RUSIEM
Всё под контролем

SIEM-система RuSIEM

Аналитический центр безопасности компании

rusiem.com

Всё
под контролем

О компании

RuSIEM – российская компания, занимающаяся созданием решений в области мониторинга и управления событиями информационной безопасности и ИТ-инфраструктуры на основе анализа данных в реальном времени.

Среди решений компании – программный комплекс обеспечения информационной безопасности (ИБ), позволяющий собирать и анализировать информацию о событиях ИБ, получаемую из разнородных источников. Работа RuSIEM позволяет увидеть максимально полную картину активности сетевой инфраструктуры и событий информационной безопасности.

Продукт обеспечивает соответствие требованиям законов № 152-ФЗ, 161-ФЗ, 187-ФЗ, приказов ФСБ России № 282, ФСТЭК России №№ 17, 21, 31, 239, приказа ФСБ России и ФСТЭК России № 416/489, СТО БР ИББС, РС БР ИББС-2.5-2014, ГОСТ Р 57580.1-2017, международного стандарта PCI DSS.

Факты

Российская разработка, сертификат ФСТЭК России (по новым требованиям) по 4УД, сертификат ОАЦ (Беларусь), в реестре отечественного ПО

Сотни кейсов успешного внедрения и тысячи активных пилотных проектов

RuSIEM — основа федеральных и коммерческих SOC

Резидент Сколково

Цифры

2014 год

Начало активной разработки

> 530

Партнеров по всему миру

> 50 млн

Событий в секунду в коммерческих проектах

> 10 000

Установок free-версии

Зачем нужна SIEM?

SIEM (Security Information and Event Management) —
решение для мониторинга и анализа любой сетевой активности, происходящей в организации. Также в систему входят приложения для контроля идентификации и доступа, 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, она может быть обнаружена при тщательном анализе и сопоставлении информации из различных источников с помощью SIEM
- 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 события с отдельных устройств

Что такое SIEM?

Принцип работы SIEM?

Сбор событий
Контроль инфраструктуры компаний

Корреляция событий
Анализ всех поступающих событий

Управление и анализ
Выявление уязвимостей и аномалий

Выявление инцидентов
Составление цепочек событий и оценка риска

Принятие решений
Уведомление администратора об инциденте

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 (сетевые устройства, приложения, 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 ПО
- оповещение об активной уязвимости по запуску ранее отключенной службы
- обнаружение распределенных по времени атак
- влияние отказа в инфраструктуре на бизнес-процессы

Источниками для SIEM-системы могут быть

- 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

ЛЮБЫЕ

Выгоды для компаний

Оптимизация ресурсов сотрудников отдела информационной безопасности

Точное определение событий более 97% «из коробки»

Снижение влияния человеческого фактора при предотвращении инцидентов

Поддержка от начала пилотного проекта до внедрения и сопровождения решения

Автоматизация рутинных процессов при выявлении аномалий

Возможность проведения расследований по «горячим следам»

Обнаружение потенциальных угроз на ранней стадии

Лучшие практики и экспертиза для выявления и предотвращения сложных угроз ИБ

Тренды и проблемы предприятий

- Формальный подход к ИБ
- Отсутствие ресурсов как финансовых, так и кадровых
- Сложный процесс обновления ПО с сохранением или минимальным нарушением непрерывности производства/бизнеса

83% **инцидентов невозможно выявить на ранней стадии без использования специализированного ПО**

Подходит организациям любого масштаба и отраслевой принадлежности

Примеры использования SIEM

- 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)

Чем уникально решение RuSIEM

Не теряем события

100% гарантия доставки событий в SIEM-систему, благодаря чему риск пропуска инцидента сводится «на нет»

No-code

Продукт не потребует дополнительных специфических знаний в процессе эксплуатации

Полностью подходит под критерии импортозамещения

Полностью отечественный продукт, входит в Единый реестр отечественного ПО, имеет все необходимые сертификаты

Максимальный предустановленный функционал

Более 350 правил корреляции и источников, более 30 шаблонов отчетов «из коробки»

Гибкость системы и компании-разработчика

Возможность горизонтального и вертикального масштабирования «на горячую»

