



Всё под контролем

**Практика  
Использования  
SIEM  
Кейс из жизни**

Максим Николаевич Степченков, совладелец RuSIEM

576756765765  
6767567656  
98785663576765574657

432543543564  
3255254354356  
5345353454  
23423543534  
3432523  
35245434523  
32352354  
4324322  
32355

45353445354  
494665435643  
64563464364374  
656547654

4965549473563445436447474534  
32435345436436243263  
64563464364374  
656547654

545332657675  
6765765765946676545765

433646433

23 24 25 26 27 28 29 30 31 32 33 34

# 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



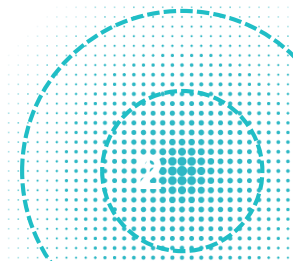
Для полной картины происходящего необходимо собрать воедино состояния с отдельных устройств



Для этого и нужна SIEM-система

**SIEM** – система, которая 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



# Инцидент. Хронология



# Что происходит?

**Была вероятность захвата сети  
злоумышленниками**

**Злоумышленники обещали  
привести в действие логическую  
бомбу 11 марта в 12:00**



# Инцидент. Расследование

## Развернули SIEM

- ✓ 30 минут на установку системы
- ✓ 2 часа на подключение основных источников

## Форензика зараженных узлов и сети

- ✓ Таймлайн и атрибуция атак

## Настройка логирования с дополнительных источников в SIEM

## Планирование блокировки заражения и защиты



### Результат

- Зараженные узлы и точки проникновения
- Много закладок с внешним доступом, WannaCryptor и др.
- Syn-flood в сети
- Golden Ticket
- Brute-Force и компрометация сервера партнеров

# Что было обнаружено?

**Следующим шагом за ручным анализом, после подключения основных источников был анализ с помощью SIEM**



## **Было обнаружено**

- Malware 9 шт.
  - The onion router 1 шт.
  - WanaCryptor 3 шт.
  - WannaCry Killswitch Domain HTTP Request 4 шт.
  - Сканеры уязвимостей 33 шт.
  - Брутфорс 8 шт.
  - Syn Flood в сети
  - Golden Ticket
  - Скомпрометированный сервер партнеров
- И множество иных, менее значимых инцидентов

# RuSIEM | Brute-Force



**Rusiem** | **Инциденты** | Инцидент 1206

Создание: 2021-03-10 03:14:09  
Дата обновления: 2021-03-10 03:15:54  
Фактического возникновения: 2021-03-10 03:12:46

Наименование инцидента: More than 1000 invalid access attempts within 1 hour and 1 ip

Категория инцидента: Брутфорс

Описание инцидента: Более 1000 неверных попыток доступа в течение 1 часа по 1 ip

Статус: Назначен | Приоритет: 1 | Объект: src.ip: 45.146.164.245

Назначено группам: Аналитик ИБ,Администратор

**Rusiem** | **Инциденты** | Инцидент 1376

Создание: 2021-03-10 03:14:30  
Дата обновления: 2021-03-10 03:15:54  
Фактического возникновения: 2021-03-10 03:12:48

Наименование инцидента: More than 1000 invalid access attempts within 1 hour and 1 ip

Категория инцидента: Брутфорс

Описание инцидента: Более 1000 неверных попыток доступа в течение 1 часа по 1 ip

Статус: Назначен | Приоритет: 1 | Объект: src.ip: 45.146.164.248

Назначено группам: Аналитик ИБ,Администратор

**Rusiem** | **Инциденты** | Инцидент 1377

Создание: 2021-03-10 03:14:30  
Дата обновления: 2021-03-10 03:15:54  
Фактического возникновения: 2021-03-10 03:12:48

Наименование инцидента: Time-distributed brute force with grouping by user name

Категория инцидента: Брутфорс

Описание инцидента: Более 1000 неверных попыток доступа в течение 1 часа по 1 ip

Статус: Назначен | Приоритет: 1 | Объект: user.name: Admin

Назначено группам: Аналитик ИБ,Администратор

**Инцидент 1206**

Наименование инцидента: More than 1000 invalid access attempts within 1 hour and 1 ip

