РУСИЕМ Единая система мониторинга информационной безопасности организации

Максим Степченков

Совладелец компаний
РуСИЕМ и БелСИЕМ

Обеспечение закрытого доверенного технологического контура

в рамках курса на импортозамещение и развития национального технологического суверенитета Российской Федерации и Республики Беларусь

+7 (495) 748-83-11

rusiem.com

info@rusiem.com

РуСИЕМ – ОТЕЧЕСТВЕННАЯ ИБ-компания

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, позволяющий собирать и анализировать информацию о событиях ИБ, получаемую из разнородных источников (SIEM), а также решение для защиты веб-приложений (WAF)

всё под контролем

РУСИЕМ СЕЙЧАС

10+ лет успешного развития

полностью российская разработка

x3

рост компании за последние 3 года

продукты компании имеют сертификаты ФСТЭК России (4 УД), ОАЦ (Беларусь)

ТОП-3

отечественных SIEM-решений

продукты компании включены в Единый реестр отечественного ПО

>650

партнеров в России, странах СНГ, Азии и Латинской Америке

ОТ РОССИЙСКОЙ РАЗРАБОТКИ К СОВМЕСТНОМУ ТЕХНОЛОГИЧЕСКОМУ КОНТУРУ

RuSIEM развивается как российская технология с локализацией и экспертизой на рынке Республики Беларусь

РуСИЕМ работает на российском ИТ-рынке с 2016 года и занимается созданием решений для мониторинга и управления событиями информационной безопасности на основе анализа данных в реальном времени.

2014	2023	2025	Следующий этап
Развитие RuSIEM на российском рынке	Системная работа в Республике Беларусь	Создание ООО «БелСИЕМ»	Совместимый доверенный технологический контур

Вектор развития: от отдельного продукта к модели локализации, сертификации и интеграции внутри российско-белорусской технологической экосистемы

Доверенный контур — это не один продукт, а управляемая совокупность совместимых технологий

Ключевые технологии, процессы развития и эксплуатационная экспертиза находятся под контролем российских и белорусских разработчиков, интеграторов и специалистов

Собственная разработка	локализация	сертификация	интеграция	поддержка
контроль кодовой базы и развития продукта	адаптация под требования рынка и инфраструктуры	подтверждение соответствия требованиям регуляторов	совместная работа продуктов в единой инфраструктуре	компетенции внутри технологического контура

Задача такого контура — обеспечить технологическую совместимость без критической зависимости от внешних поставщиков

RUSIEM

– это ядро системы информационной безопасности

Технология SIEM обеспечивает мониторинг и анализ событий в реальном времени, исходящих от сетевых устройств и приложений, и позволяет реагировать на них до наступления существенного ущерба

ЧЕМ УНИКАЛЬНО РЕШЕНИЕ RUSIEM

Не теряем события

No-code

Полностью подходит под критерии импортозамещения

Максимальный предустановленный функционал

Интуитивно понятный и «дружелюбный» интерфейс

Подключение любых источников данных

Real-time и историческая корреляция

Интеграция с ГосСОПКА «из коробки»

Оптимальное соотношение цена/ качество на рынке России

Взаимодействие с ФинЦЕРТ

Разработка и поддержка от вендора

Лояльность вендора и готовность к оперативной доработке

ЛИНЕЙКА ПРОДУКТОВ

Продукты закрывают несколько уровней мониторинга и защиты: от сбора событий до анализа аномалий и работы с индикаторами компрометации