Подключение любых источников данных

Возможность самостоятельной разработки парсеров под нужные источники, в том числе самописный софт

Централизованное управление

Единый веб-интерфейс и работа «в одном окне»

Интеграция с ГосСОПКА «из коробки»

Карточки предзаполненных инцидентов, уже готовы к отправке в ГосСОПКу

Адаптация под любые рынки и страны

Продукт полностью поддерживает английский язык, не имеет законодательных ограничений на экспорт, не входит в санкционные списки

Взаимодействие с ФинЦЕРТ

Возможность загружать в систему фиды от ФинЦЕРТ

Разработка и поддержка от вендора

Оперативное решение вопросов напрямую от разработчика

Экосистема RuSIEM

RuSIEM

коммерческая версия системы класса SIEM, включающая корреляцию в режиме реального времени, визуализацию данных и поиск по ним, долгосрочное хранение сырых и нормализованных событий, инцидент-менеджмент и отчеты

RuSIEM Analytics

модуль для коммерческой версии системы RuSIEM, дополняющий возможностями ML, DL, по визуализации данных, управлению активами и множеством других, способствующих обнаружению угроз и аномалий, решающих различные кейсы с помощью современных методик

RuSIEM IoC

модуль SIEM-системы, препятствующий взаимодействию корпоративных устройств с вредоносной инфраструктурой злоумышленников, включая ботнеты и командные сервера. Списки индикаторов компрометации обновляются ежедневно из нескольких сотен источников, нормализуются и ранжируются по степени опасности

RuSIEM Monitoring

система мониторинга ИТ-инфраструктуры с возможностью удаленного администрирования и встроенной системой HelpDesk

RvSIEM free

свободно распространяемая и ограниченная по возможностям версия

Демонстрационная версия RuSIEM

Мы предоставляем возможность попробовать триальную версию.

RuSIEM

Полнофункциональная версия системы предназначена для сбора и анализа информации, а также обнаружения атак и различных аномалий в организации, проведения глубокого анализа и проактивного поиска угроз и быстрого реагирования на инциденты и их дальнейшего расследования. Система способна обнаруживать угрозу, когда обычные средства обнаружения по отдельности ее не видят, но ее можно обнаружить при детальном анализе и корреляции информации из различных источников

Полная версия системы предоставляет следующие функциональные возможности

- сбор с собственным агентом и пассивный прием событий
- нормализация событий с длительным хранением и быстрым поиском
- обогащение события метаинформацией, описывающей, о чем идет речь, в удобном для пользователя формате
- поиск событий без знания типов и состава событий на основе их симптомов
- приоритизация событий с помощью весов симптомов, включая суммарные веса
- корреляция по последовательным событиям (счетчик)
- корреляция, активируемая на основе различных типов событий
- агрегирование весов по объектной модели для обнаружения угроз без использования сигнатур
- ip, fqdn, md5/sha1 файл, url, проверка электронной почты с использованием угрозы IoC и уязвимостей
- встроенное управление инцидентами для реагирования на угрозы и их захвата
- автоматическое обновление продукта, правила корреляции, симптомов, IoC и уязвимостей;
- модель системного доступа на основе ролей

Подробное описание коммерческой версии на сайте
rusiem.com/ru/products/rusiem

RuSIEM Analytics

Подсистема предоставляет функционал поведенческого анализа, осуществляющий сбор количественной статистики по значениям различных полей событий и генерацию инцидентов при обнаружении отклонений от собранной статистики

Поведенческий анализ предназначен для выявления на ранних стадиях инцидентов информационной безопасности, связанных с аномалиями в поведении пользователей или сущностей.

Модуль расширенной аналитики обеспечивает решение следующих сценариев

- превышение пороговых значений по параметру за час
- отклонение от поведения за прошедшие сутки
- превышение пороговых значений по параметру за сутки
- отклонение от поведения за аналогичный час прошедших суток
- отклонение от поведения за аналогичный час с привязкой к аналогичному дню недели за диапазон обучения

Модуль поведенческого анализа основан на машинном обучении и позволяет выдавать предположения об ожидаемом поведении сущностей и пользователей, основываясь на ранее собранных данных. В случае выявления отклонений от ожидаемого поведения модуль информирует о выявлении данной аномалии.

