www.rusiem.com | +7(495)748-83-11 | info@rusiem.com | ООО "РуСИЕМ" ИНН: 7731317045

Описание функциональных характеристик программного комплекса «Система централизованного управления событиями информационной безопасности RuSIEM»

ООО «РуСИЕМ»

г. Москва, 2023 г.

www.rusiem.com | +7(495)748-83-11 | info@rusiem.com | ООО "РуСИЕМ" ИНН: 7731317045

АННОТАЦИЯ

Данный документ разработан для описания функциональных характеристик программного комплекса «Система централизованного управления событиями безопасности «RuSIEM» (далее ПК «RuSIEM»).

Документ содержит 3 раздела:

1. Введение

В разделе «Введение» приведена краткая характеристика ПК «RuSIEM».

2. Функциональные характеристики

В разделе «Функциональные характеристики» описывается функциональное назначение ПК «RuSIEM».

3. Информация необходимая для установки и эксплуатации продукта

В разделе «Информация необходимая для установки и эксплуатации продукта» описываются требования к функциональным характеристикам, надежности, составу и параметрам технических средств, к информационной и программной совместимости, к маркировке и упаковке, к транспортированию и хранению, а также условия эксплуатации ПК «RuSIEM».

www.rusiem.com | +7(495)748-83-11 | info@rusiem.com | ООО "РуСИЕМ" ИНН: 7731317045

СОДЕРЖАНИЕ

www.rusiem.com | +7(495)748-83-11 | info@rusiem.com | ООО "РуСИЕМ" ИНН: 7731317045

1. ВВЕДЕНИЕ

Программный комплекс «RuSIEM» является программным средством общего назначения со встроенными средствами защиты информации от несанкционированного доступа.

ООО «РуСИЕМ» российская компания, занимающаяся созданием решений в области мониторинга и управления событиями информационной безопасности на основе симптомов и анализа данных в реальном времени.

RuSIEM представлен на рынке тремя продуктами с разными функциональными возможностями. Возможна поставка в трех вариантах, отличающихся друг от друга функционалом:

1. RvSIEM – бесплатный, свободно распространяемый продукт класса Log Management (управление журналами), с помощью которого можно выполнять нормализацию полученных логов, обогащать события, искать данные в журналах, строить отчёты и создавать информационные панели. Количество обрабатываемых событий – до 500 в секунду.
2. RuSIEM – SIEM-система, занимающаяся как сбором, так и обработкой, и корреляцией событий. Она не имеет таких ограничений по событиям в секунду, которые свойственны RvSIEM, обладает большими функциональными возможностями в том числе в части работы с инцидентами и потоками данных Threat Intelligence.
3. RuSIEM Analytics – модуль, который позволяет выявлять аномалии, формировать аналитические отчёты, управлять активами, построить процесс управления уязвимостями и реализовать много других дополнительных возможностей.

Полная версия системы предназначена как для сбора и анализа информации, так и для обнаружения атак и различных аномалий в организации, проведения глубокого анализа и проактивного поиска угроз, а также оперативного реагирования на инциденты и их дальнейшего расследования. Система способна выявить угрозу, когда обычные

средства детектирования по отдельности её не видят, но она может быть обнаружена при тщательном анализе и корреляции информации из различных источников.

Полная версия системы предоставляет следующие функциональные возможности:

- сбор с помощью собственного агента и пассивный прием событий;
- нормализация событий с долгосрочным хранением и оперативным поиском;
- обогащение событий мета-информацией, описывающей о чем событие в понятном для пользователя формате;
- поиск по событиям без знания типов и состава событий на основе симптоматики;
- приоритезация событий посредством весов симптоматики, в том числе составным весом;
- корреляция на последовательных событиях (счетчик);
- триггерная корреляция фактов различных событий;
- агрегация весов по объектной модели для обнаружения угроз без применения сигнатур;
- проверка ip, fqdn, md5/sha1 file, url, email по фид-листам с угрозами;
- встроенный инцидент-менеджмент для реагирования и фиксации угроз;
- автоматическое обновление продукта, правил корреляции, симптоматики и фидов;
- ролевая модель доступа в систему.