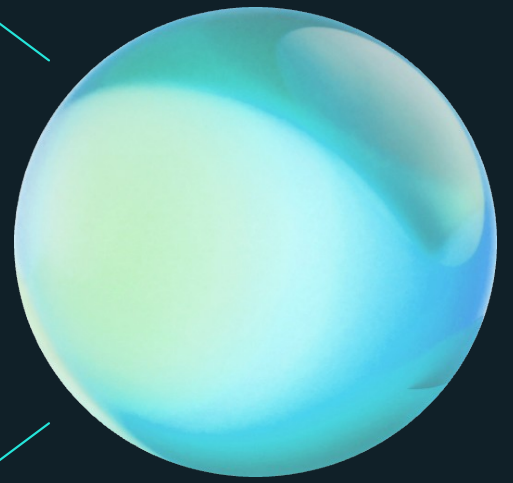
RuSIEM
коммерческая
версия класса SIEM

RuSIEM IOC
модуль индикаторов
компрометации

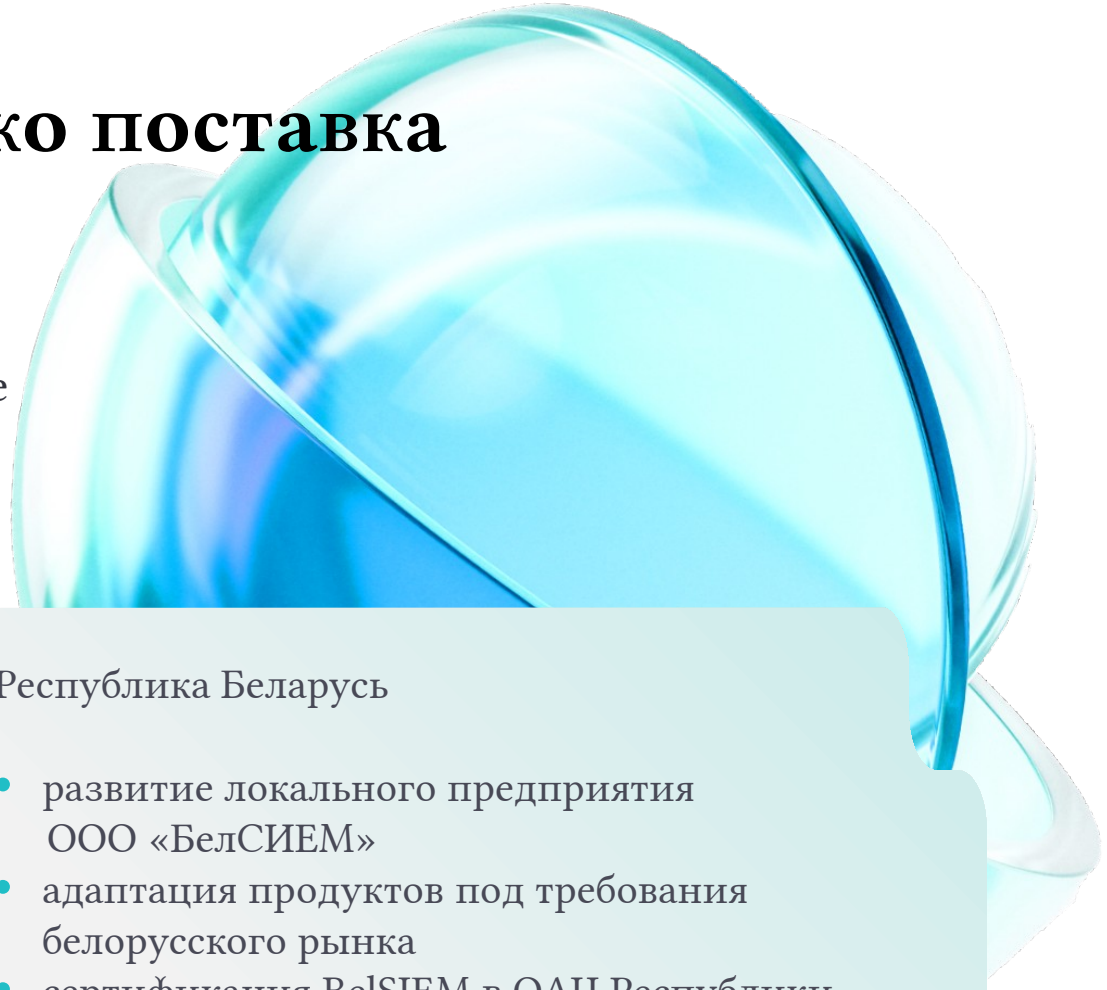
RvSIEM free
классическое решение
класса LM

RuSIEM ANALYTICS
модуль для анализа событий,
основанный на ML

RuSIEM WAF
решение для защиты веб-
приложений



Локализация — это не только поставка продукта на другой рынок



Это адаптация технологии, сертификация, развитие локальной экспертизы и включение продукта в национальную экосистему решений

Российская Федерация

- разработка и развитие технологий RuSIEM
- собственная команда разработки и поддержки
- включение RuSIEM в Реестр российского ПО
- сертифицированные версии RuSIEM по требованиям ФСТЭК России
- развитие интеграций с отечественными ИТ- и ИБ-решениями