Поведенческий анализ использует события реального времени, не выполняя запросы в подсистеме хранения данных, благодаря чему снижается нагрузка на систему хранения. Дополнительно модуль поведенческого анализа позволяет отслеживать аутентификацию пользователей и предоставляет возможность генерации инцидентов при входе любого пользователя в любую систему-источник с IP-адреса, вход с которого ранее не осуществлялся данным пользователем, либо на хост, вход на который ранее не осуществлялся данным пользователем.

Функция поведенческого анализа также предоставляет возможность создания пользовательских сценариев входа и выхода.

RuSIEM Monitoring

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

Непрерывность – одно из основных требований бизнеса по отношению к ИТ и ИБ вне зависимости от масштабов и сферы деятельности организации. Киберустойчивость организации определяется как бесперебойным функционированием оборудования и информационных систем, так и защищенностью от хакерских атак. RuSIEM Monitoring:

- **для ИТ** — контроль состояния компонентов всей вычислительной инфраструктуры в реальном времени;
- **для ИБ** — выявление аномалий в функционировании оборудования и информационных систем, указывающих на вероятные действия внешних и внутренних злоумышленников.

Задачи

- мониторинг и устранение неполадок узлов ИТ-инфраструктуры, включая серверы, сетевое оборудование и рабочие станции
- мониторинг приложений, работающих в режиме реального времени для обеспечения бесперебойной работы
- мониторинг информационных систем и бизнес-критичных серверов
- улучшение процесса управления ИТ-инфраструктурой за счет упрощения выявления узких мест, пропускной способности и других потенциальных проблемных точек в сетевой среде
- удаленный и защищенный доступ к управлению ИТ-инфраструктурой и, как результат, снижение затрат
- простое и удобное администрирование рабочих станций пользователей и серверов, включая удаленные, что стало очень актуальным в нынешнее время

Преимущества

- мониторинг не требует установки агентов на сервера
- запуск системы в работу осуществляется за 10 минут: подключение к серверам и сетевому оборудованию в один клик
- удаленная поддержка: наличие внутренней системы HelpDesk с доменной авторизацией и подключение к пользователю в один клик из тикета
- одно решение для направлений ИТ и ИБ
- эффективно работает как самостоятельно, так и в связке с SIEM

RuSIEM IoC

Подсистема обеспечивает функционал для обнаружения попыток захвата корпоративных устройств хакерами

Подключить сервер, ПК или смартфон к зараженным узлам собственной сети, чтобы развивать атаку – любимая тактика злоумышленников. Понимайте намерения хакеров до того, как захват ими конкретных устройств приведет к ощутимым ИБ-последствиям. RuSIEM IoC укажет на возможность развития подобных инцидентов. Модуль подгружает в SIEM данные об IP-адресах, доменах, URL, хэшах вредоносного ПО. Как только система фиксирует в сетевом потоке или хостовой активности обращение к ресурсам из базы, она сообщает об этом оператору, указывая на то, какой именно элемент ИТ-инфраструктуры скомпрометирован и требует «лечения».

Преимущества

- анализирует данные из более чем 260 открытых источников
- сбор индикаторов происходит из социальных сетей (Telegram, Twitter), репозиториев Github, а также данных публичных TI-отчетов
- на текущий момент система насчитывает более 250 тысяч уникальных индикаторов в сутки, при этом 30 тысяч из которых имеют наивысший уровень опасности
- интеллектуальная нормализация, очистка, обогащение индикаторов
- определение степени опасности каждого индикатора на базе уникальной математической модели ранжирования

Какие угрозы можно выявлять с помощью использования IoC

- загрузка вредоносных файлов с зараженных ресурсов сети Интернет
- автоматические запросы с компьютеров к инфраструктуре злоумышленников
- обращение компонентов клиентской инфраструктуры на вредоносные узлы
- запросы и обращения с инфраструктуры злоумышленников либо зараженных узлов
- идентификация конкретного ВПО либо хакерской группировки

