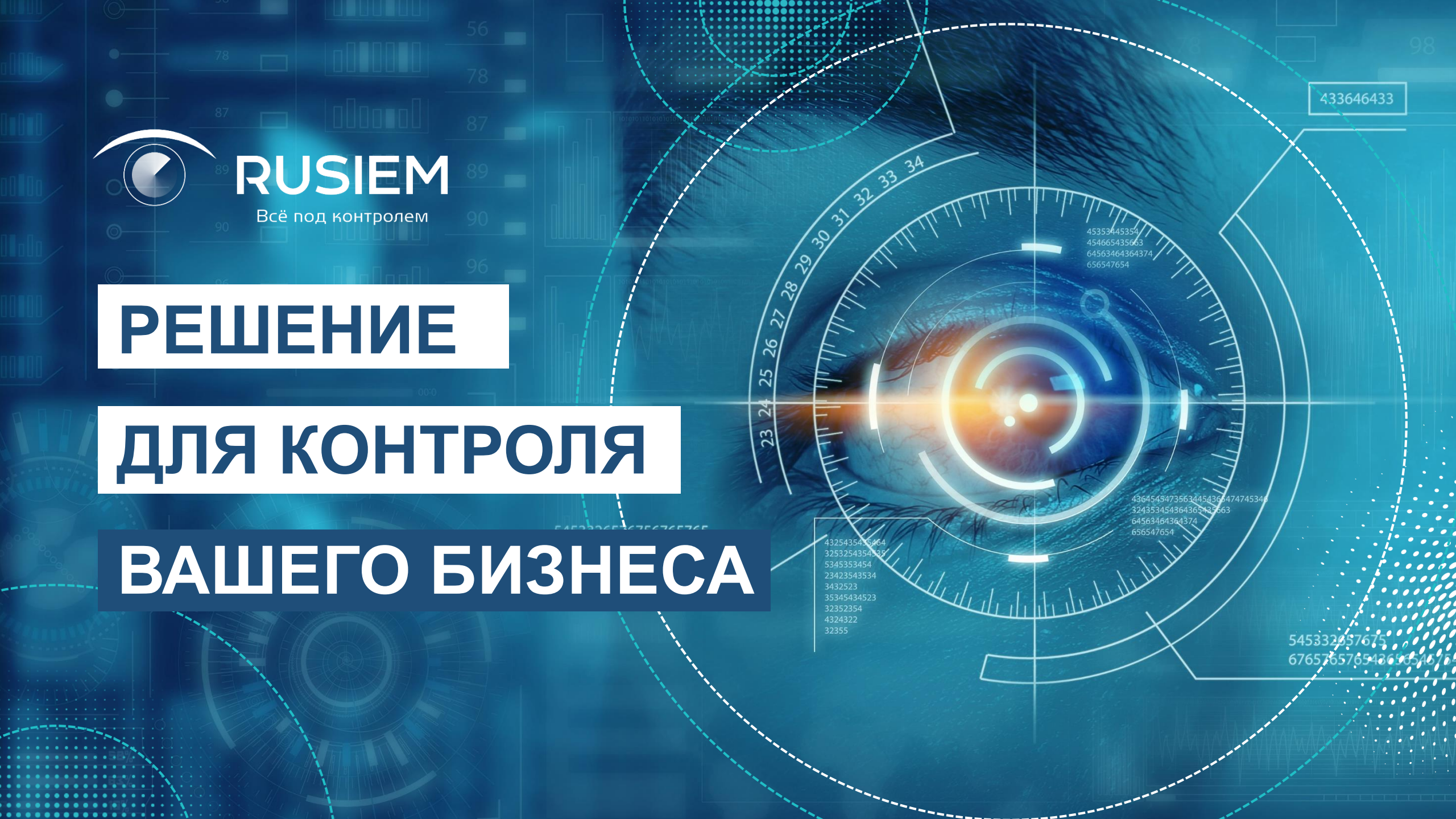
RUSIEM

Всё под контролем

РЕШЕНИЕ ДЛЯ КОНТРОЛЯ ВАШЕГО БИЗНЕСА



О КОМПАНИИ RUSIEM

Программный код создан российскими программистами

>300

пилотных внедрений

Резидент Сколково

>50

партнеров

2014

с этого года ведется активная разработка

Группа компаний Программный Продукт

входит в состав учредителей

ФСТЭК + реестр отечественного ПО

>10000

установок free-версии в мире в 2019-20 годах

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.