Республика Беларусь

- развитие локального предприятия ООО «БелСИЕМ»
- адаптация продуктов под требования белорусского рынка
- сертификация BelSIEM в ОАЦ Республики Беларусь
- доработка продуктов под требования заказчиков
- локальная экспертиза и сопровождение
- интеграция российских технологий с белорусскими решениями

RuSIEM приводит события из разных источников к единой модели анализа

Это позволяет включать в контур решения разных производителей без необходимости перестраивать всю инфраструктуру

Сбор событий → нормализация → обогащение → корреляция → Выявление инцидентов

Подключение различных источников данных

Единые подходы к обработке и корреляции событий

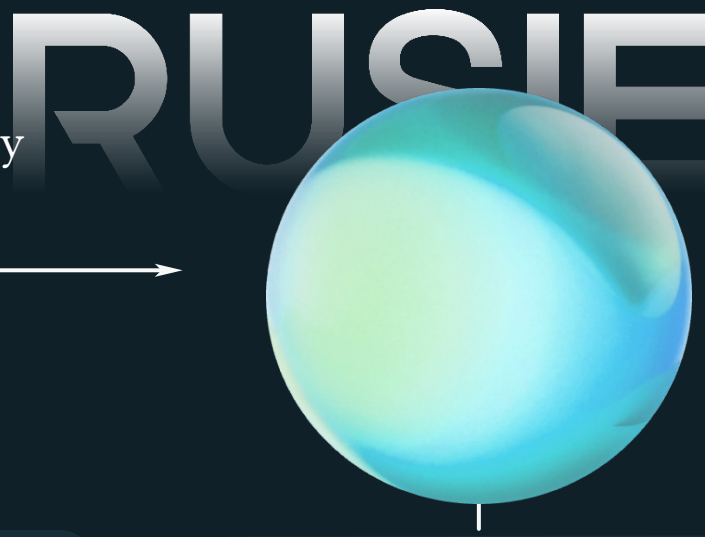
Развитие интеграций с отечественными продуктами

Работа в распределенной инфраструктуре

Совместимость становится не дополнительной функцией продукта, а одним из условий технологической независимости

КАК ФОРМИРУЕТСЯ СОВМЕСТНЫЙ ТЕХНОЛОГИЧЕСКИЙ КОНТУР

Закрытый доверенный контур объединяет российские и белорусские решения без необходимости строить всю инфраструктуру на продуктах одного производителя



Российские и белорусские решения

- Средства защиты
- Сетевое оборудование
- Операционные системы
- Прикладные системы
- Отраслевые ИС

RuSIEM

Ядро мониторинга и анализа событий ИБ

Единый контур контроля

Централизованная картина событий информационной безопасности при сохранении самостоятельности отдельных компонентов инфраструктуры

Архитектура SIEM-системы позволяет постепенно включать новые источники и сценарии контроля

Технологическая база SIEM-системы позволяет выстраивать интеграции с решениями, которые уже используются в инфраструктуре организации

Подключение источников

SIEM получает события от программных и аппаратных решений

Приведение данных к единой модели

События нормализуются и становятся доступными для централизованного анализа независимо от их источника

Единые сценарии контроля

На основе поступающих данных формируются правила корреляции, сценарии выявления угроз и модели реагирования

Централизованный мониторинг

Специалисты получают единую картину происходящего во всей инфраструктуре.

Развитие интеграции

Новые источники и сценарии могут подключаться по мере развития инфраструктуры без перестройки всего контура.

Такой подход позволяет использовать российские технологии в связке с белорусскими решениями и постепенно формировать единый доверенный технологический контур

Схема работы RUSIEM

- Рабочие станции
- Firewall
- Роутеры
- Сетевые коммутаторы
- Серверы
- Мейнфреймы
- Системы обнаружения и предотвращения вторжений

SIEM

- Предупреждения
- Дашборды
- Журнал событий
- Отчеты
- Мониторинг

МОДУЛЬ RUSIEM ioc

Позволяет выявить угрозу для корпоративных устройств в виде попыток связаться с вредоносной инфраструктурой злоумышленника

Модуль подгружает в систему информацию об IP-адресах, доменах, URL

Как только SIEM-система фиксирует в сетевом потоке или хостовой активности обращение к ресурсам, которые есть в базе, она сообщает об этом оператору, указывая, какой конкретно элемент ИТ-инфраструктуры скомпрометирован и требует «лечения»

МОДУЛЬ
RUSIEM Analytics

Выявление поведенческих аномалий на основе статистики в случаях, когда логику инцидента невозможно описать правилами корреляции

