

Единая система мониторинга информационной безопасности организации



+7 (495) 748-83-11

info@rusiem.com

rusiem.com



RuSIEM

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

Одна из ведущих высокопроизводительных и полнофункциональных российских SIEM-систем по соотношению цена/качество

RuSIEM сейчас

ТОП
3

отечественных
SIEM-решений



полностью
русская
разработка

x3

рост компании за
последние 3 года



продукт имеет
сертификаты
ФСТЭК России (4 УД),
ОАЦ (Беларусь)

10 лет

продукту
в 2024 году



Продукт включен
в Единый реестр
отечественного ПО

> 630

партнеров в России,
странах СНГ, Азии и
Латинской Америке

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

Схема работы RuSIEM

5



Рабочие станции



Firewall



Роутеры



Сетевые коммутаторы



Серверы



Мейнфреймы



Системы обнаружения
и предотвращения
вторжений

SIEM



Предупреждения



Дашборды



Журнал событий



Отчеты



Мониторинг

Понятный принцип работы RuSIEM

Сбор событий

Контроль инфраструктуры компании

Нормализация событий

Приведение к единому виду представления

Обогащение и симптоматика

Проверка на соответствие симптомам и добавление веса событий

Корреляция событий

Правила корреляции событий

Выявление инцидентов

Составление цепочек событий и оценка риска

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

Линейка продуктов



RuSIEM

коммерческая
версия класса SIEM



RvSIEM (free)

