RUSIEM

Всё под контролем

РЕШЕНИЕ ДЛЯ КОНТРОЛЯ ВАШЕГО БИЗНЕСА

SIEM: МИФЫ И РЕАЛЬНОСТЬ

ЧТО ТАКОЕ SIEM И ЗАЧЕМ ОНА НУЖНА

SIEM представляет собой улучшенную систему обнаружения вредоносной активности и различных системных аномалий. Работа SIEM позволяет увидеть более полную картину активности сети и событий безопасности. Когда обычные средства обнаружения по отдельности не видят атаки, но она может быть обнаружена при тщательном анализе и корреляции информации из различных источников.

Сотни и тысячи устройств живут своей жизнью и генерируют миллионы событий, сообщая о том, что происходит с ними и вокруг. При этом необходимо реагировать только на часть из них.

Отдельные устройства, операционные системы только предоставляют события без детального анализа

Для полной картины происходящего необходимо собрать воедино состояния с отдельных устройств

Для этого и нужна SIEM система

SIEM - система собирает, анализирует и представляет информацию из сетевых устройств, средств защиты информации и информационных систем.
Также в систему входят приложения для контроля идентификацией и доступом, инструменты управления уязвимостями.

ГДЕ МОЖЕТ ПРИМЕНЯТЬСЯ SIEM?

Везде, где из журналов событий можно извлечь полезную информацию

ПРИМЕРЫ СОБЫТИЙ

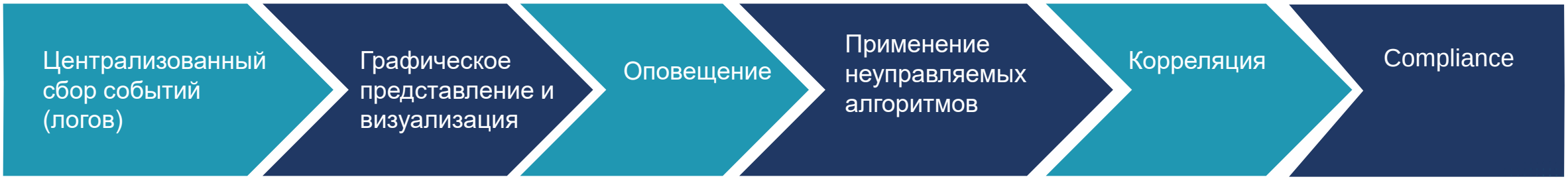
- Сетевые атаки
- Фрод и мошенничество
- Откуда и когда блокировались учетные записи
- Изменение конфигураций «не админами»
- Повышение привилегий
- Выявление несанкционированных сервисов
- Обнаружение НСД (вход под учетной записью уволенного сотрудника)
- Отсутствие антивирусной защиты на новом установленном компьютере
- Изменение критичных конфигураций с VPN подключений
- Контроль выполняемых команд на серверах и сетевом оборудовании
- Аудит изменений конфигураций (сетевых устройств, приложений, ОС)
- Выполнение требований Законодательства и регуляторов (PCI DSS, СТО БР, ISO 27xx)
- Аномальная активность пользователя (массовое удаление/копирование)
- Обнаружение вирусной эпидемии
- Обнаружение уязвимости по событию об установке софта
- Оповещение об активной уязвимости по запуску ранее отключенной службы
- Обнаружение распределенных по времени атаках
- Влияние отказа в инфраструктуре на бизнес-процессы

ВЧЕРА
СЕГОДНЯ

SIEM

Какова причина роста функционала SIEM систем?

- Потребность?
- Отсутствие персонала?
- Рост уровня угроз?



СЕГОДНЯ ЗАВТРА

SIEM

Направление развития SIEM систем очень обширно и выбор остается за Вами, что необходимо именно Вам.