Технологичность алгоритмов машинного обучения позволяет выявлять на ранней стадии и предотвращать возможные инциденты ИБ

От интеграции продуктов к технологической платформе Союзного государства

Интеграция отдельных решений

Подключение российского или белорусского продукта к единому контуру мониторинга

типовые сценарии

Формирование готовых моделей взаимодействия для разных классов систем

Инфраструктура предприятия

Объединение информационных систем, средств защиты и распределённых площадок в общий контур контроля

Отраслевой уровень

Применение единого подхода в организациях со схожими технологическими и регуляторными требованиями

Контур Союзного государства

Развитие совместимой российско-белорусской технологической экосистемы с локальной разработкой, поддержкой, сертификацией и компетенциями внутри России и Беларуси

Масштабируется не только программный продукт -- масштабируется сама модель технологического взаимодействия

ВАРИАНТЫ РАЗВЕРТЫВАНИЯ СИСТЕМЫ

RUSIEM

Всё под контролем

Для технологической независимости недостаточно заменить один зарубежный продукт другим

- собственные технологии, которые можно самостоятельно развивать
- локальная экспертиза внутри России и Беларуси
- сертифицированные решения под требования каждого государства
- совместимые продукты, работающие в едином контуре
- совместные разработки, которые можно тиражировать и масштабировать

Связка RuSIEM и BelSIEM позволяет перейти от поставки отдельных продуктов к модели совместной разработки, локализации и интеграции технологий России и Беларуси

ЛИЦЕНЗИРОВАНИЕ RUSIEM

БЕССРОЧНЫЕ
И СРОЧНЫЕ
ЛИЦЕНЗИИ

МОДУЛЬНЫЕ
СПЕЦИФИКАЦИИ

Разработка
Сложных парсеров

Разработка правил
корреляции

Количество
СОБЫТИЙ в секунду

Event per second (EPS)

2 000

3 000

4 000

...

20 000

80 000

100 000

RUSIEM ДЛЯ КРУПНОГО БИЗНЕСА

Безлимитная лицензия

это уникальный вид лицензирования решений RuSIEM
для действительно крупных организаций как коммерческого, так и государственного сектора

НЕОГРАНИЧЕННОЕ КОЛИЧЕСТВО

УСТРОЙСТВ

EPS

УСТАНОВОК

КОЛЛЕКТОРОВ

- Гибкое управление бюджетом
- Неограниченное масштабирование под количество устройств и филиалов
- Индивидуальная поддержка и настройка под задачи бизнеса от вендора
- В среднем на 50% выгоднее по сравнению со стандартными лицензиями

RUSIEM WAF

Сертификат соответствия ФСТЭК России № 5061 от 28.04.2026 г.
по профилю защиты межсетевых экранов типа «Г» 4-го класса защиты (ИТ.МЭ.Г4.ПЗ) и 4-му уровню доверия (УД4)

Реестр российского программного обеспечения - № 32 163 от 17.02.2026

ГРАФИЧЕСКИЙ
Конструктор правил

Гибкая настройка правил

- Выбор фазы работы правила
- Возможность построения каскада правил (срабатывание одного правила активирует работу другого)

Блокировка атак
до их реализации

- SQL-инъекции
- Угрозы из OWASP TOP 10
- Мгновенное реагирование на HTTP/HTTPS-аномалии
- Виртуальный патчинг

Возможность
Запуска в контейне-
ризированной среде

Поддержка
Astra Linux и debian

Высокая
Производительность и Малое
потребление ресурсов

ЛИЦЕНЗИРОВАНИЕ RUSIEM WAF

БЕССРОЧНЫЕ
ЛИЦЕНЗИИ

МОДУЛЬНЫЕ
СПЕЦИФИКАЦИИ

Разработка
правил

Количество
Запросов в секунду

Requests per second (RPS)

250

...