классическое
решение класса LM



RuSIEM IoC

модуль индикаторов
компрометации



RuSIEM Analytics

модуль для анализа
событий, основанный на ML



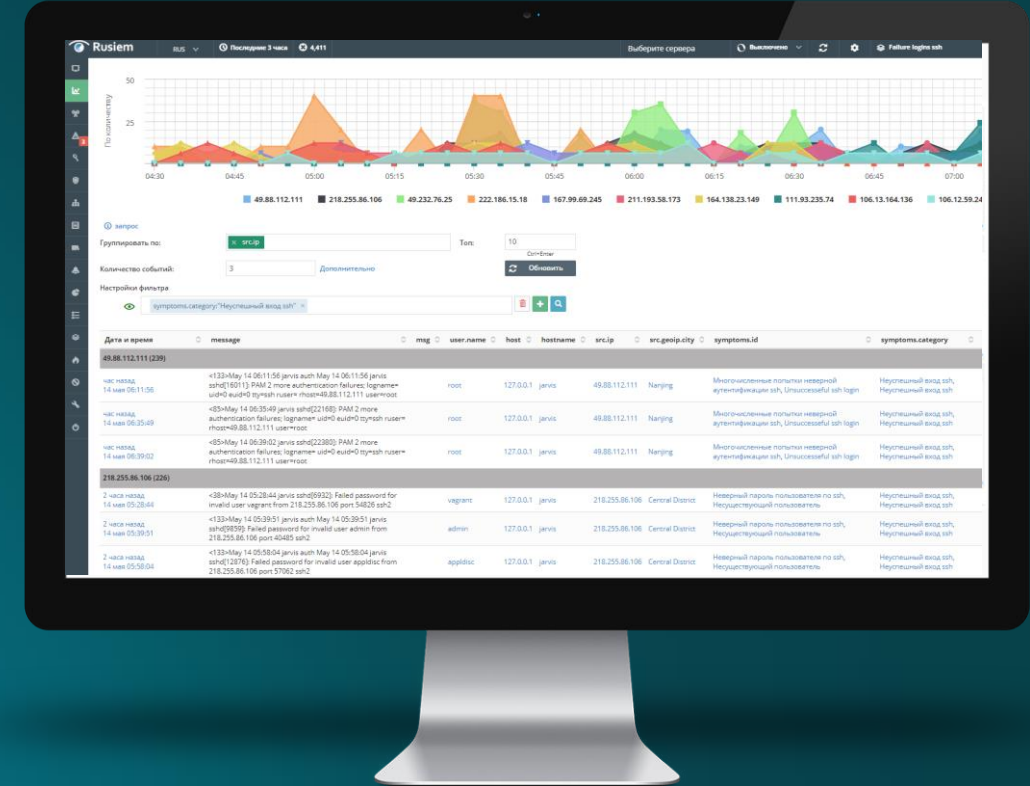
RuSIEM WAF

решение для защиты
веб-приложений

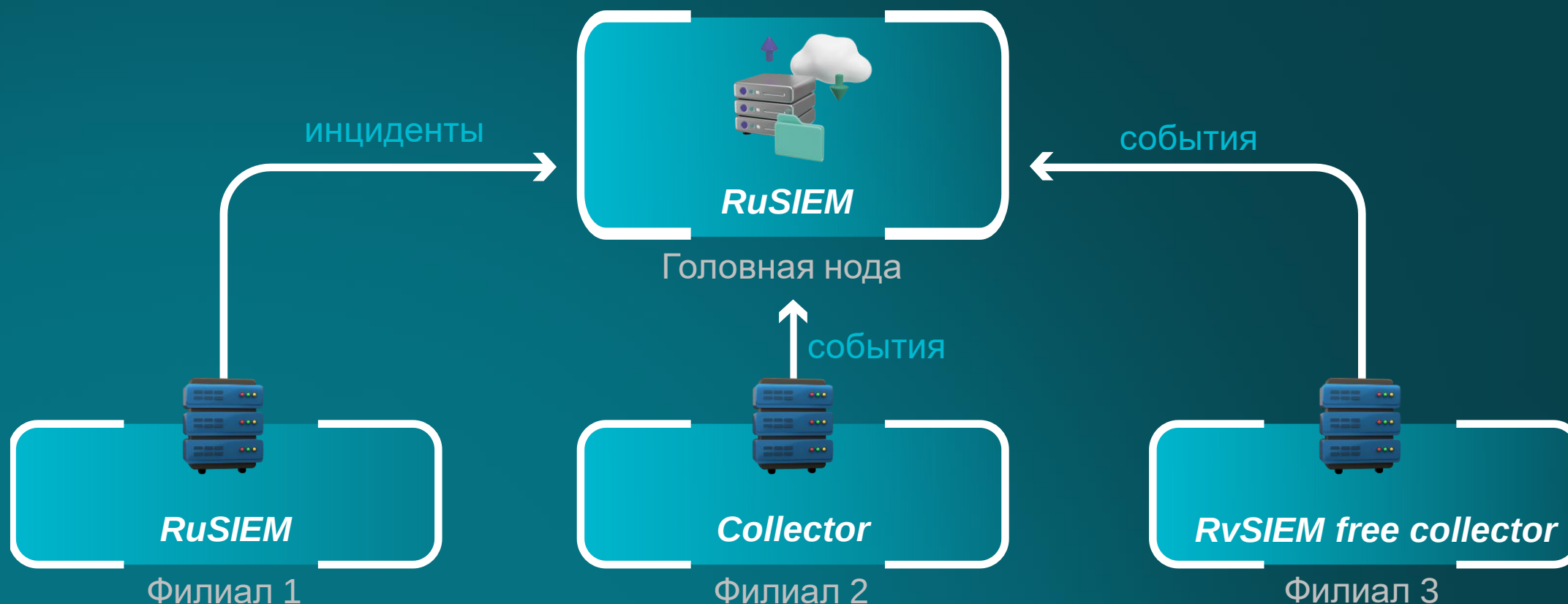
Позволяет выявить угрозу для корпоративных устройств в виде попыток связаться с вредоносной инфраструктурой злоумышленника

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

- 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



Варианты развертывания системы





Одна из самых выгодных SIEM

Информационная безопасность
доступна компаниям любого уровня

Лицензирование RuSIEM

- Модульные спецификации
- БЕССРОЧНЫЕ и срочные лицензии
- 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

...

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

Интеллектуальная система защиты веб-приложений от атак и уязвимостей для оперативного предотвращения угроз, гибкой настройки правил фильтрации и интеграции с системами ИБ

- Конструктор правил
- Гибкая система настройки правил корреляции
 - Выбор фазы работы правила
 - Возможность построения каскада правил (сработка одного правила, провоцирует работу другого)
- Малое потребление ресурсов
- Возможность запуска в контейнеризированной среде
- Поддержка Astra Linux
- Высокая производительность