Статус: Назначен | Приоритет: 1 | Объект: src.ip: 45.146.164.245

Назначено группам: Аналитик ИБ,Администратор

Источники		Назначение	
Исходный ip адрес	45.146.164.248 (1912), 45.146.164.245 (1444), 218.189.86.210 (94), 209.146.19.18 (7), 91.191.209.14 (6)	Конечный ip адрес	
Порт источника	57064 (4), 50828 (3), 49496 (3), 50753 (3), 59067 (3) <a href="#">Подробнее</a>	Порт назначения	
Имя источника		Имя конечного пользователя	
Имя хоста-источника событий	10.44.5.15 (3114)	Имя источника	
Имя хоста-источника событий	AH-SRV-037.akson.local (3114)	Имя конечного пользователя	

Источники		Назначение	
Исходный ip адрес	45.146.164.248 (1912), 45.146.164.245 (1444), 218.189.86.210 (94), 209.146.19.18 (7), 91.191.209.14 (6)	Эл.адрес отправителя	
Порт источника	57064 (4), 50828 (3), 49496 (3), 50753 (3), 59067 (3) <a href="#">Подробнее</a>	Имя исходного пользователя	AH-SRV-0375 (3167)
Имя источника		Имя конечного пользователя	
Имя хоста-источника событий	10.44.5.15 (3114)	Имя конечного пользователя	
Имя хоста-источника событий	AH-SRV-037.akson.local (3114)	Имя конечного пользователя	

Источники: 10.44.5.15 (3114), AH-SRV-037.akson.local (3114)

Назначение: 10.44.5.15 (3114), AH-SRV-037.akson.local (3114)

Имя источника: AH-SRV-0375 (3167)

Имя конечного пользователя: AH-SRV-0375 (3167)

Категория симптома: Неуспешный вход windows (3114), Тип входа/выхода (3114)

Идентификатор симптома: MS Windows: Отказ входа в систему. (3114), RDP доступ (3109), Сетевой доступ (7), MS Windows: Интерактивный (вход с клавиатуры или экрана системы) (2)

Показать: 10

Первая < > Последняя

Вернуться | Просмотр истории | Просмотр правил | Сохранить инцидент

# RuSIEM | WannaCryptor



**Rusiem** | RUSSIA | Выберите ноду

**Инциденты**  
Инцидент 8251  
Создания: 2021-03-30 09:40:45  
Дата обновления: 2021-03-30 09:40:45  
Фактического возникновения: 2021-03-30 09:40:37

Наименование инцидента: WannaCryptor C&C servers detected  
Категория инцидента: Malware  
Описание инцидента:

Статус: Назначен  
Назначено группам: Оператор

**Инцидент 8252**  
Создания: 2021-03-30 09:46:04  
Дата обновления: 2021-03-30 09:47:21  
Фактического возникновения: 2021-03-30 09:45:55

Наименование инцидента: WannaCryptor C&C servers detected  
Категория инцидента: Malware  
Описание инцидента:

Статус: Назначен  
Назначено группам: Оператор

**Инцидент 8076**  
Создания: 2021-03-24 11:38:38  
Дата обновления: 2021-04-11 09:58:48  
Фактического возникновения: 2021-03-24 11:38:32

Наименование инцидента: WannaCry Killswitch Domain HTTP Request  
Категория инцидента: Malware  
Описание инцидента:

Статус: Назначен  
Назначено группам: Оператор, Аналитик ИБ, Администратор

**Инцидент 8149**  
Создания: 2021-03-25 11:42:50  
Дата обновления: 2021-04-08 14:53:58  
Фактического возникновения: 2021-03-25 11:42:57

Наименование инцидента: WannaCry Killswitch Domain HTTP Request  
Категория инцидента: Malware  
Описание инцидента:

Статус: Назначен  
Назначено группам: Оператор, Аналитик ИБ, Администратор

Приоритет: 1  
Объект: src.ip: 192.168.50.44

Источники	
Исходный IP адрес	192.168.50.44 (ip)
Порт источника	49157 (nl), 49155 (nl), 49156

