RUSIEM
Всё под контролем

Unified system of the information security monitoring in an organization

+7 (495) 748-83-11

info@rusiem.com

rusiem.com

RuSIEM

Russian company engaged in developing solutions for monitoring and managing information security and IT infrastructure events based on the real-time data analysis

---

One of the leading high-performance and fully functional Russian SIEM-systems in terms of price/performance ratio

RuSIEM now

TOP
3
SIEM-systems
in Russia

fully Russian development

x 3
the company's growth over the last 3 years

the product has certificates in Russia and Belarus

11 years
the product's age

the product is included in the Unified Register of the Russian software

> 630
partners in Russia, the CIS countries, Asia, and Latin America

RuSIEM is the core of the information security system

The SIEM technology provides monitoring and event analysis in the real-time mode
Events are originated by network devices and applications
The SIEM technology allows responding to events before the significant damage occurs

What is RuSIEM

- Workstations
- Firewall
- Routers
- Network devices
- Servers
- Mainframes
- Intrusion detection and prevention systems

SIEM

- **Warnings**
- **Dashboards**
- **Event Logs**
- **Reports**
- **Monitoring**

RuSIEM operation principle

Events collection

Company infrastructure control

Events normalization

Bringing to a uniform representation form

Enrichment and symptoms

Checking for symptom compliance and events weight adding

Events correlation

Event correlation rules

Incident detection

Event chains development and risk assessment

What makes RuSIEM unique?

No event missing

No-code

Maximum pre-installed functionality

Intuitive and user-friendly interface

Any data sources connection

Real-time and historical correlation

Optimal price/quality ratio

Development and support from the vendor

Product line

RuSIEM
commercial
SIEM-class version

RvSIEM (free)
traditional
LM-class solution

RuSIEM IoC
module of compromise
indicators

RuSIEM WAF
solution for
web application
protection

RuSIEM Analytics
module for the commercial version,
supplemented with DL

RuSIEM IoC

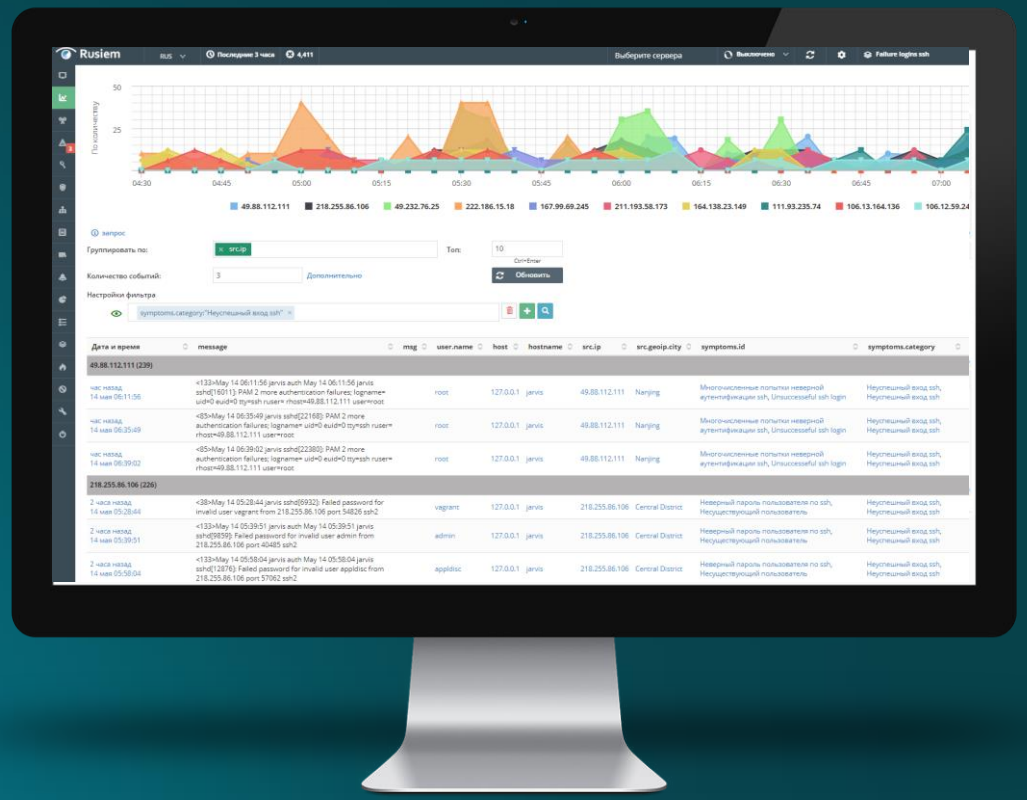
The module allows to identify a threat to corporate devices in the form of attempts to connect with the malicious infrastructure of the attacker