Лицензирование RuSIEM WAF

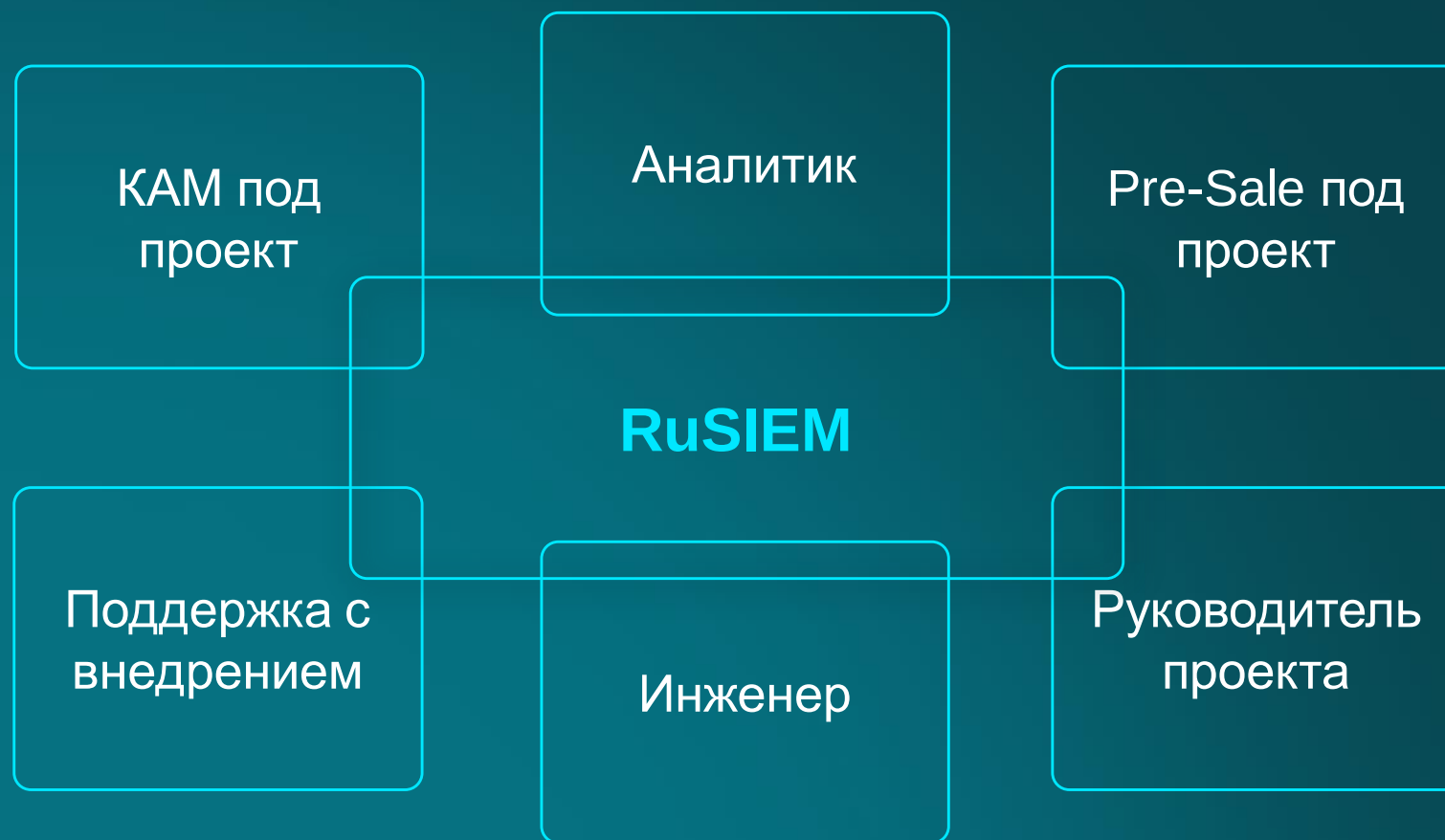
- Модульные спецификации
- БЕССРОЧНЫЕ и срочные лицензии
- Разработка правил

Количество запросов в секунду

Requests per second (RPS)

1
...
10 000
20 000
80 000
100 000
...

Поддержка на всех этапах пилотного проекта и в процессе внедрения



Некоторые успешные проекты

18



DataSpace



ПРОФЕССИОНАЛЬНЫЙ
негосударственный пенсионный фонд



Другие некоторые успешные проекты

19

АКСОН**ПРОФЕССИОНАЛЬНЫЙ**
негосударственный пенсионный фонд**Благодарственное письмо**

Уважаемый Роман Александрович!

Настоящим компания «АКСОН» выражает благодарность ООО «РУСИЕМ» за партнерское участие в реагировании на инцидент информационной безопасности, ликвидацию его последствий и содействие в дальнейшем укреплении периметра защиты компании на базе SIEM-системы собственной разработки компании.