Назначение	
Конечный IP адрес	104.17.244.81 (nl), 104.16.173.80 (nl)
Порт назначения	80 (nl)
Эл. адрес получателя	
Имя конечного пользователя	

Источники событий	
IP источника событий	172.30.1.254 (nl)
Имя хоста-источника событий	tp01-zenlog (nl)
Категория симптома	
Идентификатор симптома	

События инцидента

Вернуться | Просмотр истории | Просмотр правил | Сохранить инцидент



# RuSIEM | Сканеры уязвимостей



The screenshot displays the RuSIEM interface with two incident detail windows and a modal window. The modal window for Incident 7963 is highlighted with a red border.

**Incident 7965 Details:**

- Наименование инцидента: Соединение более чем на 20 уникальных портов за 60 секунд
- Статус: Назначен
- Приоритет: 2
- Объект: src.ip: 10.100.10.2
- Назначено группам: Аналитик ИБ, Администратор
- Создания: 2021-03-12 07:01:11
- Дата обновления: 2021-04-11 22:11:45
- Фактического возникновения: 2021-03-12 06:44:11

**Incident 7963 Details (Modal Window):**

- Наименование инцидента: Соединение более чем на 20 уникальных портов за 60 секунд
- Статус: Назначен
- Приоритет: 2
- Объект: src.ip: 10.100.10.3
- Назначено группам: Аналитик ИБ, Администратор
- Создания: 2021-03-12 01:31:02
- Дата обновления: 2021-04-12 10:32:16
- Фактического возникновения: 2021-03-12 01:13:51

**Incident 7963 Details (Background Window):**

- Наименование инцидента: Соединение более чем на 20 уникальных портов за 60 секунд
- Статус: Назначен
- Приоритет: 2
- Объект: src.ip: 10.100.10.3
- Назначено группам: Аналитик ИБ, Администратор

**Task List (Background Window):**

ID задачи	Время назначения	Описание
Записи с 0	0	0 из 0 записей

**Source Information (Background Window):**

Исходный IP адрес	Порт источника
10.100.10.3 (1470488)	53 (1378902), 138 (7578), 137 (902), 3389 (831), 62490 (86)

**Destination Information (Background Window):**

Конечный IP адрес	Порт назначения
10.100.10.205 (1458737), 10.100.10.255 (8480), 192.168.80.213 (832), 10.110.5.75 (174)	3515 (83016), 138 (7578), 137 (902), 63897 (832), 45930 (220)

**Event Source Information (Background Window):**

IP источника событий	Имя хоста-источника событий
127.0.0.1 (1467217), 172.30.1.254 (8271)	rusiem (1467217), ip01-sensor (8271)

**Symptom Information (Background Window):**

Категория симптома	Идентификатор симптома
Блокированные/фильтрованные соединения (1467217)	Блокированное соединение (iptables) (1467217)

**Navigation Buttons:** Вернуться, Просмотр истории, Просмотр правил, Сохранить инцидент

# RuSIEM | Всего найдено

**Rusiem** RUS Выберите ноду

Инциденты

Мои инциденты | Все инциденты | Закрытые

Группировать по: Категория | Кол-во: 99

Статус: | Поиск

Показать: 100

**Статусы**

- Назначен: 8434
- Другие: 0

**Приоритет**

- 1: 117
- 3: 5138
- 5: 32
- 2: 3147

ID	Наименование	Категория	Приоритет	Статус	Назначен	Исполнитель	Объект	Суммарный вес симптомов	Количество событий	Дата создания	Дата изменения
	Malware (9)										
	Rusiem (46)										
	The Onion Router (TOR) (1)										
	Windows (32)										
	Аномалии (121)										
	Аудит (24)										
	Аутентификация (1)										
	Аутентификация и авторизация (67)										
	Брутфорс (8)										
	Входы/выходы (2829)										
	Нарушение политик (232)										
	Общие web атаки (1)										
	Отслеживающее ПО (24)										
	Сбои в инфраструктуре (177)										
	Сканеры уязвимостей (39)										
	Средства удаленного администрирования (48)										
	Угрозы (88)										
	Управление учетными записями и группами (4662)										

