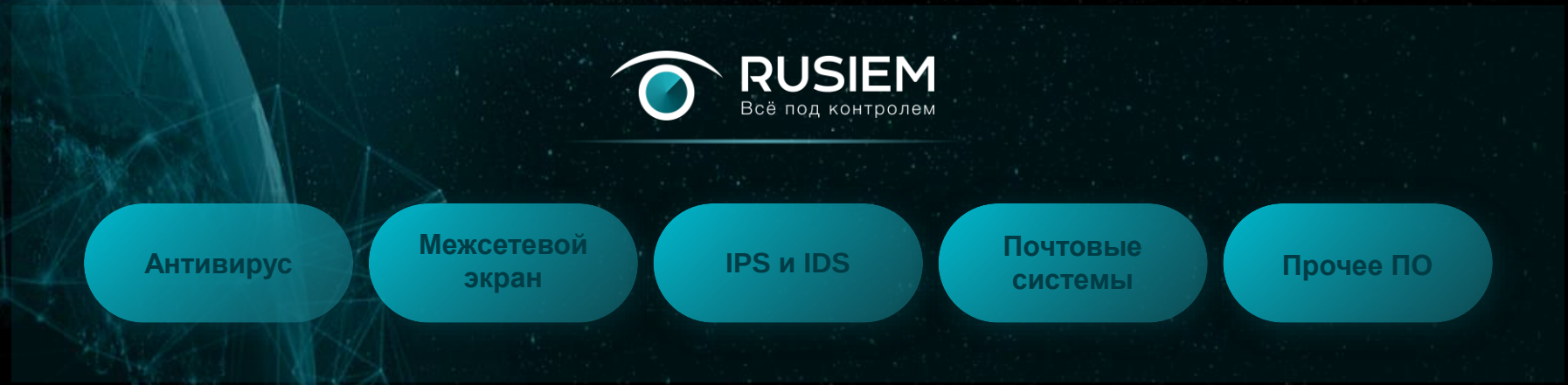
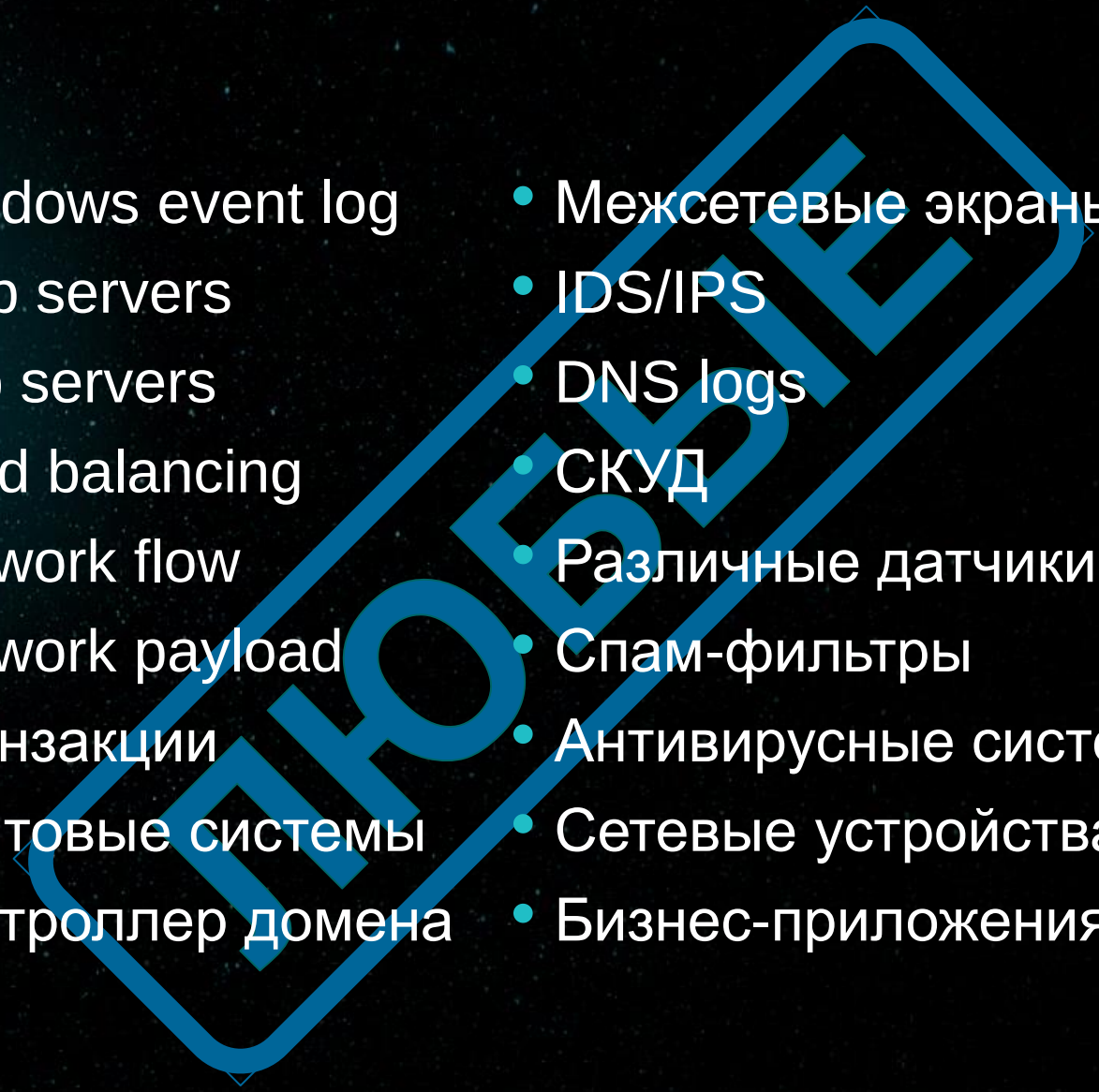