АКСОН — крупнейшая российская динамично развивающаяся сеть магазинов для дома и ремонта с минимальной системой продаж и высоким уровнем логистического сервиса. Компания представлена в 3 федеральных округах, 10 областях и 14 городах. АКСОН занимает 2 место среди отечественных ритейлеров по количеству сервисов крупнейших розничных и оптово-розничных операторов сегмента HardSoft DIY. Значительная доля бизнеса компании приходится на онлайн-каналы: так, ежемесячный трафик интернет-магазина составляет 1 млн посетителей. В этой связи непрерывность практики любых IT-процессов имеет ключевое значение для бизнеса компании.

В марте 2021 года компания подверглась мощнейшей кибератаке. В России на данный момент практически отсутствуют требования к обеспечению требований информационной безопасности информационных систем на стадии их разработки. Очень немногие IT-компании уделяют киберустойчивости своих решений необходимое внимание. В результате даже те организации, где разработаны и внедрены политики и соблюдаются стандарты информационной безопасности, сталкиваются с рисками реализации различных угроз. В нашем случае это была атака преступной группы, которая использовала уязвимости иностранного ПО, получила доступ к системам управления рядом сервисов, перехватила доступ к части из них, зашифровала данные и потребовала уплаты выкупа в течение двух суток. В случае отказа злоумышленники угрожали заблокировать доступ ко всем управляющим серверам, что было бы равносильно полной остановке всех бизнес-процессов.

Необходимо было принять решение: выплатить выкуп и не обращаться за помощью либо найти компанию, которая в оперативном режиме и профессионально обнаружит угрозы, устранит их, заблокирует злоумышленникам доступ к инфраструктуре и установит систему для предотвращения подобных угроз в дальнейшем, а также обратиться за помощью в БСТМ МВД России.

Среди существующих на рынке решений выбор был сделан в пользу решения от ООО «РУСИЕМ». Учитывая территориальную распределенность нашей компании и количества оборудования в каждой локации, ни один другой продукт не решал нашу задачу. Уже в день обращения специалисты компании подключились к расследованию. От обращения до блокировки угрозы и разветвления полноценной SIEM-системы прошло два часа, при этом мы не наблюдали каких-либо сложностей с интеграцией. В течение суток были выявлены точки проникновения и зараженные узлы, ограничено распространение ВПО, изолирован скомпрометированный сегмент сети и выстроен периметр защиты. Собранные данные были переданы сотрудникам органов.

На сегодняшний день система позволила компании «АКСОН» решить следующие ключевые с точки зрения обеспечения непрерывности бизнеса и устойчивости его процессов задачи:

- реализация качественного мониторинга происходящих в инфраструктуре ООО «АКСОН» событий безопасности;
- создание единой точки входа;
- настройка контроля и защиты периметра;
- разработка и внедрение усиленной ИБ-политики.

Решение «РУСИЕМ» помогает нам в реальном времени оценивать защищенность информационных систем и минимизировать риски информационной безопасности. Так, с момента развертывания системы было предотвращено несколько возможных инцидентов.

Иск № 6/4 - от 14.12.2021г.

В ООО «РУСИЕМ»

Благодарственное письмо

ООО СК «УРАЛСИБ СТРАХОВАНИЕ» (ОГРН 1027739608005, ИНН 7806001534, КПП 772801001) (далее – Компания) в лице Заместителя генерального директора по ИТ и операционной деятельности Буто Владислава Андреевича, выражает благодарность ООО «РУСИЕМ» за разработку и внедрение SIEM-системы RuSIEM в Компании, позволившей повысить эффективность выявления потенциальных инцидентов информационной безопасности и обеспечить своевременное реагирование на них. Предложенное компанией ООО «РУСИЕМ» решение позволяет обеспечить контроль соблюдения политики информационной безопасности, решая следующие задачи:

- контроль большого количества событий, поступающих с внутренних систем критических сегментов заказчика и из пользовательских сегментов;
- выявление новых угроз путем корреляции данных из различных источников, включая АРМ, серверную подсистему, сетевые компоненты;
- проверка гипотез при появлении новых уведомлений и угроз;
- централизованное хранение данных и быстрый поиск по событиям информационной безопасности (далее – ИБ);
- поведенческий анализ на базе собранной статистики и выявление случаев отклонения от статистической модели;
- получение уведомлений о выявленных подозрительных событиях в журналы.

Сотрудники ООО «РУСИЕМ» помогли установить систему RuSIEM, подключить источники, написать и доработать ряд парсеров. В результате наша Компания получила инструмент, значительно ускоряющий процесс обработки инцидентов ИБ и обеспечивающий получение требуемой информации о событиях ИБ в консолидированном виде в одном удобном интерфейсе. Благодаря использованию хранилища в системе дополнительной информации, расследовать инциденты стало намного проще.