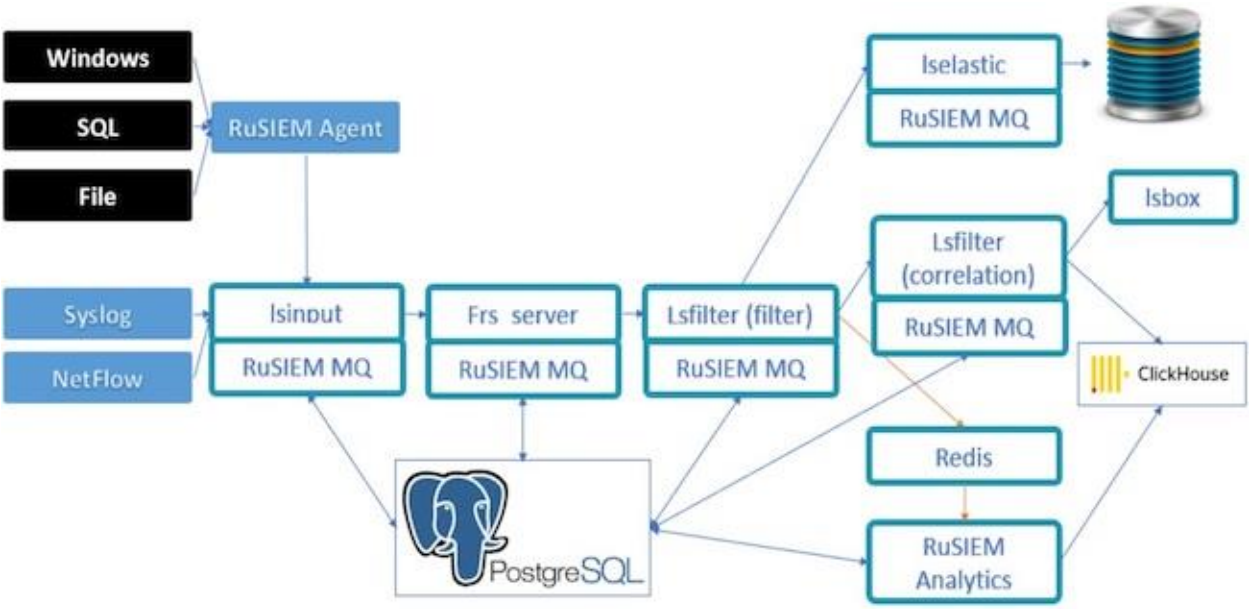
Бесплатная версия системы является системой класса Log Management и предназначена для сбора информации, ее нормализации и обогащения, без возможности проводить анализ.

www.rusiem.com | +7(495)748-83-11 | info@rusiem.com | ООО "РуСИЕМ" ИНН: 7731317045

Программный комплекс «RuSIEM» представляет из себя микросервисную архитектуру, обеспечивающую перенос части функции системы управления событиями информационной безопасности на отдельные сервера, выполняющие функции:

- Приема событий;
- Нормализации событий;
- Корреляции событий;
- Хранения событий;
- Поведенческого анализа.

Архитектура программного комплекса «RuSIEM»:



2. ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ

2.1. Цели и назначение

ПК «RuSIEM» предназначен для сбора, обработки и анализа данных от источников событий ИБ; последующего реагирования на эти события, ведения статистики и формирования результирующих отчётов по итогам работы.

Источниками событий ИБ для ПК «RuSIEM» являются:

- Клиентский программный компонент «Агент»;
- Журналы событий администраторов и пользователей ЭВМ под управлением ОС: Windows, MacOS, Linux, Astra;
- Специальное программное обеспечение: веб-серверы (nginx, Apache), почтовые серверы, СУБД (MySQL, Oracle и др.), ActiveDirecory и другое ПО;
- Межсетевые экраны (программные и аппаратные);
- Средства антивирусной защиты, системы обнаружения вторжений, средства мониторинга, контроля доступа и защиты от несанкционированного доступа.

2.2. Ключевые функции

В состав программного комплекса «RuSIEM Сервер» входят следующие компоненты:

- сервер;
- хранилище данных;
- аналитика;
- визуализация;
- корреляция;
- симптоматика;
- нормализация;
- интерфейс.