Схема работы SIEM

Источники событий для SIEM

- Windows event log
- Web servers
- App servers
- Load balancing
- Network flow
- Network payload
- Транзакции
- Почтовые системы
- Контроллер домена
- Межсетевые экраны
- IDS/IPS
- DNS logs
- СКУД
- Различные датчики
- Спам-фильтры
- Антивирусные системы
- Сетевые устройства
- Бизнес-приложения



Где может применяться SIEM

Примеры событий

- Сетевые атаки
- Фрод и мошенничество
- Откуда и когда блокировались учётные записи
- Изменение конфигураций «не админами»
- Повышение привилегий
- Выявление несанкционированных сервисов
- Обнаружение НСД (вход под учётной записью уволенного сотрудника)
- Отсутствие антивирусной защиты на новом установленном компьютере
- Изменение критичных конфигураций с VPN подключений
- Контроль выполняемых команд на серверах и сетевом оборудовании
- Аудит изменений конфигураций (сетевых устройств, приложений, ОС)
- Аномальная активность пользователя (массовое удаление/копирование)
- Обнаружение вирусной эпидемии
- Обнаружение уязвимости по событию об установке ПО
- Оповещение об активной уязвимости по запуску ранее отключенной службы
- Обнаружение распределённых по времени атаках
- Влияние отказа в инфраструктуре на бизнес-процессы

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

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»

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

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

RvSIEM Free vs RuSIEM

RUSIEM
Всё под контролем

RuSIEM Monitoring

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

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

RuSIEM IoC

Модуль выявления угроз для корпоративных устройств на основе индикаторов компрометации

- 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

RUSIEM
Всё под контролем

Построение Центра Мониторинга Информационной безопасности (SOC)

Примеры проектов

RUSIEM
Всё под контролем

Задачи SOC

Центр мониторинга информационной безопасности (Security Operations Center, SOC) — структурное подразделение организации, отвечающее за оперативный мониторинг IT-среды и предотвращение киберинцидентов. Специалисты SOC собирают и анализируют данные с различных объектов инфраструктуры организации и при обнаружении подозрительной активности принимают меры для предотвращения атаки

- Постоянный поиск, мониторинг и анализ вторжений
- Проактивное предотвращение угроз
- Проверка сетей компании на уязвимость и анализ инцидентов безопасности
- Фильтрация ложных срабатываний и быстрая реакция на подтвержденные инциденты
- Подготовка отчетов об актуальном состоянии ИТ-инфраструктуры, зарегистрированных инцидентах и действиях потенциальных злоумышленников

SOC на RuSIEM

SOC был развернут для ряда крупных заказчиков на базе SIEM-системы RuSIEM совместно с партнерами

МегаФон Мобильный оператор №1 по скорости и покрытию by Ookla 2022

ЭР-Телеком

Информационный центр

@Страл Безопасность

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!

Даниил Вылегжанин
d.vylegzhanin@rusiem.com
+7 (926) 840-84-10