RUSIEM

Всё под контролем

РЕШЕНИЕ ДЛЯ КОНТРОЛЯ ВАШЕГО БИЗНЕСА

Эксперты: взлом JPMorgan может быть связан с Москвой

Главное

США и Великобритания обвинили шесть россиян в хакерских атаках на Олимпиаду

Владимир Козловский
Русская служба Би-би-си, Нью-Йорк

8 октября 2014

Американские эксперты по кибербезопасности всерьез обеспокоены взломом

British Airways компенсирует клиентам потери от хакерской атаки

Главное

США и Великобритания обвинили шесть россиян в хакерских атаках на Олимпиаду и выборы во Франции

8 сентября 2018

Хакеры взломали 380 тысяч транзакций британской авиакомпании B
Airways. Мошенникам стали известны номера кредитных карт покуп
авабилетов. Авиаперевозчик обязуется покрыть все убытки клиенто

Генеральный директор компании Алекс Круз принес извинения за ут

Данные производителя Jack Daniel's выставили на продажу за $1,5 млн в BTC

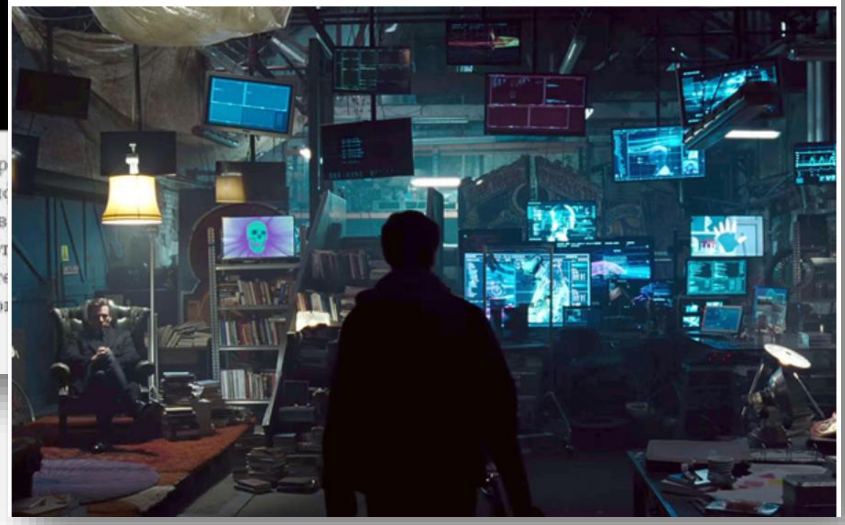
Хакеры взломали сервера корпорации Brown-Forman и предложили купить украденную информацию за криптовалюту. Ранее в компании заявили, что смогли предотвратить а

Хакеры выставили на продажу данные корпор
Forman, выпускающей виски Jack Daniel's. Конф
информация размещена в блоге преступников
позора» и продается за $1,5 млн в криптовалют
эксперт по кибербезопасности Филипп Дюарте
Cointelegraph. По его словам, в таких случаях о
в Bitcoin и Monero.

