RUSIEM

Всё под контролем

Система централизованного управления событиями информационной безопасности RuSIEM

Для чего нужна SIEM

RUSIEM

SIEM (Security Information and Event Management) —
решение для мониторинга и анализа любой сетевой активности, происходящей в организации. Также в систему входят приложения для контроля идентификацией и доступом, инструменты управления уязвимостями

- 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 сопоставлении 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

Факты

RUSIEM

> 50 млн

СОБЫТИЙ В СЕКУНДУ
В КОММЕРЧЕСКИХ
ПРОЕКТАХ

2014

ГОД НАЧАЛА АКТИВНОЙ
РАЗРАБОТКИ

> 450

ПАРТНЕРОВ
ПО ВСЕМУ МИРУ

>10000

УСТАНОВОК
FREE-ВЕРСИИ

- Российская разработка
- Сотни кейсов успешного внедрения и тысячи активных пилотных проектов
- Резидент Сколково

- В реестре отечественного ПО
- Продажа через дистрибьюторов, партнеров, SOC
- Продукт имеет сертификат ФСТЭК России (4 УД), ОАЦ (Беларусь)

Почему RuSIEM

RUSIEM

Почему RuSIEM подходит под ваши задачи

- Соответствие требованиям регуляторов (Федеральные законы № 152-ФЗ, 161-ФЗ, 187-ФЗ, приказы ФСТЭК России № 21, 17 и 31, СТО БР ИББС и РС БР ИББС-2.5-2014, международного стандарта PCI DSS, ISO 27001)
- Помогаем с начала пилотного тестирования до полного внедрения
- Решение быстро настраивается, просто кастомизируется, адаптируется к вашим повседневным потребностям
- Проводим бесплатное обучение для наших партнеров и заказчиков
- Можно использовать данные из любых источников. Помогаем с подключением новых и нетиповых источников

Какие задачи решает SIEM-система RuSIEM

- Оперативное обнаружение, реагирование и контроль обработки инцидентов
- Оперативный контроль состояния инфраструктуры компании
- Создание единого центра мониторинга
- Определение прав, обязанностей и разграничение зон ответственности персонала компании (ИТ- и ИБ-служб)

Линейка продуктов

RUSIEM

RuSIEM

Коммерческая версия системы класса SIEM

RuSIEM Analytics

Модуль для коммерческой версии системы RuSIEM, дополненный возможностями AI (artificial intelligence), DL (data learning) и др.

RuSIEM Monitoring

Система для отслеживания состояния объектов ИТ-инфраструктуры и выявления нарушений, связанных с изменением их статуса

RvSIEM IoC

Модуль для обнаружения попыток захвата корпоративных устройств хакерами (индикаторы компрометации)

RvSIEM free

Решение класса LM (Log Management), ограниченная по возможностям коммерческая версия RuSIEM

+7 (495) 748-83-11

info@rusiem.com

rusiem.com