



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



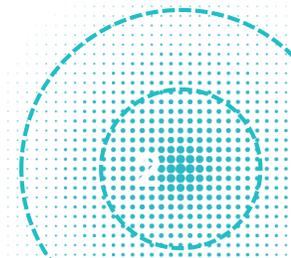
Для полной картины происходящего необходимо собрать воедино состояния с отдельных устройств



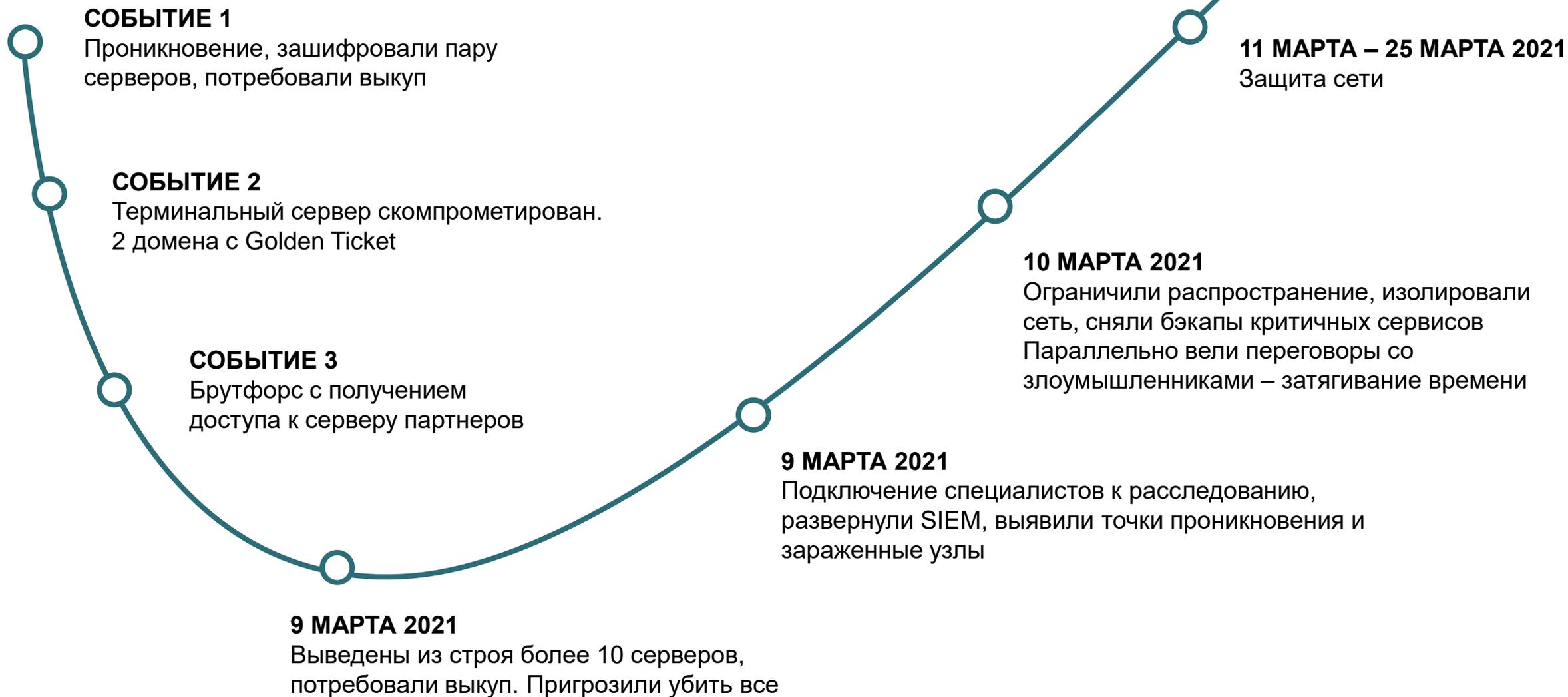
Для этого и нужна SIEM-система

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

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

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

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

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

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

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

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

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

Инциденты | **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 (144), 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) Подробнее	Порт назначения	
Имя источника		Имя конечного пользователя	
Имя хоста-источника событий	10.44.5.15 (3114)	Имя источника пользователя	
Имя хоста-источника событий	AH-SRV-037.akson.local (3114)	Имя конечного пользователя	
		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)

Первая < > Последняя

Показать: 10

Вернуться | Просмотр истории | Просмотр правил | Сохранить инцидент

RuSIEM | WannaCryptor



The screenshot displays the RuSIEM web interface with a focus on incident details. The interface is in Russian and shows a list of incidents on the left and a detailed view of incident 8149 in the foreground.