Встроились в систему

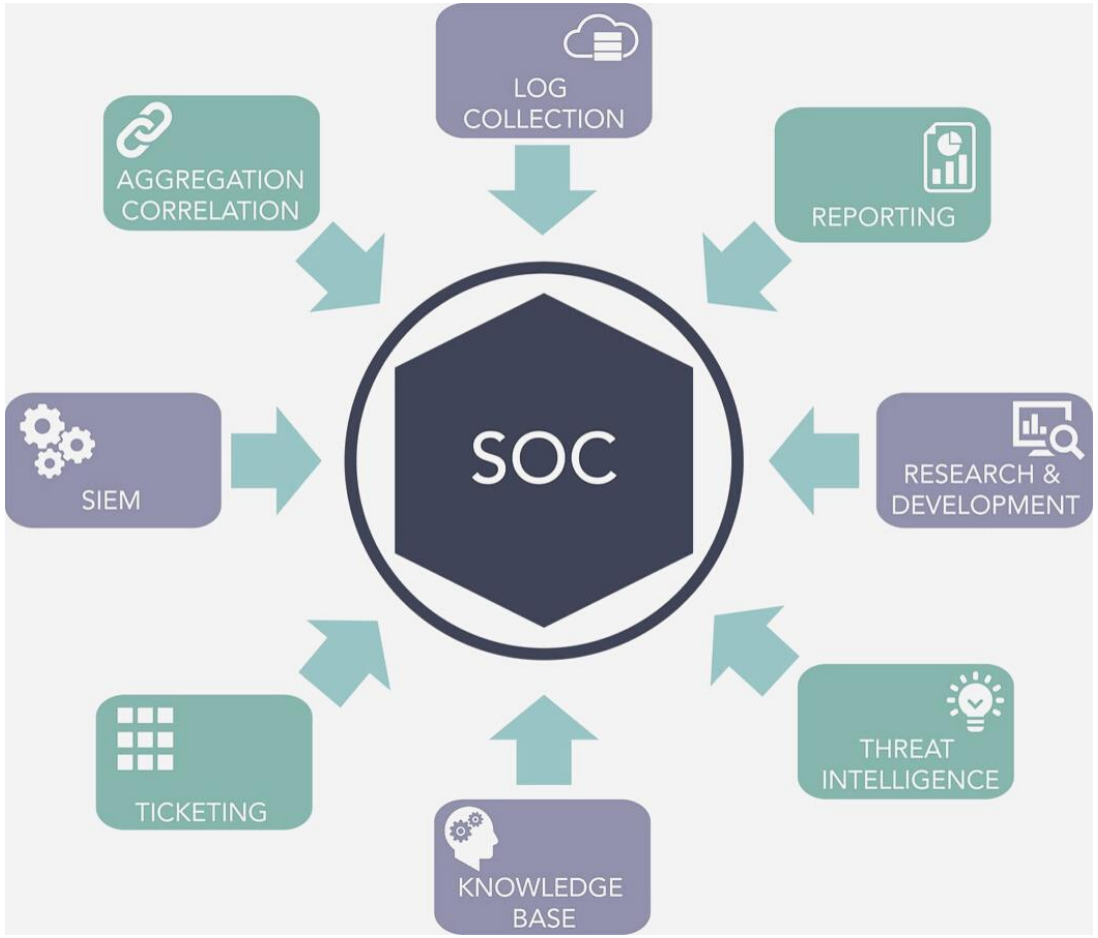
Самых опасных хакеров мира засекли в России. Они крадут миллиарды, и их не остановить

26 21 17 Добавить в «Мою Ленту»



RUSIEM
Всё под контролем


Все
нормально



ЧТО ТАКОЕ SOC?

Центр мониторинга и реагирования на инциденты информационной безопасности

*SOC - security operations center

RUSIEM
Всё под контролем

ЧТО ТАКОЕ SIEM И ЗАЧЕМ ОНА НУЖНА

SIEM - улучшенная система обнаружения вредоносной активности и различных системных аномалий. Позволяет увидеть более полную картину активности сети и событий безопасности. Когда обычные средства обнаружения, по отдельности, не видят атаки - **SIEM обнаружит! Благодаря тщательному анализу 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 - собирает, анализирует и представляет информацию из сетевых устройств, средств защиты информации и информационных систем.
В систему входят приложения для контроля идентификацией и доступом, инструменты управления уязвимостями

