RUSIEM

Всё под контролем

SIEM критично не только для КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

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.

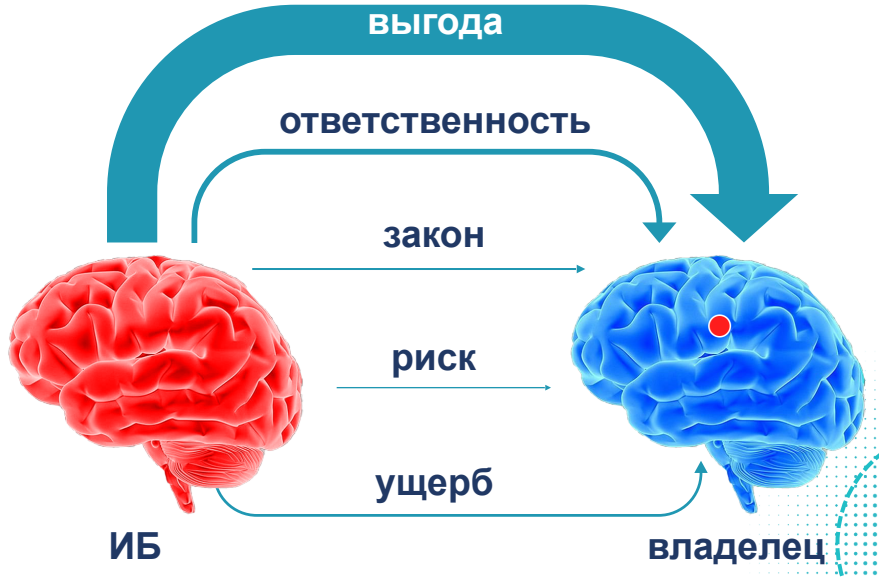
Сотни и тысячи устройств живут своей жизнью и генерируют миллионы событий, сообщая о том, что происходит с ними и вокруг. При этом необходимо реагировать только на часть из них.

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.



Приказ ФСТЭК №239

Приказ ФСТЭК от 25.12.2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

	Категория значимости 3	Категория значимости 2	Категория значимости 1
АУД.4 Регистрация событий безопасности	✓	✓	✓
АУД.6 Защита информации о событиях безопасности	✓	✓	✓
АУД.7 Мониторинг безопасности	✓	✓	✓
АУД.8 Реагирование на сбои при регистрации событий безопасности	✓	✓	✓
ИНЦ.1. Выявление компьютерных инцидентов.	✓	✓	✓
ИНЦ.2. Информирование о компьютерных инцидентах	✓	✓	✓
ИНЦ.3. Анализ компьютерных инцидентов.	✓	✓	✓
ИНЦ.4. Устранение последствий компьютерных инцидентов	✓	✓	✓
ИНЦ.6. Хранение и защита информации о компьютерных инцидентах.	✓	✓	✓