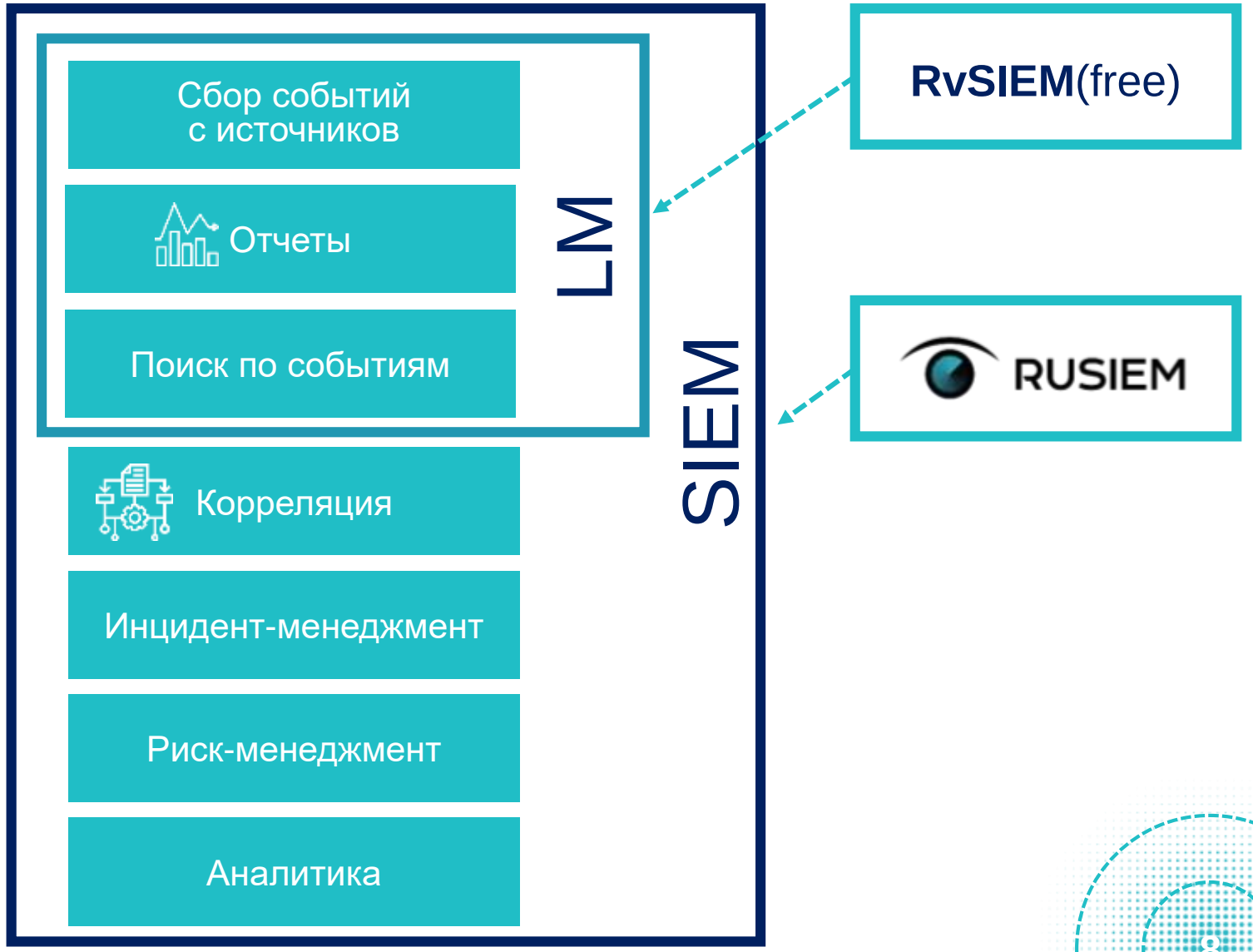
Нормализация	Asset Management	SOC	Threat Intelligence	UBA
Симптоматика	Vulnerability management	GRC	DL/ML/AI	SOAR

SIEM: Мифы и реальность!

Стандартные вопросы и заблуждения

- Дорого?
- Нужен только в зрелой инфраструктуре? Будем внедрять как внедрим остальные СЗИ?
- Сложно подключить не типовые источники?
- Необходим высококвалифицированный персонал?
- Нужна поддержка 24*7*365?
- Долго настраивать правила корреляций?
- Да мы можем сами быстро сделать!

SIEM vs LM


Сбор событий
с источников
Отчеты
Поиск по событиям
LM
Корреляция
Инцидент-менеджмент
Риск-менеджмент
Аналитика
SIEM
RvSIEM(free)
RUSIEM