Как это работает

- автоматическая настройка без отвлечения ресурса ИБ-команды
- обновление раз в сутки для актуального статуса базы данных
- минимум ложных срабатываний за счет сроков истечения (TTL) для записей в списках индикаторов компрометации
- совместимость с индикаторами других поставщиков
- поддержка кастомных правил корреляции наряду с предустановленными
- работа с индикаторами регуляторов, например, ФинЦЕРТ

RvSIEM free

Решение класса LM (Log Management), которое позволяет собрать, нормализовать события, строить отчеты, долгосрочно хранить, визуализировать данные без возможности выполнения анализа

RvSIEM free – ограниченная по возможностям коммерческая версия RuSIEM. Может быть использована вместе с RuSIEM в сложных проектах в качестве решения для сбора событий для снижения общей стоимости владения системой.

Демо-версия

Мы предоставляем возможность попробовать триальную версию. Продукт может быть развернут у вас вашими силами, либо мы можем подобрать сертифицированного партнера, который вам поможет установить и настроить его.

Перед установкой коммерческой версии необходимо связаться со службой технической поддержки RuSIEM и получить доступ к репозиторию и обновлению, сообщив hardware id сервера.

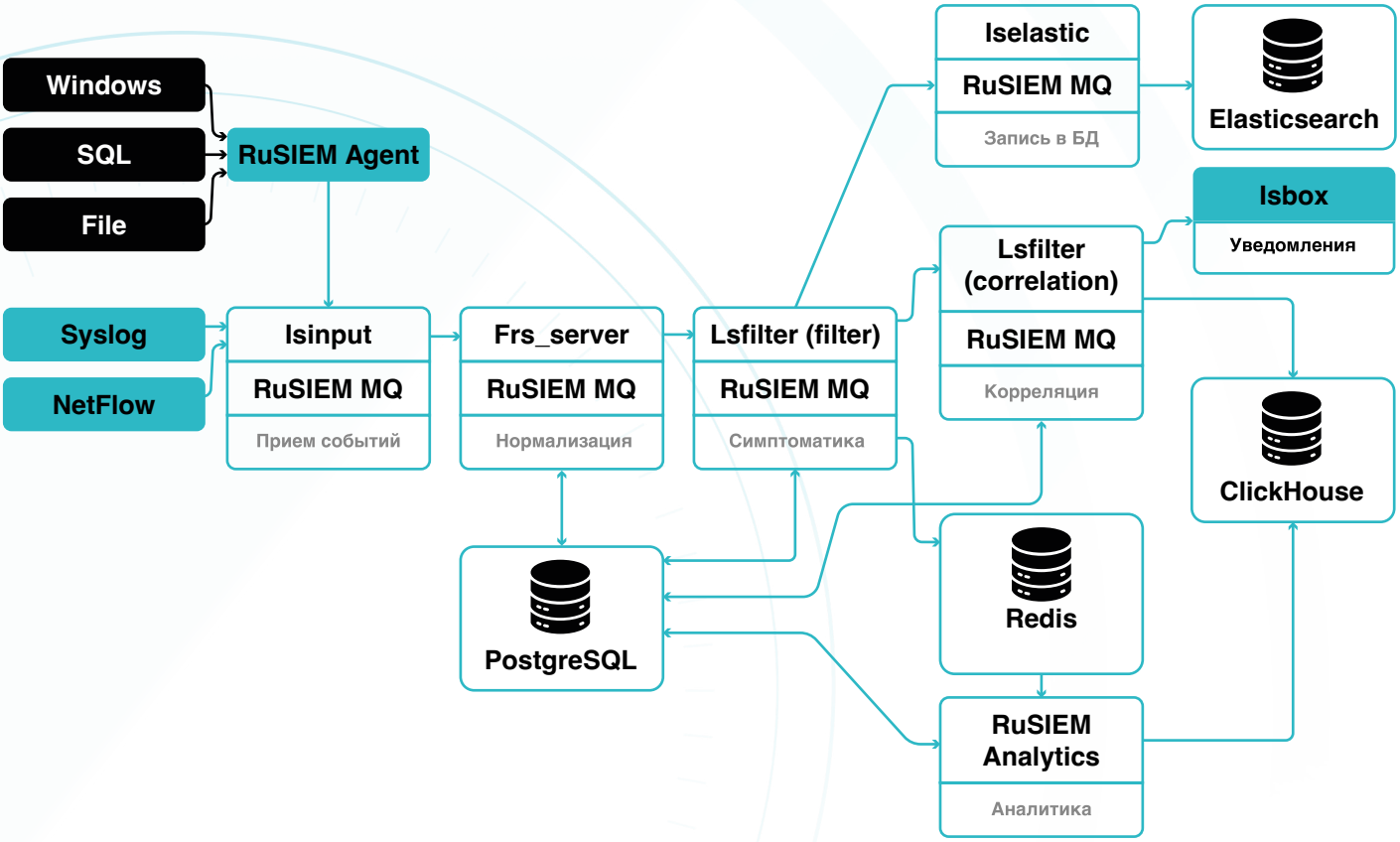
Запросить демо-версию можно по ссылке
rusiem.com/ru/demo