RUSIEM
Всё под контролем

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

RUSIEM
Всё под контролем

РЕШЕНИЕ

RUSIEM

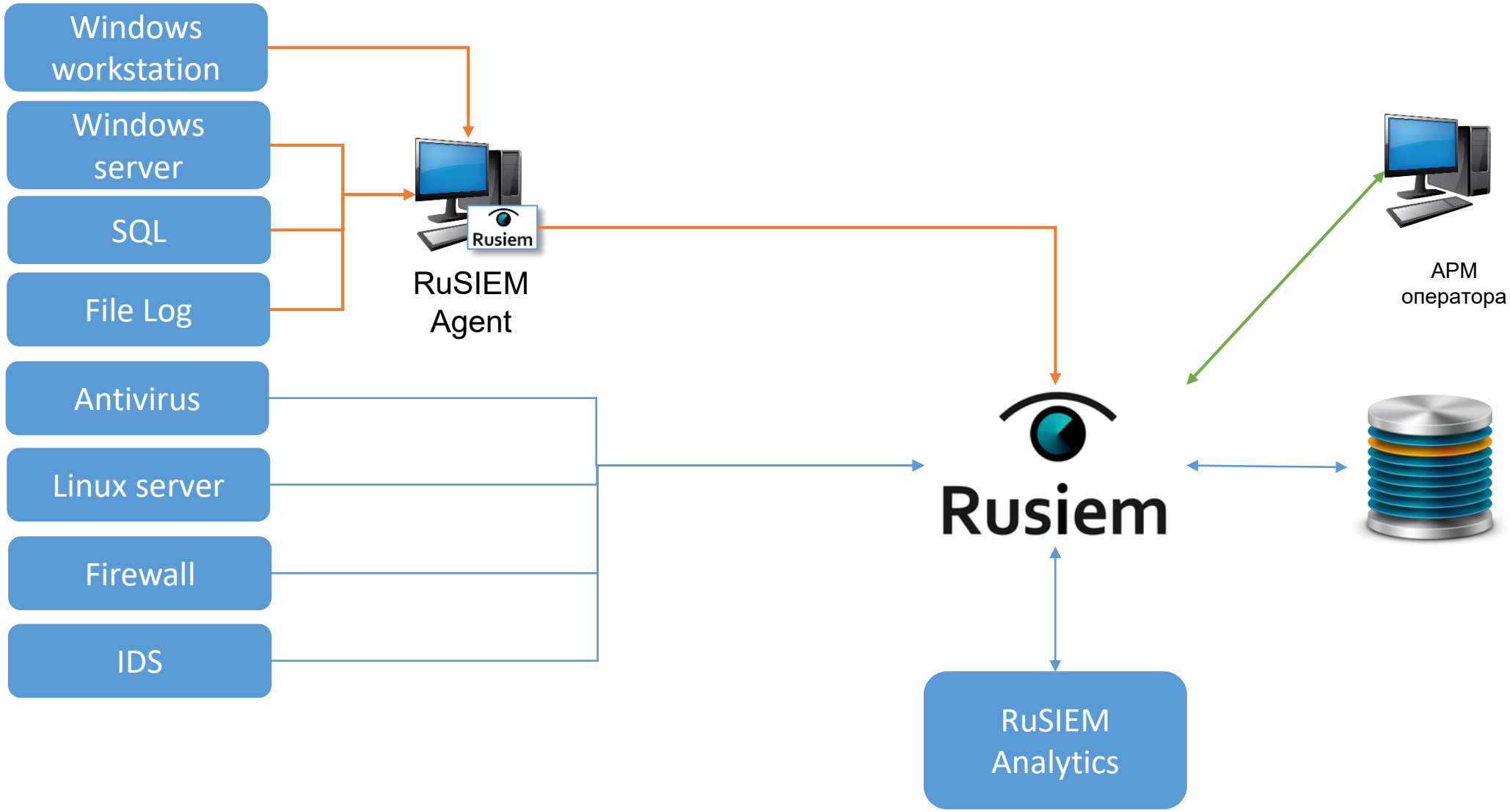
система мониторинга и управления событиями информационной безопасности на основе симптомов и анализа данных в реальном времени, для компаний любого масштаба