10 000

20 000

80 000

100 000

120 000

ПОДДЕРЖКА НА ВСЕХ ЭТАПАХ ПИЛОТНОГО ПРОЕКТА И В ПРОЦЕССЕ ВНЕДРЕНИЯ

Нам доверяют

ПРОФЕССИОНАЛЬНЫЙ
негосударственный и пенсионный фонд

РОСЭКСИМБАНК

ГЕМОТЕСТ

БИЗКОММ

РСХБ

АКСОН

ЭР-ТЕЛЕКОМ

ЦОДД

ПРИМ
ТЕПЛО
ЭНЕРГО

КРИПТОНИТ

ГКУ СК "Краевой центр
информтехнологий"

DataSpace

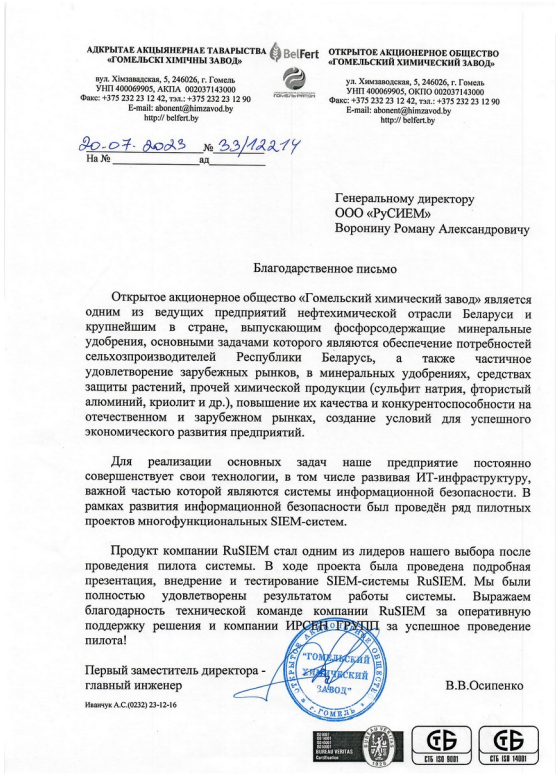
Уралсиб

МегаФон

УСПЕШНЫЕ ПРОЕКТЫ в беларуси

BelFert

Могилёвская ОКБ



АДКРЫТАЕ АКЦЫЯНЕРНАЕ ТАВАРЫСТВА «ГОМЕЛЬСКІ ХІМІЧНЫ ЗАВОД»
вул. Хімзаводская, 5, 246026, г. Гомель
УНП 400069905, АКПА 002037143000
Факс: +375 232 23 12 42, тэл.: +375 232 23 12 90
E-mail: abonent@himzavod.by
http:// belfert.by

ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО «ГОМЕЛЬСКИЙ ХИМИЧЕСКИЙ ЗАВОД»
ул. Химзаводская, 5, 246026, г. Гомель
УНП 400069905, ОКПО 002037143000
Факс: +375 232 23 12 42, тел.: +375 232 23 12 90
E-mail: abonent@himzavod.by
http:// belfert.by

20.07.2023 № 33/12214
На № _____ад_____

Генеральному директору
ООО «РуСИЕМ»
Воронину Роману Александровичу

Благодарственное письмо

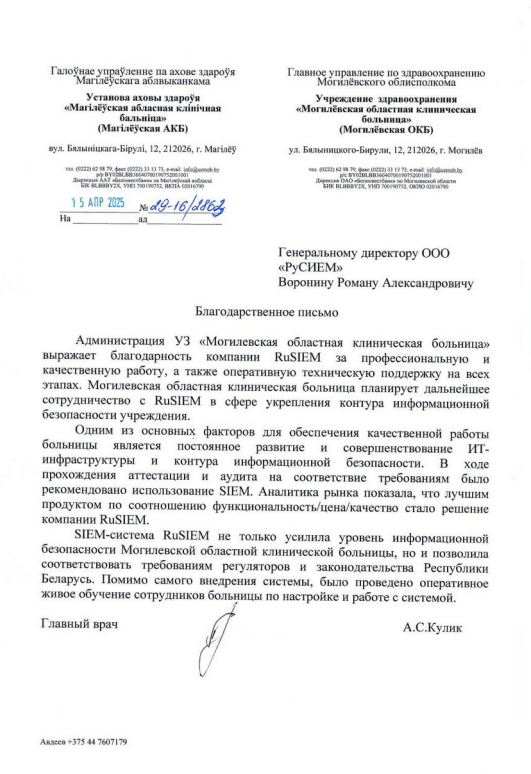
Открытое акционерное общество «Гомельский химический завод» является одним из ведущих предприятий нефтехимической отрасли Беларуси и крупнейшим в стране, выпускающим фосфоросодержащие минеральные удобрения, основными задачами которого являются обеспечение потребностей сельхозпроизводителей Республики Беларусь, а также частичное удовлетворение зарубежных рынков, в минеральных удобрениях, средствах защиты растений, прочей химической продукции (сульфит натрия, фтористый алюминий, криолит и др.), повышение их качества и конкурентоспособности на отечественном и зарубежном рынках, создание условий для успешного экономического развития предприятий.