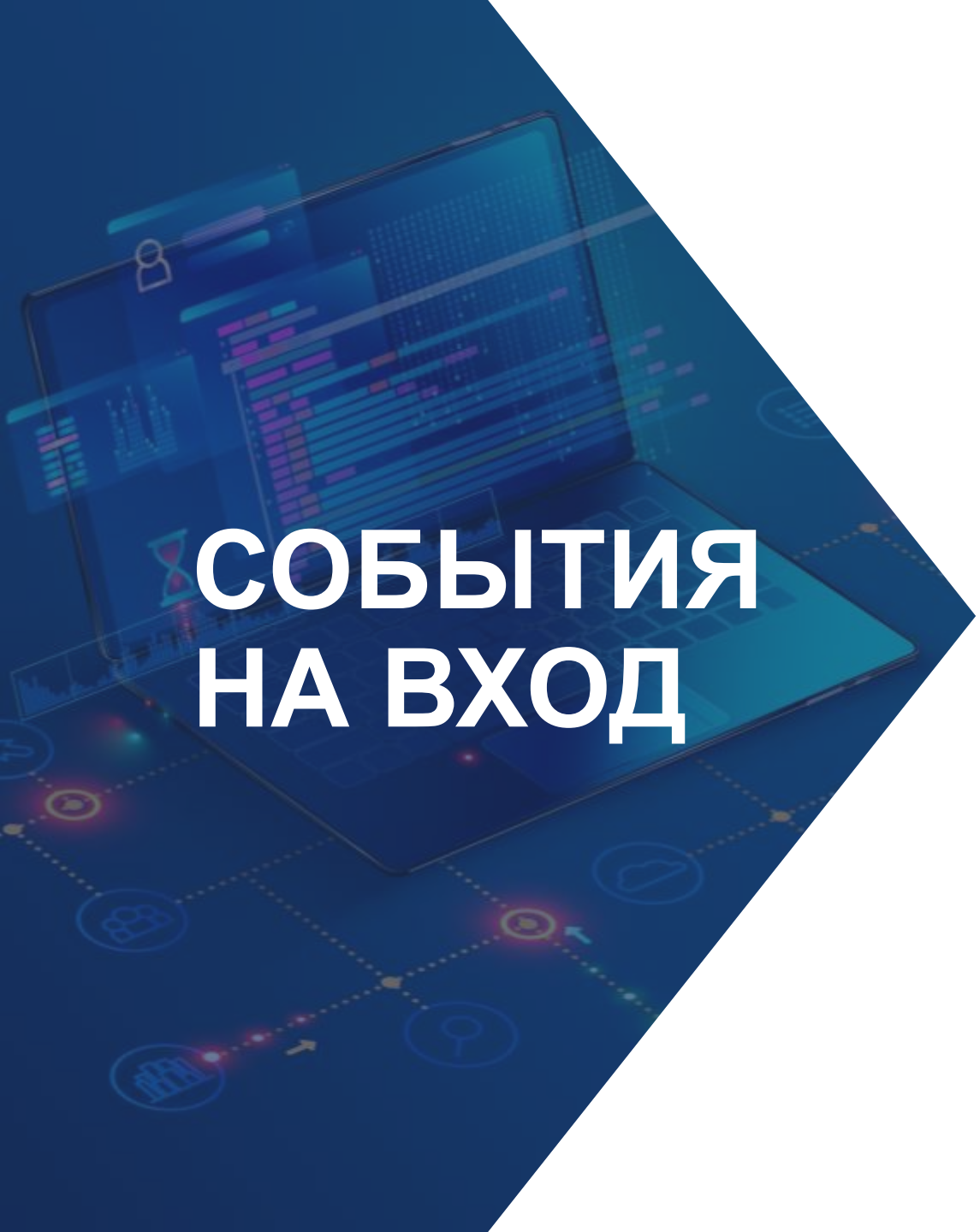
	RuSIEM	RuSIEM Analytics	RvSIEM (free)
Дашборды (набор виджетов для оценки показателей в режиме реального времени)	✓	✓	✓
Поиск по событиям	✓	✓	✓
Сохраненные запросы	✓	✓	✓
RBR (rule-based) корреляция	✓	✓	
Инцидент менеджмент по ITIL	✓	✓	
Симптоматика для тегирования событий понятным описанием	✓	✓	✓
Риск-метрики	✓	✓	✓
Отчеты	✓	✓	✓
Отчеты соответствия стандартам и политикам	✓	✓	
Аналитика (агрегация событий) для обнаружения инцидентов без корреляции		✓	
Аналитика (baseline) для обнаружения инцидентов без корреляции		✓	
Обновляемые ленты угроз (feeds: потенциально опасные ip, hash, url, fqdn, mail)		✓	
Аналитика (сложные отчеты с расчетами)		✓	
ИТ активы с обновлением в режиме реального времени		✓	
Агент с универсальными коннекторами к источникам	✓	✓	✓
Масштабируемость	✓	✓	limited
Обновление базы знаний (правила корреляции, отчеты, симтомы)	✓	✓	✓
Поддержка	24x7	24x7	limited
Обновление версий	✓	✓	✓

ТЕХНОЛОГИИ

1. В основе решения заложена собственная технология, основанная на потребительском спросе, практическом опыте и техническом анализе конкурентов.