Линейка продуктов

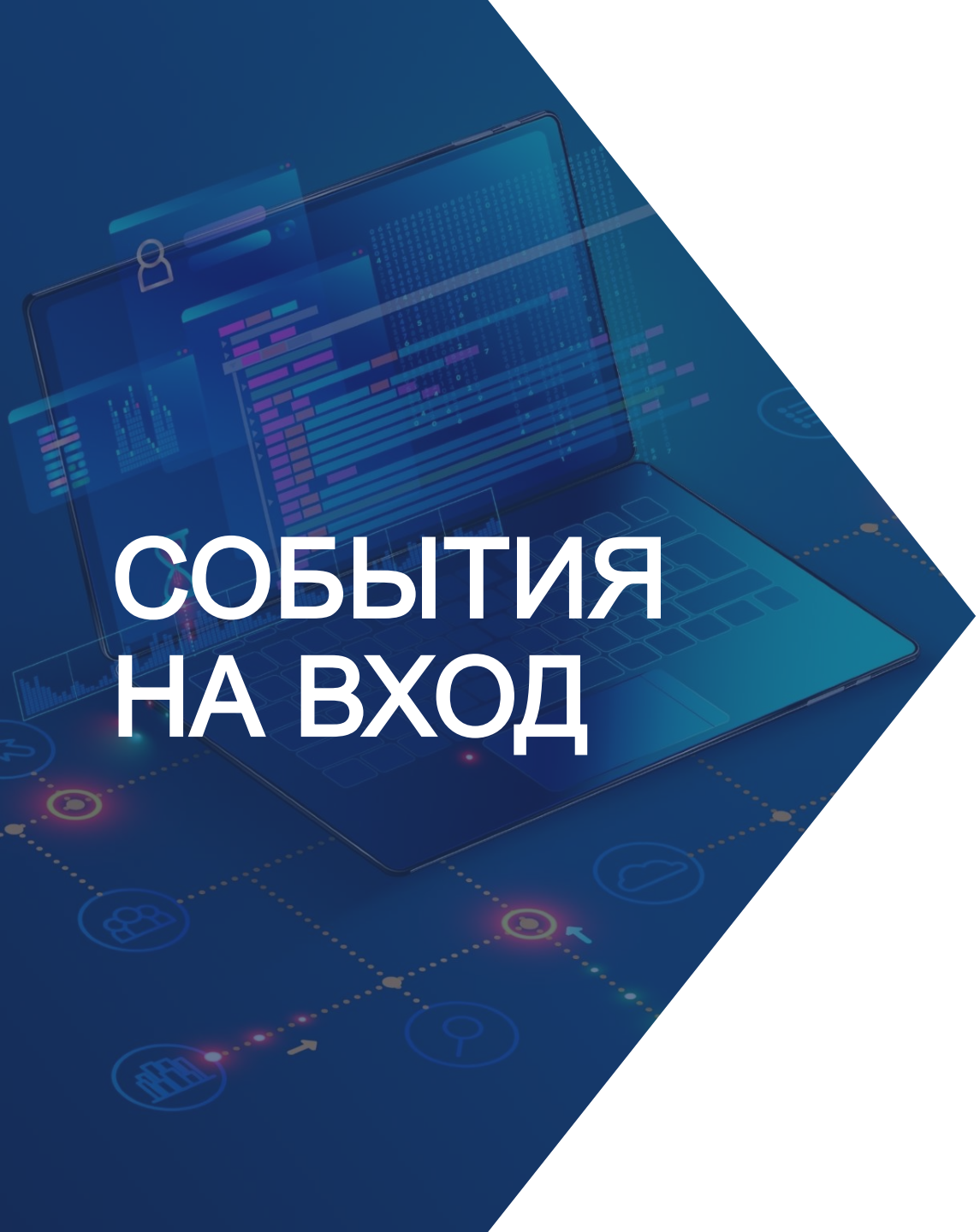
RvSIEM (free)
классическое решение класса LM