Мы рассчитываем на то, что с операционной и экономической точки зрения расходы на внедрение системы RuSIEM окупят себя в ближайшее время, т.к. автоматизация обработки инцидентов ИБ позволяет избежать затрат на персонал, необходимый для контроля всех средств защиты информации в ручном режиме. Также хотим отметить, что раннее выявление потенциальных угроз минимизирует возможные экономические потери от потенциальной утечки данных клиентов или хищения денежных средств.

Выражаем искреннюю благодарность коллективу ООО «РУСИЕМ» за профессионализм, оперативность и ответственный подход к решению задач ООО СК «УРАЛСИБ СТРАХОВАНИЕ» полностью удовлетворена качеством работы и уровнем компетенции сотрудников ООО «РУСИЕМ» и рекомендует компанию как надежного партнера.

Заместитель генерального директора по ИТ и операционной деятельности

В.А. Буто



Общество с ограниченной ответственностью
«УРАЛСИБ СТРАХОВАНИЕ»
ИНН 7806001534, ОГРН 1027739608005
т. (495) 784-77-55, факс: (495) 731-00-64
e-mail: info@uralsib.ru

Адрес: ул. Профсоюзная, д. 65, корпус 1, эт. 15, пом. 1517, Москва, Россия, 117342
ОГРН 1027739608005, ИНН 7806001534, КПП 772801001

Адрес: 119180, г. Москва, ул. Чалюшкова, д. 11, эт. 5
Тел.: +7 (495) 003-36-75ОГРН 1147799010022
ИНН/КПП 7701399098/77010001
р/с: 40701810895000001960
БИК: 070701399
к/с: 30101810200000000023
БИК: 044525023иск. № ИСКХ202206011
от 01.06.2022**Благодарственное письмо**

Настоящим Негосударственный пенсионный фонд «Профессиональный» (Акционерное общество) выражает искреннюю благодарность ООО «РУСИЕМ» за помощь во внедрении и технической поддержке системы обнаружения вредоносной активности, мониторинга и управления событиями информационной безопасности на базе SIEM-системы RuSIEM.

SIEM-система RuSIEM позволила НПФ «Профессиональный» (АО) обеспечить соответствие требованиям Положения Банка России от 20.04.2021 № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций».

Отдельно хотелось бы отметить профессионализм, оперативность и ответственный подход сотрудников ООО «РУСИЕМ» по обеспечению информационной безопасности.

Рекомендуем участникам финансового сектора рынка обратить внимание на SIEM-систему RuSIEM при решении задач, связанных с выполнением требований ГОСТ 57580.1-2017.

НПФ «Профессиональный» (АО) заинтересован в дальнейшем сотрудничестве с компанией ООО «РУСИЕМ», развитии и совместной реализации новых масштабных проектов.

Президент



Ю. А. Зверев

ООО «РУСИЕМ»
Генеральному директору
Р.А. Воронину

Юридический адрес: Хлебозаводский проезд, д. 7, стр. 9,
эт. 3, пом. 3, ком. 25, оф. 14, Москва, Россия, 115230
Почтовый адрес: а/я 66, Москва, Россия, 119334
ОГРН 11174602093 // ИНН 7714856880 // КПП 772401002
Телефон: +7 (495) 500-10-65
www.bizkomm.ru

18.04.2022 № ИСКХ-БК-220418/-3
На № от

О направлении благодарственного письма

Уважаемый Роман Александрович!

Благодарю Вас за профессиональный подход, своевременную помощь и техническую поддержку, оказанную специалистами ООО «РУСИЕМ» в ходе реализации мероприятий по созданию информационной системы мониторинга и управления событиями информационной безопасности на базе программного обеспечения «RuSIEM», используемой в ООО «БизКомм» для обеспечения лицензированной деятельности по мониторингу событий информационной безопасности.

С уважением,
Заместитель
генерального директора

А.В. Пестунов

На базе SIEM-системы RuSIEM для ряда крупных заказчиков совместно с партнерами были успешно развернуты и функционируют центры мониторинга информационной безопасности



Для нас главное

Слышать заказчика и понимать его потребности,
а также активно участвовать в оперативной реализации запросов

RuSIEM @rusiem

последние новости, важные события



<https://t.me/rusiem>

RuSIEM Support @rusiemsupport

возможность быстро связаться с технической поддержкой



<https://t.me/rusiemsupport>