Записи с 1 по 18 из 18 записей

**Кол-во:** 99

**Статусы**

- Назначен: 8434
- Другие: 0

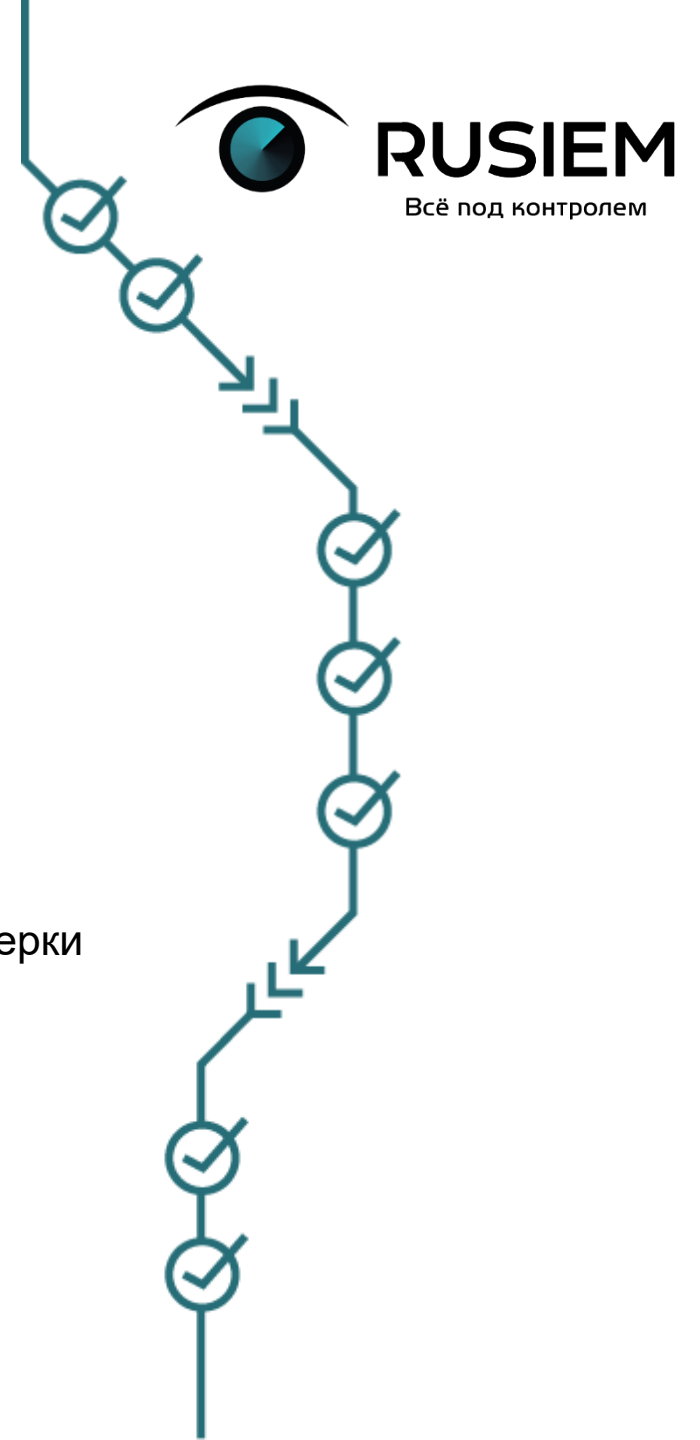
**Приоритет**

- 1: 117
- 3: 5138
- 5: 32
- 2: 3147

Категория | Приоритет | Статус | Назначен | Исполнитель | Объект

# Реагирование и защита

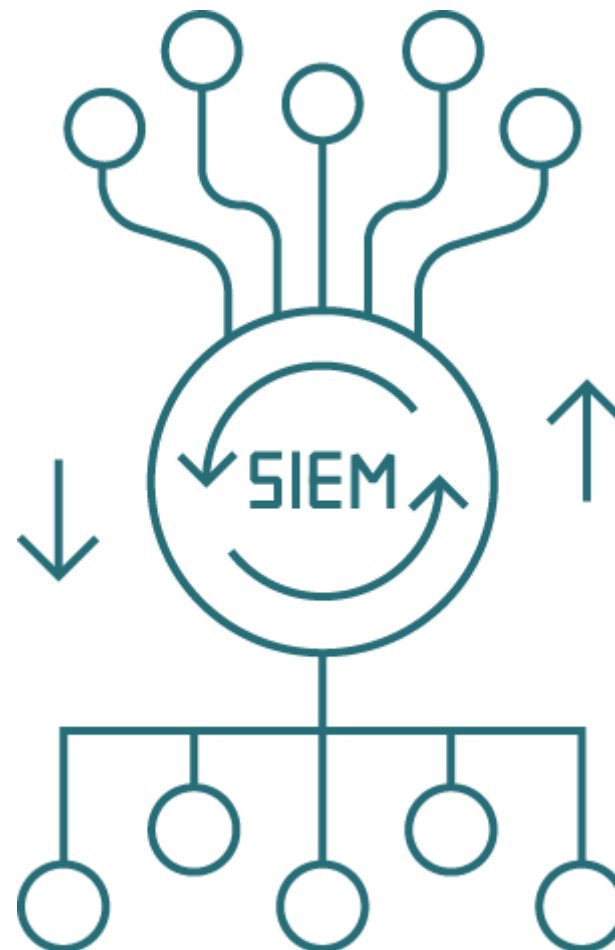
- Контроль всех инцидентов в SIEM
- Закрыли все точки входа, оставили 1 – центральную
- Была перенастроена сеть по правилу: все, что не разрешено, то запрещено
- Доступ только к бизнес-критичному сервису
- Бэкап всех критичных сервисов на внешнее хранилище
- Новая, защищенная доменная инфраструктура
- Изолированная инфраструктура, куда переносятся узлы после тщательной проверки
- Зараженные узлы выводятся из сети и обнуляются



# Текущая ситуация

## Сегодня 22 апреля

- Благодаря проделанной работе удалось полностью отразить атаку злоумышленников
- Составлен план последующих действий
- Новая доменная инфраструктура с чистыми хостами
- Процедура архивации
- Единая точка входа
- NGFW для контроля периметра
- Все источники в SIEM и инциденты мониторятся
- Усиленная политика ИБ и парольная политика



# Где может применяться SIEM?



Везде, где из журналов событий можно извлечь полезную информацию

## ПРИМЕРЫ СОБЫТИЙ

- Сетевые атаки
- Шифрование файлов
- Откуда и когда блокировались учетные записи
- Изменение конфигураций «не админами»
- Выявление несанкционированных сервисов
- Отсутствие антивирусной защиты на новом установленном компьютере
- Контроль выполняемых команд на серверах и сетевом оборудовании
- Аудит изменений конфигураций (сетевых устройств, приложений, ОС)
- Повышение привилегий
- 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 атак
- Влияние отказа в инфраструктуре на бизнес-процессы

# Линейка продуктов RuSIEM



**RuSIEM** — система мониторинга и управления событиями информационной безопасности на основе симптомов и анализа данных в реальном времени, для крупных и средних компаний