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

РЕШЕНИЕ

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

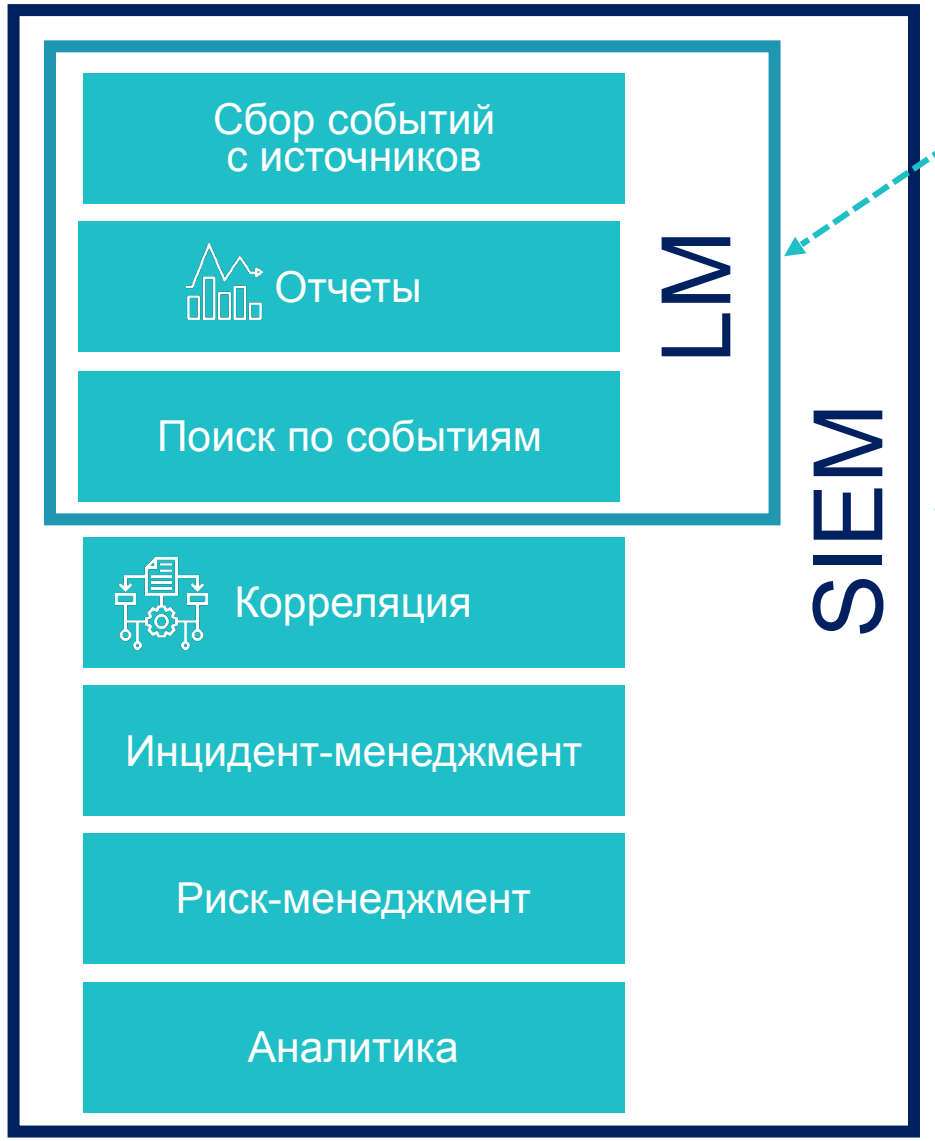
RuSIEM Analytics

RuSIEM Agent – агент под Windows OS

RuSIEM Replicator – утилита для массовой установки и управления агентами

Линейка продуктов

SIEM vs LM



RvSIEM(free)

RUSIEM

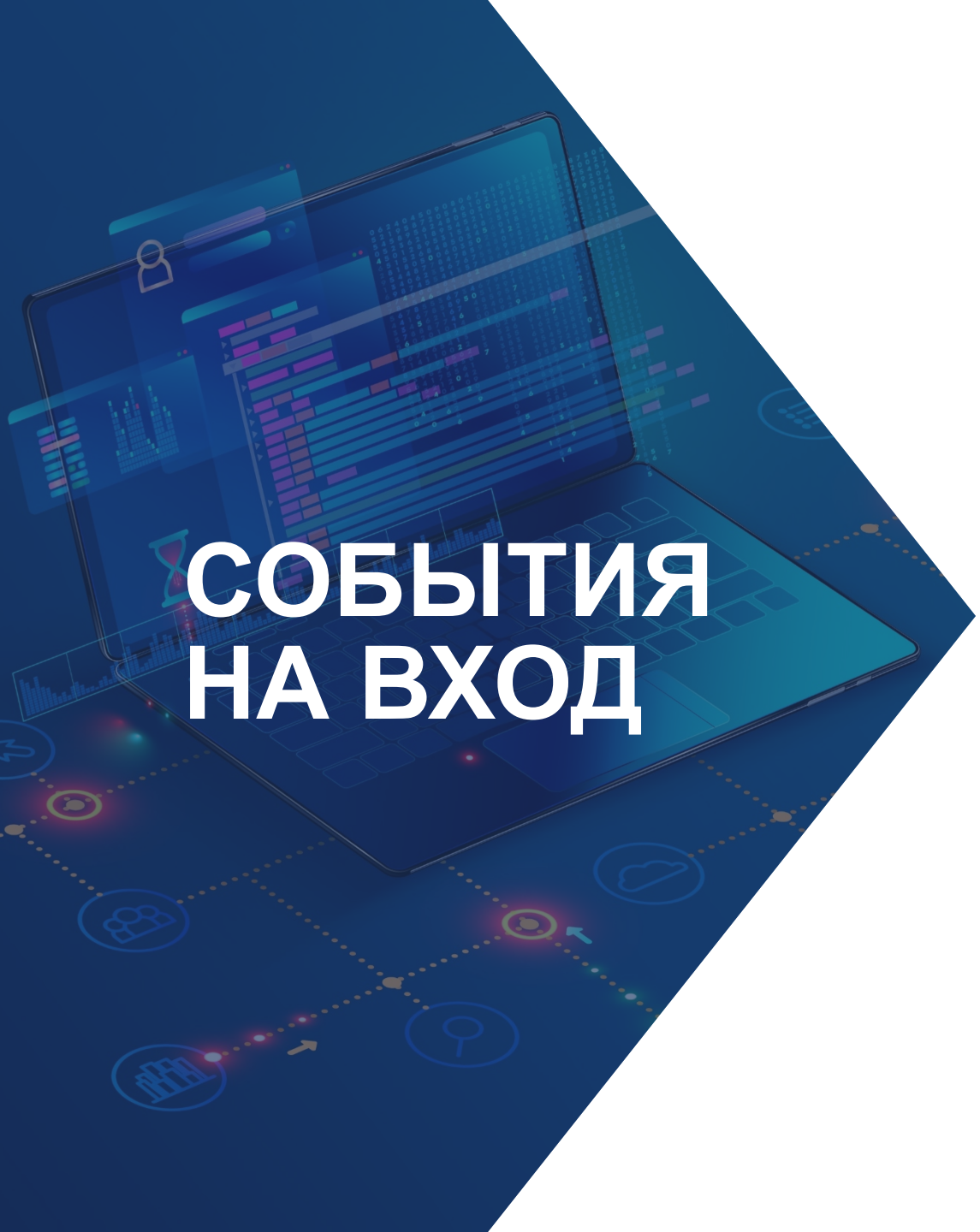
	RuSIEM	RuSIEM Analytics	RvSIEM (free)
Дашборды (набор виджетов для оценки показателей в режиме реального времени)	✓	✓	✓
Поиск по событиям	✓	✓	✓
Сохраненные запросы	✓	✓	✓
RBR (rule-based) корреляция	✓	✓	
Инцидент менеджмент по ITIL	✓	✓	
Симптоматика для тегирования событий понятным описанием	✓	✓	✓
Риск-метрики	✓	✓	✓
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