Для реализации основных задач наше предприятие постоянно совершенствует свои технологии, в том числе развивая ИТ-инфраструктуру, важной частью которой являются системы информационной безопасности. В рамках развития информационной безопасности был проведён ряд пилотных проектов многофункциональных SIEM-систем.

Продукт компании RuSIEM стал одним из лидеров нашего выбора после проведения пилота системы. В ходе проекта была проведена подробная презентация, внедрение и тестирование SIEM-системы RuSIEM. Мы были полностью удовлетворены результатом работы системы. Выражаем благодарность технической команде компании RuSIEM за оперативную поддержку решения и компании ИРОБИ ГРУПП за успешное проведение пилота!

Первый заместитель директора - главный инженер В.В.Осипенко

Иванчук А.С.(0232) 23-12-16



Галоўнае управаўленне па ахове здароўя Магілёўскага аблвыканкама
Установа аховы здароўя «Магілёўская абласная клінічная бальніца» (Магілёўская АКБ)
вул. Бялыніцкага-Бірулі, 12, 212026, г. Магілёў

Главное управление по здравоохранению Могилёвского облисполкома
Учреждение здравоохранения «Могилёвская областная клиническая больница» (Могилёвская ОКБ)
ул. Бялыницкого-Бирули, 12, 212026, г. Могилёв

15 АПР 2025 № 09-16/1863
На _____ад_____

Генеральному директору ООО «РуСИЕМ»
Воронину Роману Александровичу

Благодарственное письмо

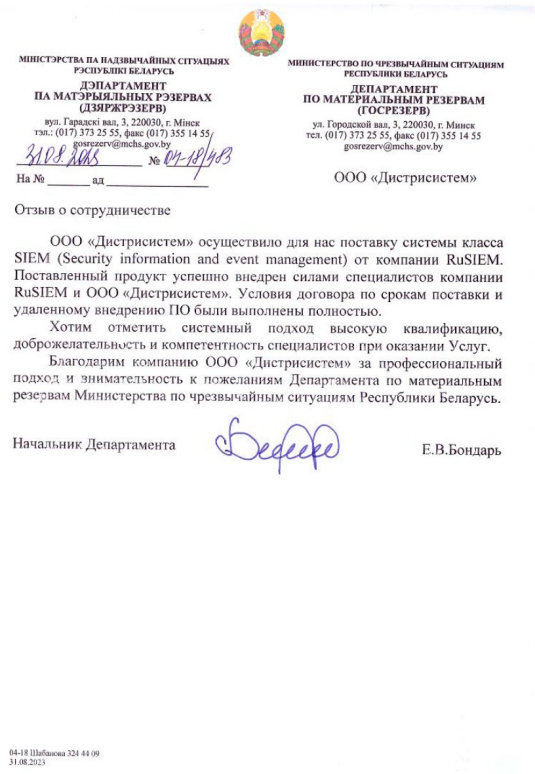
Администрация УЗ «Могилевская областная клиническая больница» выражает благодарность компании RuSIEM за профессиональную и качественную работу, а также оперативную техническую поддержку на всех этапах. Могилевская областная клиническая больница планирует дальнейшее сотрудничество с RuSIEM в сфере укрепления контура информационной безопасности учреждения.

Одним из основных факторов для обеспечения качественной работы больницы является постоянное развитие и совершенствование ИТ-инфраструктуры и контура информационной безопасности. В ходе прохождения аттестации и аудита на соответствие требованиям было рекомендовано использование SIEM. Аналитика рынка показала, что лучшим продуктом по соотношению функциональность/цена/качество стало решение компании RuSIEM.

SIEM-система RuSIEM не только усилила уровень информационной безопасности Могилевской областной клинической больницы, но и позволила соответствовать требованиям регуляторов и законодательства Республики Беларусь. Помимо самого внедрения системы, было проведено оперативное живое обучение сотрудников больницы по настройке и работе с системой.