Состав программных компонентов ПК «RuSIEM» с описанием их назначения представлен в таблице 1.1.

www.rusiem.com | +7(495)748-83-11 | info@rusiem.com | ООО "РуСИЕМ" ИНН: 7731317045

Таблица 1.1-Состав компонентов ПК «RuSIEM»

№ п/п	Наименование компонента	Описание функций компонента
1.	Компонент «Лог-менеджер»	Обеспечивает сбор данных от источников ИБ:
		Локально и удалённо;
2.	Компонент «Агентское ПО» (Агентское ПО для установки на рабочих станциях и серверах Windows и сбора событий с них)	Сбор и отправку событий ИБ на сервер, для дальнейшего анализа.
		При отсутствии связи с сервером Агент обеспечивает локальное хранение информации о зарегистрированных событиях ИБ
3.	Компонент «Связь с хранилищем данных»	Связь с БД для обеспечения хранения собранной информации о событиях ИБ в процессе работы ПК «RuSIEM».
4.	Компонент «Нормализация»	Нормализация событий ИБ от разнородных источников к унифицированному виду.
		Выборки из обработанных данных по параметрам.
5.	Компонент «Симптоматика»	Обогащение собранных данных событий ИБ метаинформацией.
		Категоризацию, выборку и управление данными по симптомам.
6.	Компонент «Корреляция»	Поиск корреляций между выявленными событиями ИБ.
		Формирование инцидентов по выявленным корреляциям.
7.	Компонент «Web-Сервер» (Веб интерфейс для взаимодействия с пользователями)	Графический веб-интерфейс для работы с ПК «RuSIEM».
		Функции управления и администрирования ПК «RuSIEM» (обновление составных частей Изделия: конфигурации компонентов, правил корреляции, правила симптоматики, новостные ленты).
		Ролевое разделение доступа к ПК «RuSIEM».
		Функции удалённого доступа к ПК «RuSIEM» по защищённому протоколу.

		Уведомления о выявленных инцидентах
		Формирование отчётов по результатам работы ПК «RuSIEM».

Функциональные возможности, которым должны удовлетворять программные компоненты «RuSIEM» приведены в таблице ниже.

Таблица 1.2 - Описание функциональных возможностей

№ п/п	Описание функциональных возможностей
1.	Сбор информации с ОС: Windows, Linux, сетевого оборудования и любых приложений, имеющих возможность вывода событий.
2.	Сбор событий из таблиц и представлений основных баз данных: MS SQL, MySQL, Oracle
3.	Сбор данных от клиентского программного компонента «Агент».
4.	Удалённый сбор данных без предоставления системе прав привилегированной учетной записи.
5.	Единое именование полей и единая классификацию событий от различных источников, с возможностью добавления пользовательской классификации событий.
6.	Функции установки весов и тегов событий, с возможностью добавления пользовательских весов и тегов событий.
7.	Возможность выборочного отключения правил корреляции пользователем.
8.	Наличие инструментов назначения приоритетов инцидентов в правилах корреляции.
9.	Возможность разделения прав доступа к просмотру уведомлений от правил корреляции по группам корреляции.
10.	Интерпретацию событий в понятный для оператора формат.
11.	Формирование правил корреляции и симптоматики.

www.rusiem.com | +7(495)748-83-11 | info@rusiem.com | ООО "РуСИЕМ" ИНН: 7731317045

№ п/п	Описание функциональных возможностей
12.	Классификацию событий с возможностью выбора событий по классу и нескольким классам.
13.	Изменение и создание пользовательских правил корреляции.
14.	Обнаружение ранее неизвестных угроз по имеющимся данным (по уже собранным событиям).
15.	Визуализацию показателей событий.
16.	Формирование графических представлений данных и их экспорт во внешний файл.
17.	Визуализацию событий с возможностью автоматического обновления информации на панелях представления.
18.	Выбор критериев и параметров отображения на панелях представления.
19.	Изменение составляющих элементов и самих панелей представления пользователем.
20.	Визуализацию трафика в инфраструктуре с возможностью выбора параметров отображения.
21.	Корреляционный анализ по временным критериям.
22.	Централизованное хранение данных (нормализованных и исходных событий, сформированных инцидентов и других обрабатываемых данных) с возможностью сжатия.
23.	Локальное хранение данных в случае недоступности центрального хранилища данных.
24.	Полнотекстовый поиск по событиям.
25.	Механизмы оперативного анализа событий, с возможностью изменения сохранённых запросов по различным критериям.
26.	Ролевое разделение прав доступа в систему.
27.	Информирование о выявленных инцидентах.

www.rusiem.com | +7(495)748-83-11 | info@rusiem.com | ООО "РуСИЕМ" ИНН: 7731317045