Поддерживаемые источники и парсеры по ссылке
rusiem.com/ru/products/parsers

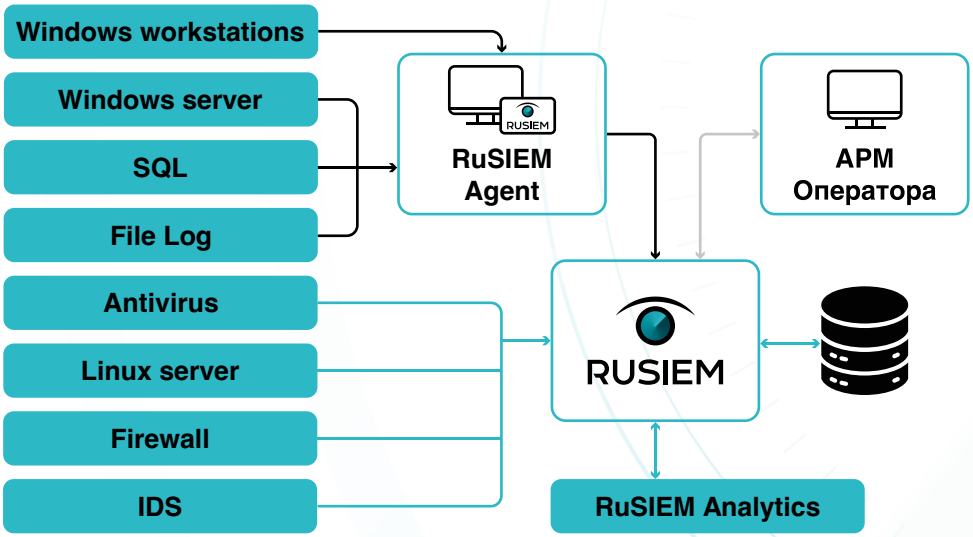
Архитектура RuSIEM

Система состоит из набора микросервисов, выполняющих специфические задачи

- **RuSIEM Agent** — отвечает за сбор событий из систем Windows, SQL-серверов и файловых журналов
- **Isinput** — отвечает за получение событий из различных источников (Syslog, NetFlow, RuSIEM Agent). Isinput получает события, ставит их в очередь и отправляет дальше по цепочке
- **Frs_server** — отвечает за нормализацию событий (разделение событий на поля на основе встроенных правил (по таксономии))
- **Lsfilter (фильтр)** — отвечает за симптоматическую функциональность (обогащение событий полезной информацией - добавление описания и критичности событий)
- **Iselastic** — отвечает за запись событий в elasticsearch для дальнейшей работы с событиями (поиск, просмотр, анализ, отчеты, ретроспективный анализ)
- **Lsfilter (корреляция)** — отвечает за корреляцию событий по инцидентам, генерируемым системой в процессе работы (доступно в коммерческой версии)
- **RuSIEM Analytics** — отвечает за поиск аномалий (доступно в коммерческой версии, отдельная лицензия)



Стандартная схема развертывания системы



Лицензирование

- ***проектные цены***
- ***модульные спецификации***
- ***бессрочные и срочные лицензии***
- ***разработка сложных парсеров***
- ***разработка правил корреляции***