Главный врач А.С.Кулик

Авдеев +375 44 7607179



МІНІСТЭРСТВА ПА НАДЗВЫЧАЙНЫХ СІТУАЦЫЯХ РЭСПУБЛІКІ БЕЛАРУСЬ
ДЭПАРТАМЕНТ ПА МАТЭРЫЯЛЬНЫХ РЭЗЕРВАХ (ДЗЯРЖРЭЗЕРВ)
вул. Гарадскі вал, 3, 220030, г. Мінск
тэл.: (017) 373 25 55, факс (017) 355 14 55
gosrezerv@mchs.gov.by

МИНИСТЕРСТВО ПО ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ РЕСПУБЛИКИ БЕЛАРУСЬ
ДЕПАРТАМЕНТ ПО МАТЕРИАЛЬНЫМ РЕЗЕРВАМ (ГОСРЕЗЕРВ)
ул. Городской вал, 3, 220030, г. Минск
тел. (017) 373 25 55, факс (017) 355 14 55
gosrezerv@mchs.gov.by

31.08.2023 № 04-18/483
На № _____ад _____

ООО «Дистрисистем»

Отзыв о сотрудничестве

ООО «Дистрисистем» осуществило для нас поставку системы класса SIEM (Security information and event management) от компании RuSIEM. Поставленный продукт успешно внедрен силами специалистов компании RuSIEM и ООО «Дистрисистем». Условия договора по срокам поставки и удаленному внедрению ПО были выполнены полностью.

Хотим отметить системный подход высокую квалификацию, доброжелательность и компетентность специалистов при оказании Услуг.

Благодарим компанию ООО «Дистрисистем» за профессиональный подход и внимательность к пожеланиям Департамента по материальным резервам Министерства по чрезвычайным ситуациям Республики Беларусь.

Начальник Департамента Е.В.Бондарь

04-18 Шабанова 324 44 09
31.08.2023

Галоўнае ўпраўленне па ахове здароўя Магілёўскага абласнога выканаўчага камітэта
Установа аховы здароўя «МАГІЛЁЎСКАЯ АБЛАСНАЯ ДЗІЦЯЧАЯ БАЛЬНІЦА» (Установа аховы здароўя «МАДЗ»)
вул. Бялыніцкага-Бірулі, 9, 212025, г.Магілёў
тэл. (0222) 41-85-65, факс (0222) 41-74-69
E-mail: modb@modb.by
р/с BY22BLBB36040700198143O1001
Дирекция ААТ Белинвестбанк, БІК BLBBBY2X
УНН 700198143 ОКПО 05566143

Главное управление по здравоохранению Могилевского областного исполнительного комитета
Учреждение здравоохранения «МОГИЛЕВСКАЯ ОБЛАСТНАЯ ДЕТСКАЯ БОЛЬНИЦА» (Учреждение здравоохранения «МОДБ»)
ул. Бельницкого-Бирули, 9, 212025, г.Могилев
тел. (0222) 41-85-65, факс (0222) 41-74-69
E-mail: modb@modb.by
р/с BY22BLBB36040700198143O1001
Дирекция ОАО Белинвестбанк, БИК BLBBBY2X
УНН 700198143 ОКПО 05566143

28.03.2025г № 5-1/1032
На _____от _____

Генеральному директору
ООО «РуСИЕМ»
Воронину Роману Александровичу

Благодарственное письмо

Могилевская областная детская больница выражает благодарность специалистам компании RuSIEM за помощь при внедрении и установке SIEM-системы для мониторинга и анализа сетевой активности в инфраструктуру нашего учреждения.

SIEM-система RuSIEM в ходе пилотного тестирования показала свою эффективность и результативность, помогая бесперебойно мониторить и анализировать события информационной безопасности в контуре больницы, тем самым обеспечивая сохранность данных самых юных пациентов Республики.

Благодаря внедренному решению Могилевской областной детской больнице удалось пройти аттестацию, и теперь ИТ-инфраструктура учреждения соответствует всем необходимым государственным стандартам.

Специалисты RuSIEM оказали полную поддержку в ходе внедрения и обучения наших сотрудников. Выражаем благодарность за высокий уровень профессионализма и надеемся на дальнейшее плодотворное сотрудничество.

Главный врач И.Б. Каско

ДЛЯ НАС ГЛАВНОЕ

слышать заказчика и понимать его потребности,

а также активно участвовать в оперативной

реализации запросов

РУСИЕМ

РУСИЕМ

ПОДПИСЫВАЙТЕСЬ В соц. сетях

@rusiem

последние новости,
важные события

@rusiemsupport

возможность быстро связаться с
технической поддержкой

@rusiem В MAX

последние новости,
важные события