№ п/п	Описание функциональных возможностей
28.	Обеспечение безопасного удалённого доступа.
29.	Механизм выполнения команд для реагирования на выявленные угрозы в режиме близком к реальному времени.
30.	Ведение статистики работы.
31.	Формирование итоговых и промежуточных отчётов в процессе работы и их экспорт во внешний файл.
32.	Механизмы контроля актуальности лицензий программного комплекса.
33.	Механизмы обновления программных компонентов.
34.	Механизмы для добавления новых элементов (источников данных).
35.	Механизмы архивации событий
36.	Механизмы архивации и шифрования данных при передаче между агентами и RuSIEM
37.	Механизмы модуля «Активы»
38.	Формирование динамических списков
39.	Механизмы модуля агента для получения низкоуровневых событий
40.	Реализация протоколов Telnet, SSH
41.	Механизмы новой версии модуля «Симптоматика»
42.	Взаимодействие с НКЦКИ - ГосСОПКА
43.	Автоматический парсер логов на основе алгоритмов машинного обучения
44.	Методы автоматической актуализации топологии источников на базе анализа косвенных характеристик
45.	Оптимизация ядра (распараллеливание операций, динамическое выделение потоков, низкоуровневая доработка)

www.rusiem.com | +7(495)748-83-11 | info@rusiem.com | ООО "РуСИЕМ" ИНН: 7731317045

№ п/п	Описание функциональных возможностей
46.	Механизмы работы с Источниками (реализация механизмов: слушать все и конкретные источники, защита от ddos, отслеживание событий с источников)
47.	Сбор статистики по парсерам и корреляции
48.	Механизмы подсистемы поведенческой аналитики (UEBA - User and Entity Behavioral Analytics)
49.	Механизмы подсистемы обнаружения вредоносных доменов DGA
50.	Механизмы модуля «Фильтрация и агрегация событий
51.	Функционал мультитенанси (работа с территориально распределенными офисами)
52.	Механизмы модуля «TI»
53.	Механизмы нового пользовательского интерфейса

www.rusiem.com | +7(495)748-83-11 | info@rusiem.com | ООО "РуСИЕМ" ИНН: 7731317045

3. ИНФОРМАЦИЯ НЕОБХОДИМАЯ ДЛЯ УСТАНОВКИ И ЭКСПЛУАТАЦИИ ПРОДУКТА

Требования к установке и эксплуатации продукта

3.1. Программный комплекс «RuSIEM» сертифицирован ФСТЭК России по требованиям к Межсетевым Экранам (4-й класс, профили А и Б) и к Системам Обнаружения Вторжений (4-й класс), а также по 4 уровню доверия. Таким образом, ПК «RuSIEM» может использоваться в составе автоматизированных систем (АС) до класса защищенности 1Г, значимых объектов КИИ I категории, информационных системах персональных данных (ИСПДн) 1 уровня защищенности, государственных информационных системах (ГИС) 1 класса защищенности.

3.2. Запрещается обрабатывать и хранить в ПК «RuSIEM» информацию, содержащую сведения, составляющие государственную тайну.

3.3. Установка, настройка и эксплуатация ПК «RuSIEM» производится на аппаратных средствах, отвечающих требованиям пункта «Технический состав оборудования» документа «Технические и эксплуатационные характеристики программного комплекса «RuSIEM»».

3.4. Технические средства, обеспечивающие функционирование ПК «RuSIEM», должны располагаться в пределах контролируемой зоны, оборудованной средствами охраны, обеспечивающими уровень защиты, соответствующий обрабатываемой информации.

3.5. При подключениях пользователей за пределами контролируемой зоны должны использоваться сертифицированные средства криптографической защиты и межсетевое экранирование.

3.8. При эксплуатации ПК «RuSIEM» на объектах информатизации необходимо обеспечить обязательное выполнение организационно-технических мероприятий по защите информации:

- осуществление ввода в эксплуатацию и эксплуатации ПК «RuSIEM» в соответствии с требованиями эксплуатационной документации;
- хранение компакт-диска с размещенным дистрибутивом и компакт-диска с эксплуатационной документацией ПК «RuSIEM» в периоды времени,

предшествующие и последующие непосредственной эксплуатации ПК «RuSIEM» только в упаковке;

- наличие администратора безопасности (администратора ПК «RuSIEM»), отвечающего за правильную настройку и эксплуатацию ПК «RuSIEM»;
- сохранение в секрете учетной информации администратора ПК «RuSIEM» и пользователей ПК «RuSIEM»;
- отсутствие вирусов на ПЭВМ на момент установки ПК «RuSIEM» и при дальнейшем функционировании.