RuSIEM
Коммерческая версия

RuSIEM
Analytics



RUSIEM
Всё под контролем



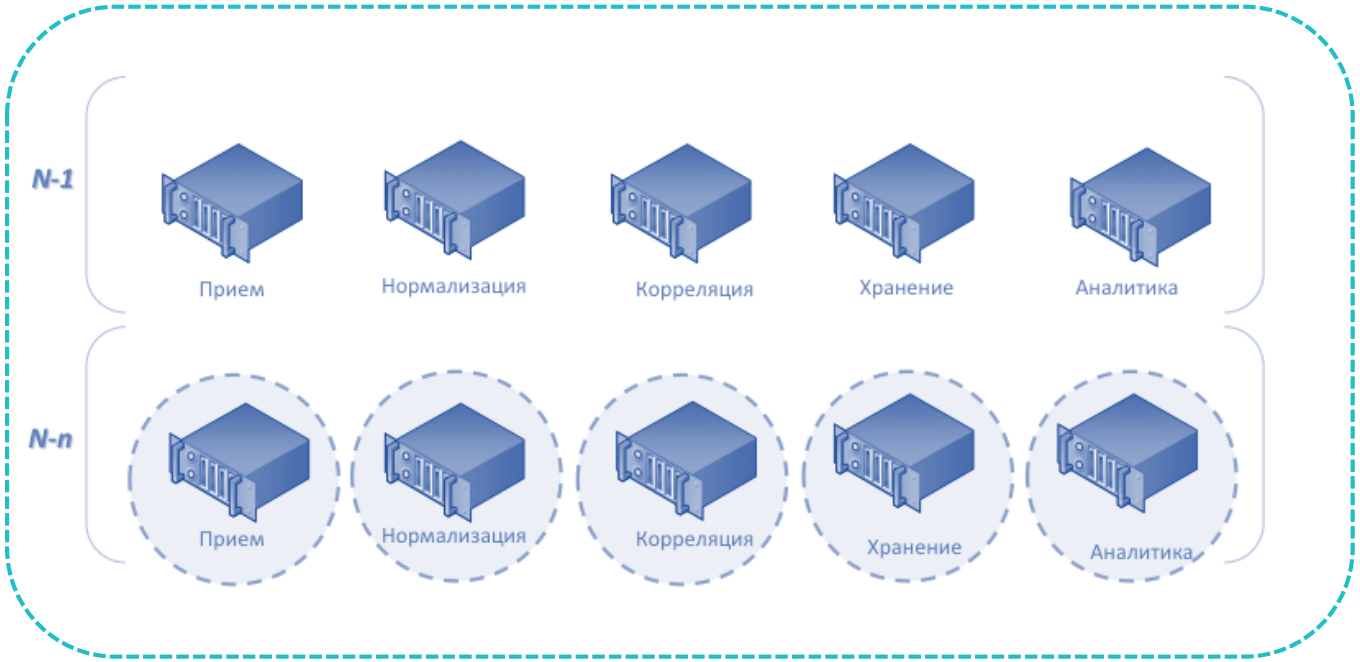
СОБЫТИЯ НА ВХОД

- 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

ЛЮБЫЕ

RUSIEM
Всё под контролем

МАСШТАБИРУЕМОСТЬ



Реальный рабочий кейс свыше 90000 EPS

- Вертикальное (филиалы) и горизонтальное (производительн
- «Горячее» расширение без оста
- Поддержка слабых каналов меж удаленными объектами
- Корреляция в центральном офи необходимости передачи всех с «наверх»
- Распределенный поиск по событ необходимости «единого хранил