Incident 8149 Details:

- Инцидент 8149**
- Наименование инцидента:** WannaCry Killswitch Domain HTTP Request
- Статус:** Назначен
- Приоритет:** 1
- Объект:** src.ip: 192.168.50.44
- Назначено:** группам: Оператор, Аналитик ИБ, Администратор

Source Information:

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

Destination Information:

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

Event Source Information:

IP источника событий	Имя хоста-источника событий	Категория симптома	Идентификатор симптома
172.30.1.254 (nl)	ip01-zenlog (nl)		

At the bottom of the interface, there are navigation buttons: [← Вернуться](#), [🕒 Просмотр истории](#), [🔍 Просмотр правил](#), and [💾 Сохранить инцидент](#).

RuSIEM | Сканеры уязвимостей



The screenshot displays the RuSIEM web interface. The top navigation bar includes the RuSIEM logo, a language dropdown set to 'RUS', and a 'Выберите ноду' (Select node) button. The main content area is divided into several sections:

- Incident 7965 (top):** Shows the title 'Инцидент 7965', a description 'Соединение более чем на 20 уникальных портов за 60 секунд', status 'Назначен', priority '2', and object 'src.ip: 10.100.10.2'. It also lists the assignee as 'Аналитик ИБ.Администратор' and provides creation and update timestamps.
- Incident 7963 (middle):** Shows the title 'Инцидент 7963', the same description, status 'Назначен', priority '2', and object 'src.ip: 10.100.10.3'. The assignee is also 'Аналитик ИБ.Администратор'.
- Tasks (Задачи) section:** A table with columns for 'ID задачи', 'Время назначения', and 'Описание'. It shows a list of tasks with their respective IDs and descriptions.
- Source (Источник) section:** A table with columns for 'Исходный ip адрес', 'Порт источника', and 'Имя хоста-источника событий'. It lists source IP addresses and ports.
- Destination (Назначение) section:** A table with columns for 'Конечный ip адрес', 'Порт назначения', and 'Имя конечного пользователя'. It lists destination IP addresses and ports.
- Symptom (Симптом) section:** A table with columns for 'Категория симптома' and 'Идентификатор симптома'. It lists symptom categories and identifiers.

At the bottom right, there is a navigation bar with buttons: 'Вернуться', 'Просмотр истории', 'Просмотр правил', and 'Сохранить инцидент'.

RuSIEM | Всего найдено

Rusiem RUS Выберите ноду

Инциденты

Мои инциденты | Все инциденты | **Закрытые** 8433

Группировать по: Категория Ж 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)										
	Сбой 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