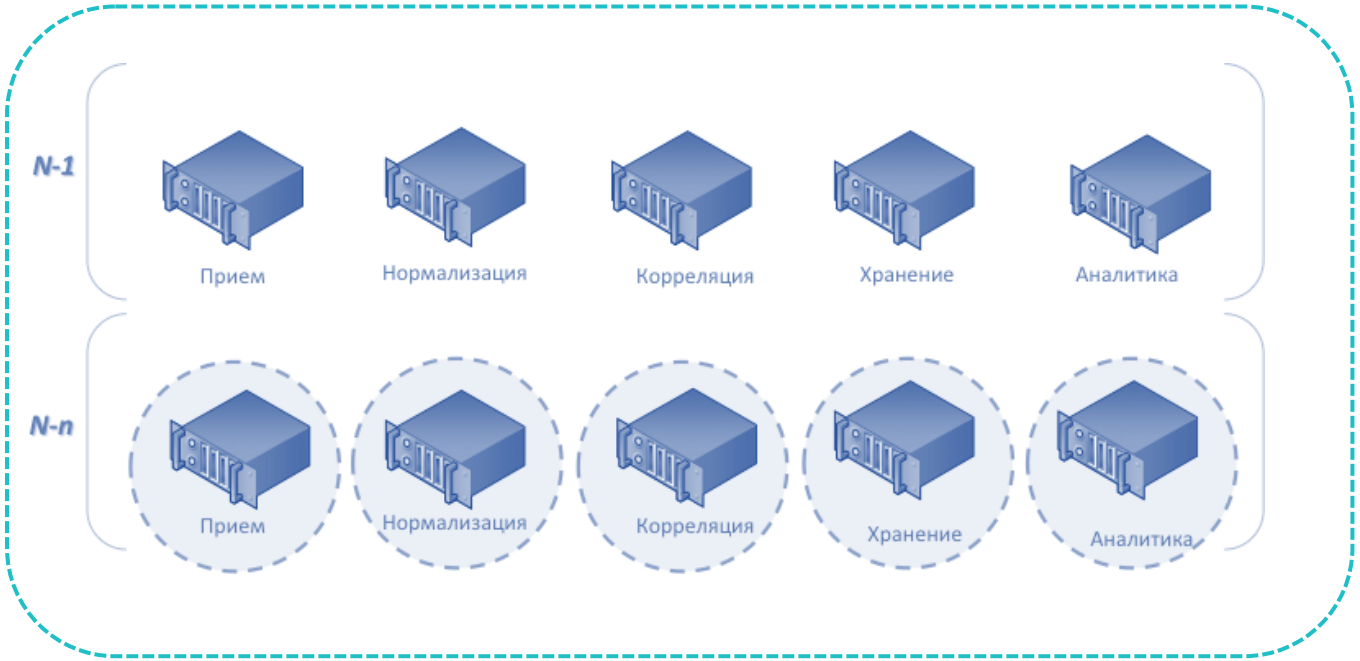


СОБЫТИЯ НА ВХОД

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

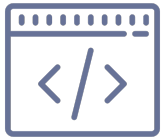
МАСШТАБИРУЕМОСТЬ



- 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

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

Ответим на все вопросы ОБРАЩАЙТЕСЬ!

Контактная информация:

Сайт : www.rusiem.com

Почта: info@rusiem.com

Телефон: +7(495)748-83-11