Количество событий в секунду
events per second

2000 eps
3000 eps
4000 eps
5000 eps
7500 eps
10000 eps
12500 eps
15000 eps
20000 eps
…

Значимые обновления и полный перечень доработок, вошедших в состав продукта, доступен на сайте:
rusiem.com > Продукты > История обновлений

Решения RuSIEM уже используют

МегаФон

Совместный проект по созданию центра мониторинга киберинцидентов

Комплексное решение, которое обеспечивает проактивную защиту компаний от всех типов современных киберрисков

Удобное решение для малого и среднего бизнеса, который не может себе позволить собственный полноценный SOC

72% новых клиентов представляют коммерческие организации, в том числе промышленные предприятия, банки и ритейл, 25% — государственные учреждения, 3% — медиа

ЭР-ТЕЛЕКОМ

Совместный проект по созданию центра мониторинга киберинцидентов

Услуга внешнего SOC (Security Operation Center)

Мониторинг событий и выявление инцидентов ИБ в режиме 24/7

Обмен информацией с ГосСОПКА и ФинЦЕРТ

@СТРАЛ

Совместный проект по созданию центра мониторинга киберинцидентов

Система, реализованная на базе ИТ-решения RuSIEM, обеспечивает сбор и анализ данных о событиях ИБ

Возможность подключения новых типов источников событий ИБ совместно с техподдержкой RuSIEM

К системе RuSIEM можно подключать неограниченное количество агентов на АРМ пользователей заказчика

АКСОН

Лучшее решение для территориально-распределенных компаний

Единая точка входа и высокое качество мониторинга событий безопасности

Контроль и защита периметра, усиленная политика ИБ

УРАЛСИБ | СТРАХОВАНИЕ

Созданное решение позволяет обеспечить контроль соблюдения политики ИБ

Сокращение затрат на персонал, необходимый для контроля всех средств защиты информации

Минимизирует возможные экономические потери от потенциальной утечки данных клиентов или хищения денежных средств

ДЕРЖАВА БАНК

Решение обеспечивает повышение уровня безопасности, дополнительную защиту средств и данных клиентов банка

Соответствие требованиям регуляторов и ГОСТ

Быстрое реагирование на инциденты и отслеживание любых подозрительных действий

Петербургский Городской Банк

Решение позволило достичь максимальной скорости и надежности финансовых транзакций через Интернет

Быстрое выявление инцидентов, автоматизация процессов реагирования

Исчерпывающая функциональность, конкурентная стоимость, простое освоение системы

Институт аэронавигации

Продукт обеспечил усиление информационной безопасности и реализацию подхода к управлению ею как процессом

Решение для организаций с повышенными требованиями к сохранности данных и неприрывности работы информационных систем

TenIT

ООО «Тэнит» — официальный дистрибьютор на территории Республики Беларусь

Республика Беларусь,
220030, г. Минск,
пр. Независимости, д. 11,
корп. 2, каб. 319

+375 17 209-95-79
+375 17 209-92-94
info@tenit.by
www.tenit.by

Партнеры RuSIEM:

OCS DISTRIBUTION

AXOFT

IT TASK системный интегратор

softline

AR integ

STEP LOGIC

@СТРАЛ

информационный центр

КОНФИДЕНТ ГРУППА КОМПАНИЙ

УЦСБ

МегаФон

ЭР-ТЕЛЕКОМ

ЛАНИТ

АСТЕРИТ

ФГУП «НПП «Гамма»

ИТ ЭНИГМА

Jet

КРОК

ЛЕГИОН

VK MASKOM ГРУППА КОМПАНИЙ

DistriSYSTEM

Бевалекс вместе – от идеи к решению

IRSEN GROUP

*и ещё **более 500 партнеров** по всему миру*


RUSIEM
Всё под контролем

RUSIEM
Всё под контролем

Отечественный SIEM
Управление инцидентами информационной безопасности

Сертификат ФСТЭК России № 4402 от 12.05.2021, 4 УД
Единый реестр отечественного ПО (№ 3808)

Остались вопросы?
Свяжитесь с нами для бесплатной
презентации системы

Москва, ул. Василисы Кожиной, 1
БЦ «Парк победы»
+7 (495) 748-83-11
info@rusiem.com
rusiem.com