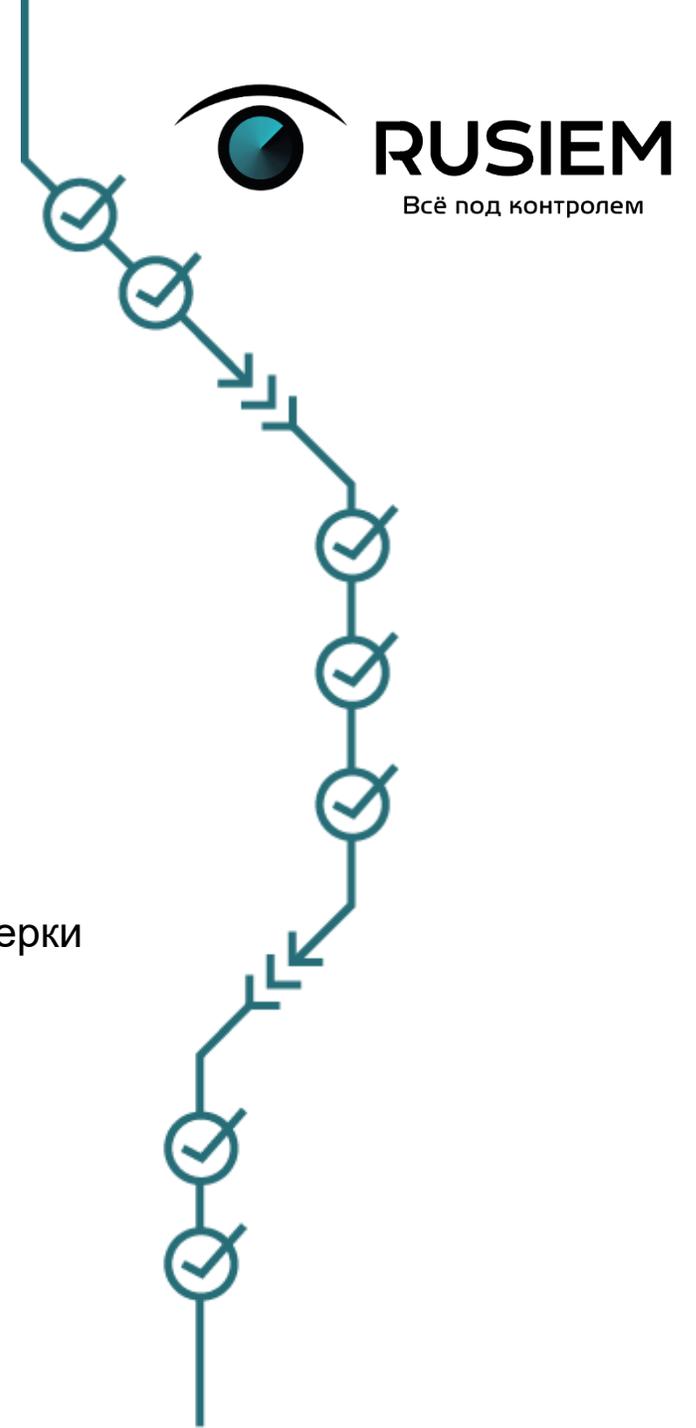
Приоритет

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

Категория | Приоритет | Статус | Назначен | Исполнитель | Объект

Реагирование и защита

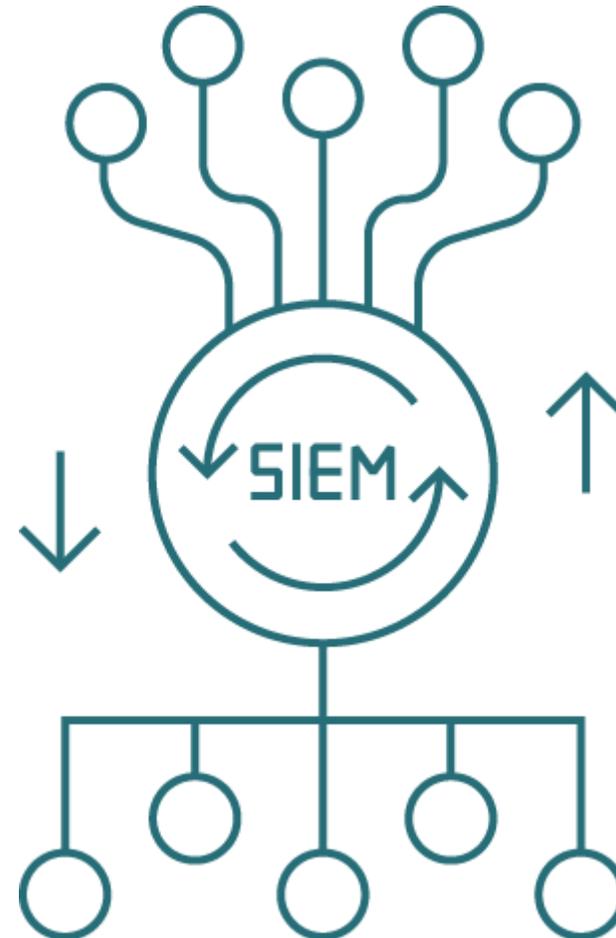
- Контроль всех инцидентов в SIEM
- Закрыли все точки входа, оставили 1 – центральную
- Была перенастроена сеть по правилу: все, что не разрешено, то запрещено
- Доступ только к бизнес-критичному сервису
- Бэкап всех критичных сервисов на внешнее хранилище
- Новая, защищенная доменная инфраструктура
- 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