---

**RvSIEM  
(free)** –  
классическое  
решение  
класса LM

---

**RuSIEM**  
коммерческая  
версия

---

**RuSIEM  
Analytics**

---

**RuSIEM  
Agent**  
– агент под  
Windows OS

# SIEM vs LM



## LM | RvSIEM (free)

Сбор событий  
с источников

Отчеты

Поиск по  
событиям

Корреляция LM

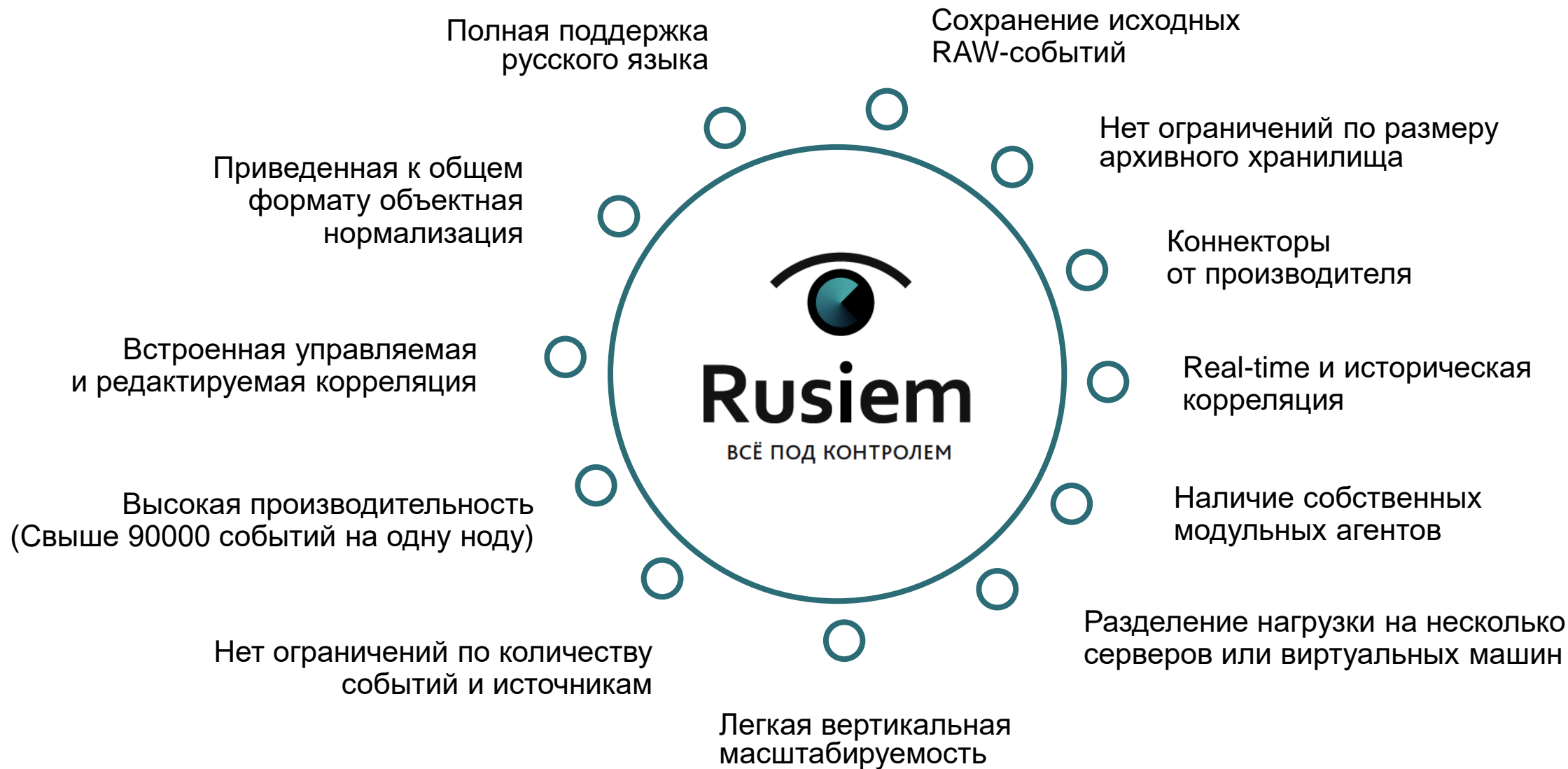
Инцидент-  
менеджмент

Риск-  
менеджмент

Аналитика

## SIEM | RuSIEM

# Конкурентные преимущества





# 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



Продукт включен в  
реестр  
отечественного ПО

**10000**

установок free-версии  
в мире в 2017-18 годах

# Клиенты





Спасибо  
за внимание!

**Ответим на все вопросы  
Обращайтесь!**

Контактная информация:

Сайт : [www.rusiem.com](http://www.rusiem.com)

Почта: [info@rusiem.com](mailto:info@rusiem.com)

Телефон: +7(495)748-83-11