RUSIEM
Всё под контролем

ПОЧЕМУ ВЫБИРАЮТ RuSIEM

SIEM: МИФЫ И РЕАЛЬНОСТЬ

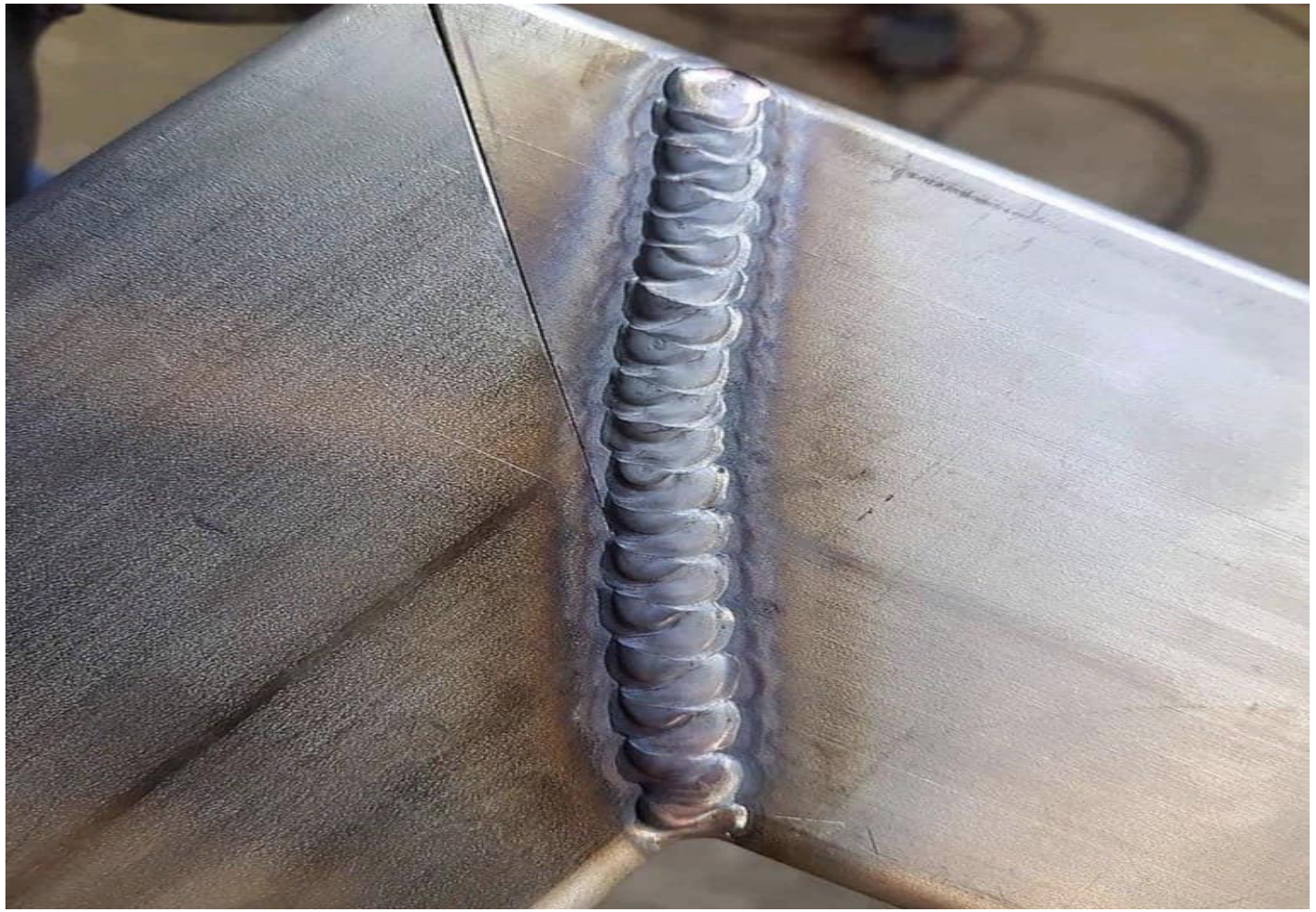
Стандартные вопросы и заблуждения

- Дорого?
- Нужен только в зрелой инфраструктуре?
- Сложно подключить не типовые источники?
- Необходим высококвалифицированный персонал?
- Нужна поддержка 24x7x365?
- Долго настраивать правила корреляций?

RUSIEM
Всё под контролем

Стандартные вопросы и заблуждения

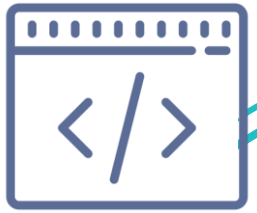
Да мы можем сами быстро сделать!