ТЕХНОЛОГИИ

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

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

3. Практическое использование AI и DL технологии

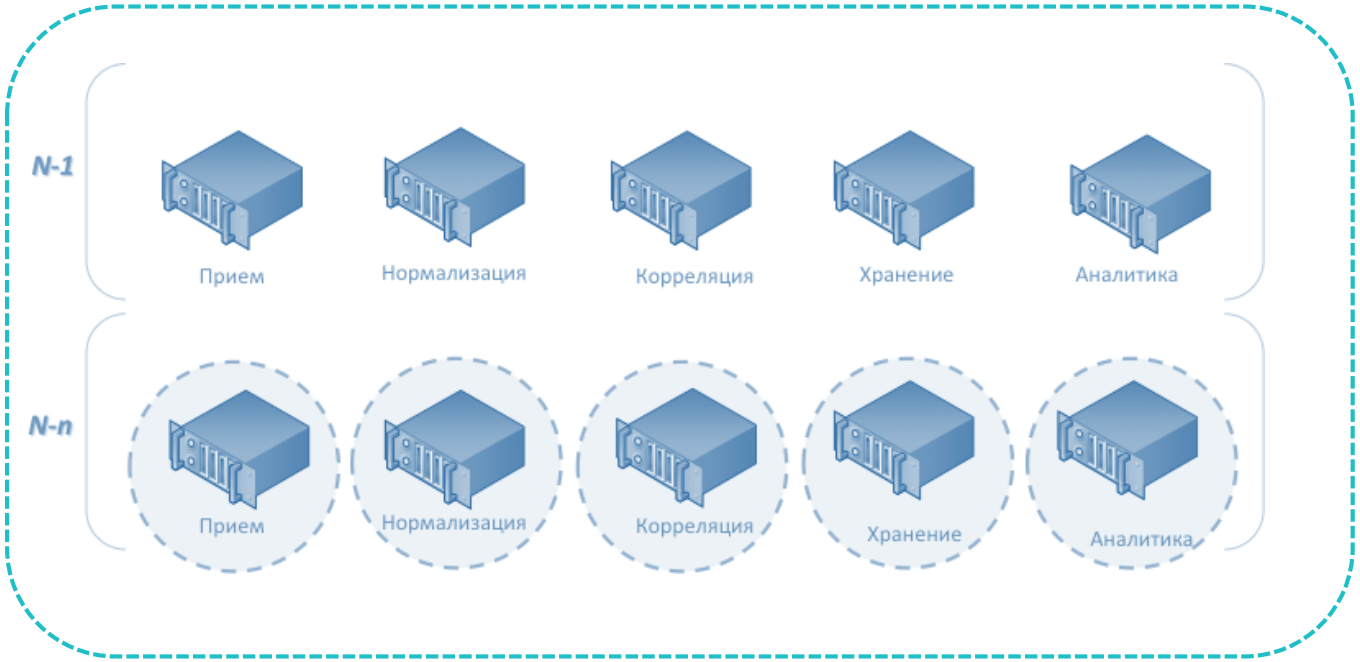
СОБЫТИЯ НА ВХОД

- Межсетевые экраны
- IPS
- DNS logs
- АСУТП
- СКУД
- Различные датчики
- Спам-фильтры
- Антивирусные системы
- Сетевые устройства
- Бизнес-приложения

ЛЮБЫЕ

- Windows event log
- Web servers
- App servers
- Load balancing
- Network flow
- Network payload
- Транзакции
- Почтовые системы

МАСШТАБИРУЕМОСТЬ



- Вертикальное (филиалы) и горизонтальное (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»

КОНКУРЕНТНЫЕ ПРЕИМУЩЕСТВА

Развитие системы

1. **IRP -> SOAR ->** Автоматизация реагирования
   Обогащение событий

2. **Управление активами** - сбор информации из различных сканеров, систем и событий, ручной ввод. Весовое разделение, использование активов в событиях и инцидентах. Связка с уязвимостями.

3. **Полноценная поддержка** TI - Stix\Taxii\Json, RestAPI, TTL (IOC)
   Упор на доработку производительности системы (меньше ресурсов, на тех же объёмах данных)
   Фильтрация
   Агрегация

4. **ML – DGA, UEBA**, Профилирование источников, автоматический парсинг…
   UX\UI


КЛИЕНТЫ
МЕДСИ
медицина компетенций
ТФОМС
РЕСПУБЛИКА ТАТАРСТАН
РСХБ страхование
РАО ЭС ВОСТОКА
РОСНАНО
Российская корпорация нанотехнологий
ПРИМ ТЕПЛО ЭНЕРГО
ДВФУ
ДАЛЬНЕВОСТОЧНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ
ЦОДД
Пойдём!
Банк, который вам по душе
КТ ГРУППА КРОНШТАДТ
INTOUCH
РОСЭКСИМБАНК
АктивБК
ActiveBusinessCollection
АКСОН

STORY TIME!