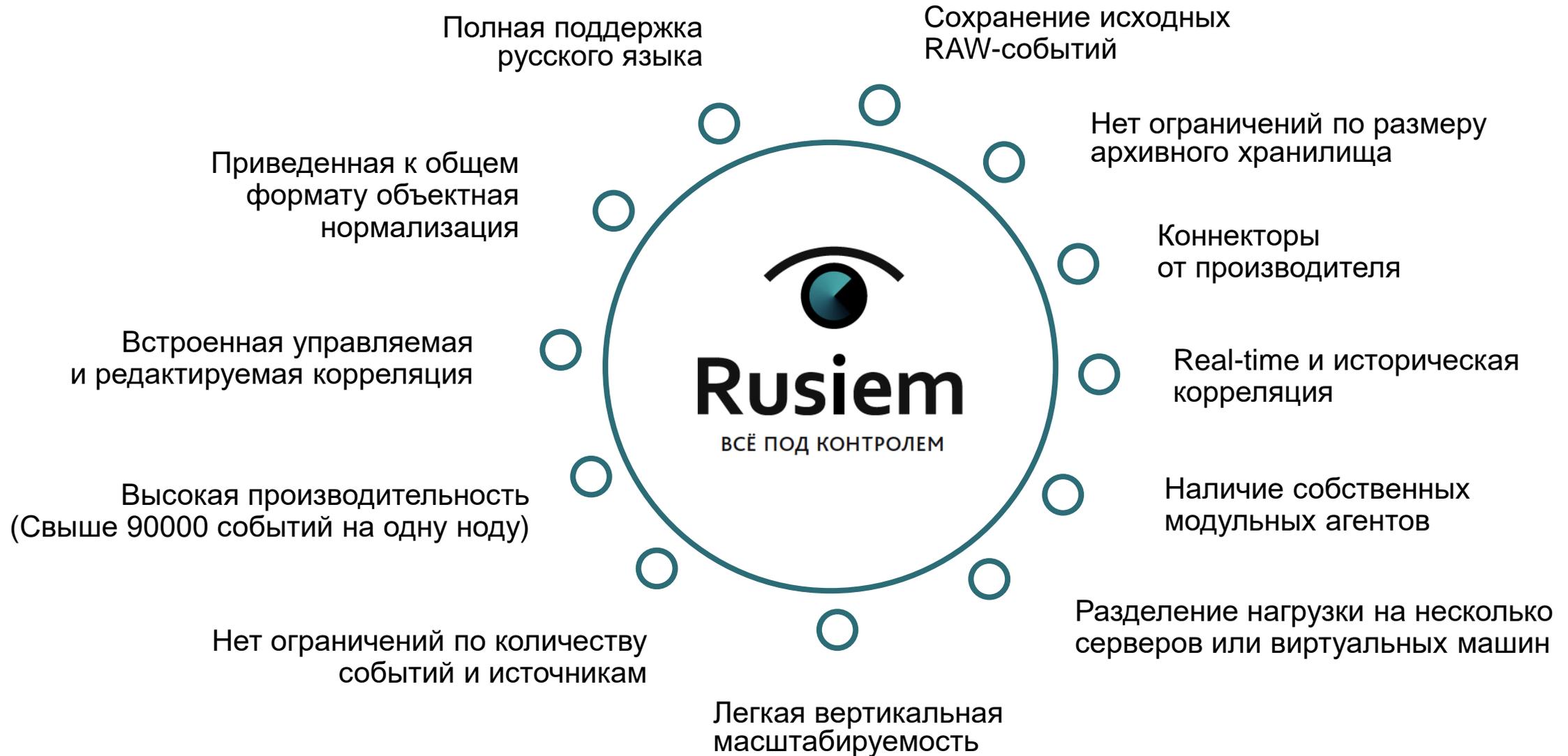
Инцидент-
менеджмент

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

Почта: info@rusiem.com

Телефон: +7(495)748-83-11