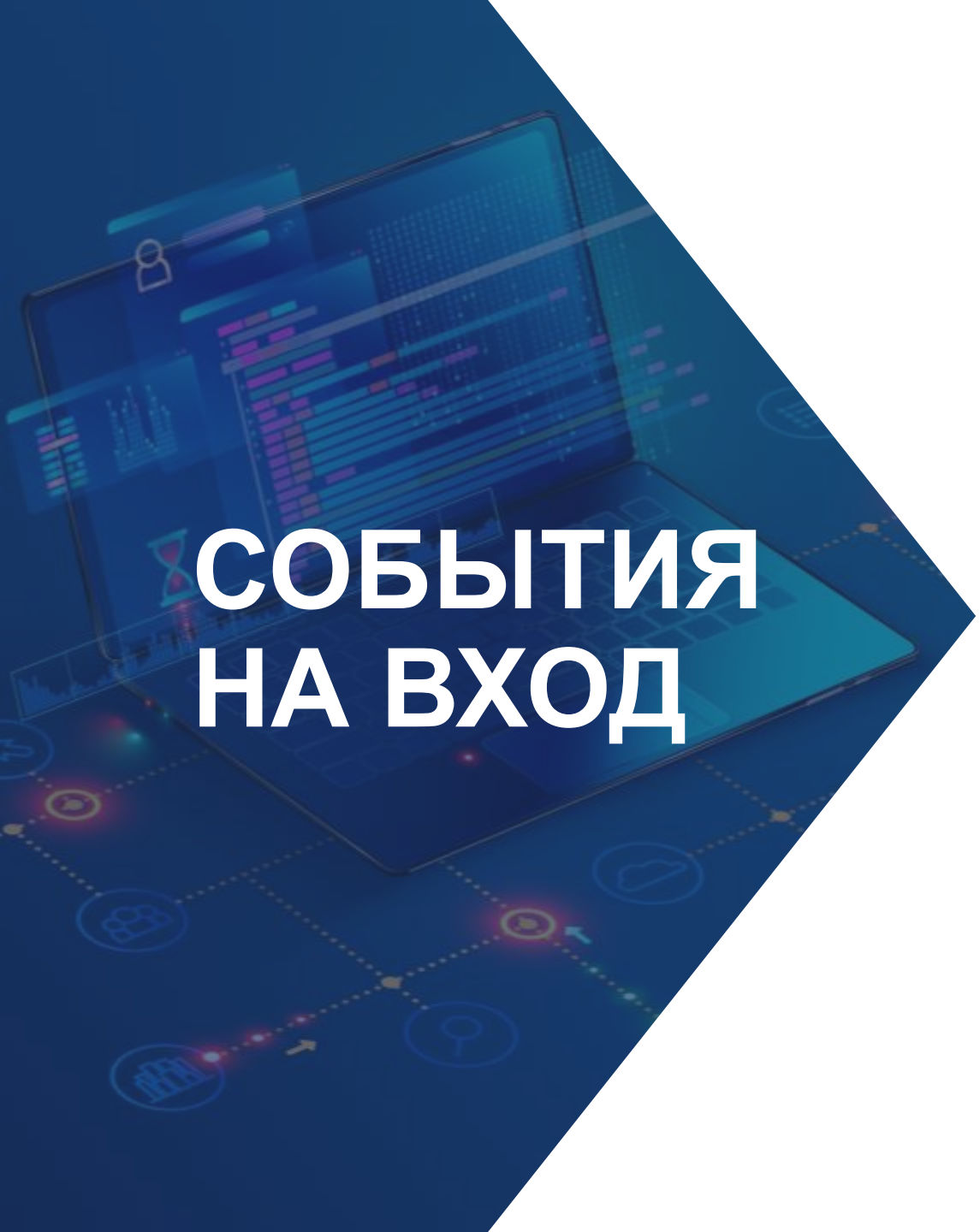
2. Используются современные принципы разработки, позволяющая решению развиваться, заменять модули и пополнять решение новыми, подстраиваться под потребности клиентов