Заказчик выбрал наиболее производительное решение

Среди всех участников пилотов и конкурса только **RuSIEM** смог обеспечить поддержку более 80 000 тысяч событий, передаваемых со множества устройств заказчика, тем самым обеспечивая постоянный мониторинг важных городских систем.

Дополнительно пользуются услугами одного из крупнейших SOC-центров России. Среднее кол-во событий около 20000 - 30000 EPS

ЦОДД - Центр организации дорожного движения Правительства Москвы

STORY TIME!

Заказчика спасли от «вымогателей»

Инцидент со взломом всей сети у заказчика произошел накануне мартовских праздников, что потребовало дополнительных трудозатрат специалистов.

АКСОН

Благодаря слаженной работе экспертов обеих компаний, за 3 дня удалось не только развернуть RuSIEM, провести масштабную аналитику, выявить точки проникновения и зараженные узлы, но и полностью парализовать действия злоумышленников до полной защиты сети заказчика.

На текущий момент все источники событий заведены в SIEM, а мониторинг ИТ-инфраструктуры осуществляется в режиме 24x7.

Аксон - крупнейшая отечественная сеть DIY центрального федерального округа. Торговые центры более чем в 14 городах России.

STORY TIME!

Заказчик выбрал решение для построения своего SOC

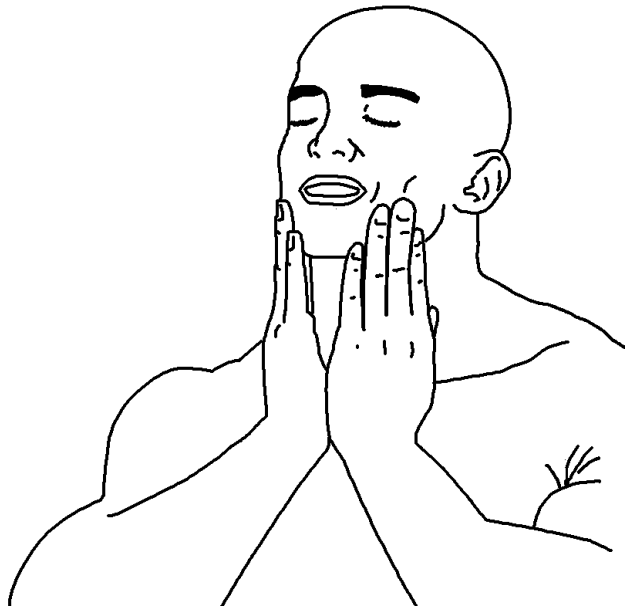
Число событий **> 10 000 EPS**
Сигналов тревоги **> 7 000 в час**
Инцидентов **> 50 в час**

ГБУ СО «СОЦИ» - Государственное бюджетное учреждение Сахалинской области «Сахалинский областной центр информатизации»

STORY TIME!

Заказчик самостоятельно стартовал пилот за 2 дня

Инженер одной из ДЗО ГК Росатом самостоятельно скачал с сайта rusiem.com бесплатную версию RvSIEM. После проведения пилота заказчик остался доволен и решил приобрести коммерческую версию **RuSIEM** на 10 000 EPS…



Росатом — российский государственный холдинг, объединяющий более 400 предприятий атомной отрасли

STORY TIME!

Заказчик на пилоте выявил «засланных казачков»

Один заказчик на пилоте поставил цель выяснить: есть ли сотрудники, которые физически не прошли в банк (не прошли через СКУД), но авторизовались на рабочих станций. В итоге оказалось, что несколько человек незаконно имели доступ ко внутренним ресурсам…

В результате **RuSIEM** был закуплен, далее проведено внутреннее расследование и привлечены к ответственности виновные

STORY TIME!

Заказчик на пилоте выявил «Таргетированную атаку»

Сценарий атаки был следующий:

1.В начале «неизвестный злоумышленник» провёл «разведку» в форме сканирования
2.На следующем этапе при помощи рассылки письма с зараженным вложением, произошёл запуск вредоносного кода на рабочей станции локальной сети.
3. Завершающий этап таргетированной атаки это исходящие HTTP соединение с одного из хостов локальной сети на адрес «неизвестного злоумышленника»

Данные действия, первоначально никак не связанные между собой, при корреляции событий с разных источников были идентифицированы RuSIEM как «таргетированная атака», которая была вовремя выявлена и остановлена.

В результате **RuSIEM** был закуплен, далее продукт был масштабирован на всю ГК.

Ответим на все вопросы – ОБРАЩАЙТЕСЬ!

Контактная информация:

Сайт : www.rusiem.com

Почта: info@rusiem.com

Телефон: +7(495)748-83-11