RUSIEM
Всё под контролем

О КОМПАНИИ

RUSIEM
Всё под контролем



программный код создан российскими программистами

300
пилотных внедрений

резидент ИЦ Сколково

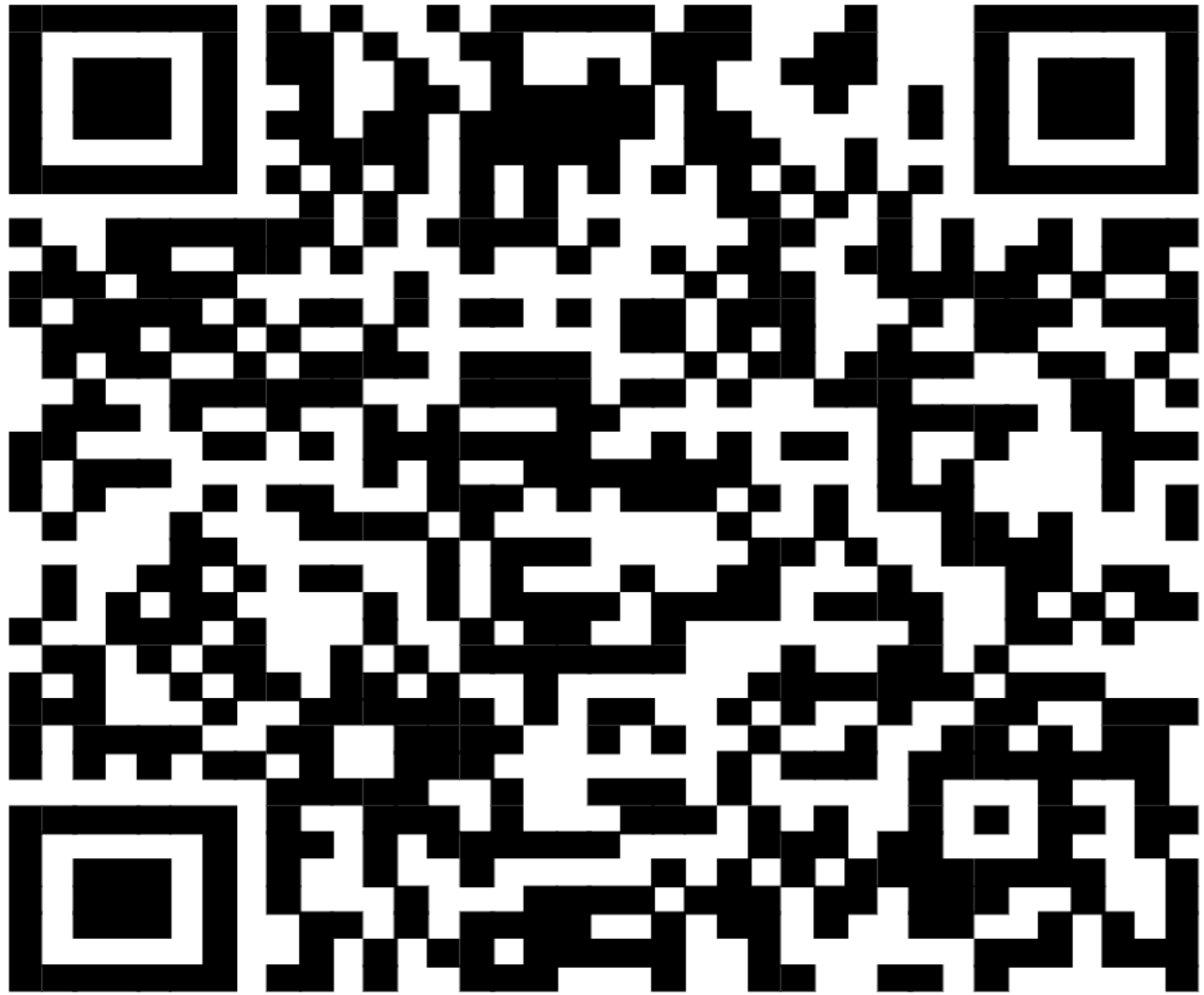
70
партнеров в РФ странах СНГ

2014
года ведется активная разработка

включен в реестр отечественного ПО лицензия ФСТЭК

15000
установок free-версий в мире с 2017 по 2019


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



RUSIEM
Всё под контролем

Помните, никогда не переходите по ссылкам, тем более полученных от неизвестного вам человека

Александр Учителев

a.uchitelev@rusiem.com
+7 916 372 04 40

www.rusiem.com

RUSIEM
Всё под контролем