3. Практическое использование AI и DL технологии



СОБЫТИЯ НА ВХОД

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

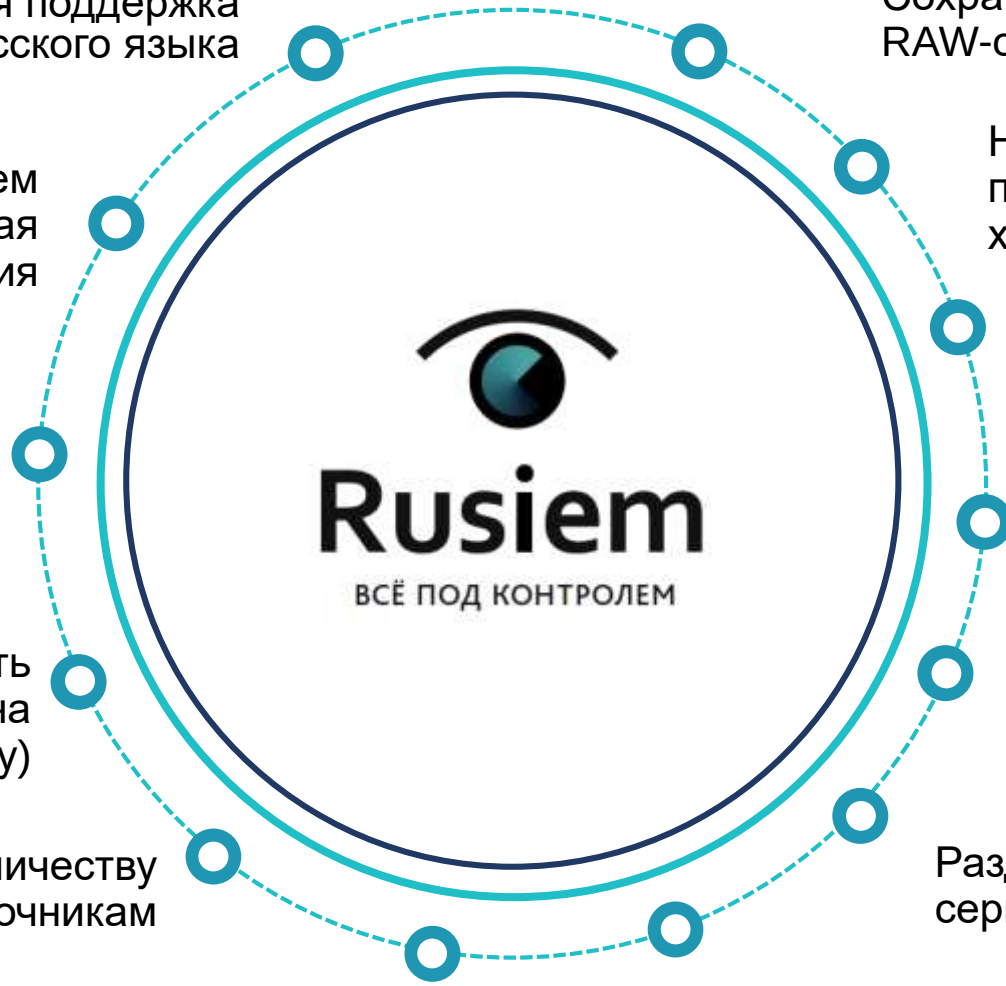


СОБЫТИЯ НА ВХОД

ЛЮБЫЕ

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

КОНКУРЕНТНЫЕ ПРЕИМУЩЕСТВА



Полная поддержка русского языка

Сохранение исходных RAW-событий

Приведенная к общем формату объектная нормализация

Нет ограничений по размеру архивного хранилища

Коннекторы от производителя

Встроенная управляемая и редактируемая корреляция

Real-time и историческая корреляция

Высокая производительность (Свыше 90000 событий на одну ноду)

Наличие собственных модульных агентов

Нет ограничений по количеству событий и источникам

Разделение нагрузки на несколько серверов или виртуальных машин

Легкая вертикальная масштабируемость

О КОМПАНИИ RUSIEM

Программный код создан российскими программистами

>300

пилотных внедрений

Резидент Сколково

>50

партнеров в странах СНГ

2014

с этого года ведется активная разработка

Включен в реестр отечественного ПО

10000

установок free-версии в мире в 2017-18 годах


КЛИЕНТЫ
ТФОМС
РЕСПУБЛИКА ТАТАРСТАН
РСХБ страхование
РАО ЭС ВОСТОКА
IBS DataFort
РОСНАНО
ПРИМ ТЕПЛО ЭНЕРГО
ДВФУ
ДАЛЬНЕВОСТОЧНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ
АктивБК
Пойдём!
Банк, который вам по душе
Modulbank
УНКОМТЕХ
www.uncomtech.ru
РОСЭКСИМБАНК
INTOUCH

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ

Глеб Косоруков
g.kosorukov@rusiem.com
+7 926 101 26 58