The module downloads information about IP-addresses, domains, URLs and malware hashes into the system

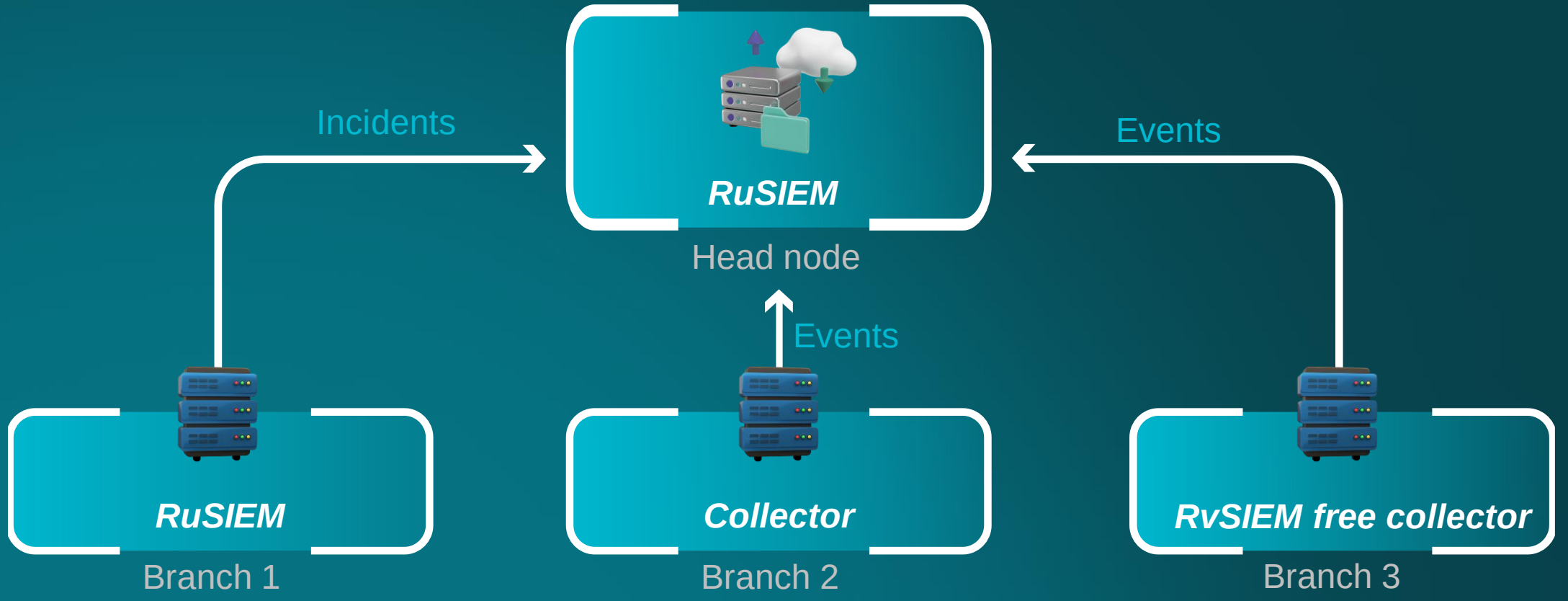
- As soon as the SIEM-system detects in the network traffic or host activity any requests to resources that are in the database, it notifies the operator, indicating which specific element of the IT infrastructure is compromised and requires ‘treatment'

RuSIEM Analytics

- The detection of behavioral anomalies based on statistics in cases where the incident logic cannot be described by the correlation rules
- The technological capabilities of machine learning algorithms allow early detection and prevention of potential information security incidents



The system deployment options



The Solution – RuSIEM

RUSIEM
Всё под контролем

One of the most profitable SIEMs

Information security is available to companies of any level

RuSIEM licensing

- Modular specifications
- UNLIMITED and fixed-term licenses
- Complex parsers development
- Correlation rules development

Number of events per second

Events per second (EPS)

2 000
3 000
4 000
…

20 000
80 000
100 000
…

Unlimited license

a unique type of licensing for RuSIEM solutions
for truly large organizations in both the commercial and public sectors

Unlimited number

devices **EPS** **installations** **collectors**

- Flexible budget management
- Unlimited scaling for the number of devices and branches
- Individual support and customization for business tasks from the vendor
- On average, **50% more cost-effective** in comparison to the standard licenses

RuSIEM WAF

An intelligent web application protection system against attacks and vulnerabilities for proactive threat prevention, flexible rule filtering configuration, and integration with cybersecurity systems

- Rule constructor
- Flexible rule correlation adjustment system
  - Selection of the rule operation phase
  - The ability to create a cascade of rules (the triggering of one rule provokes the operation of the other one)
- Low resource consumption
- Ability to run in a containerized environment
- High performance

RuSIEM WAF licensing

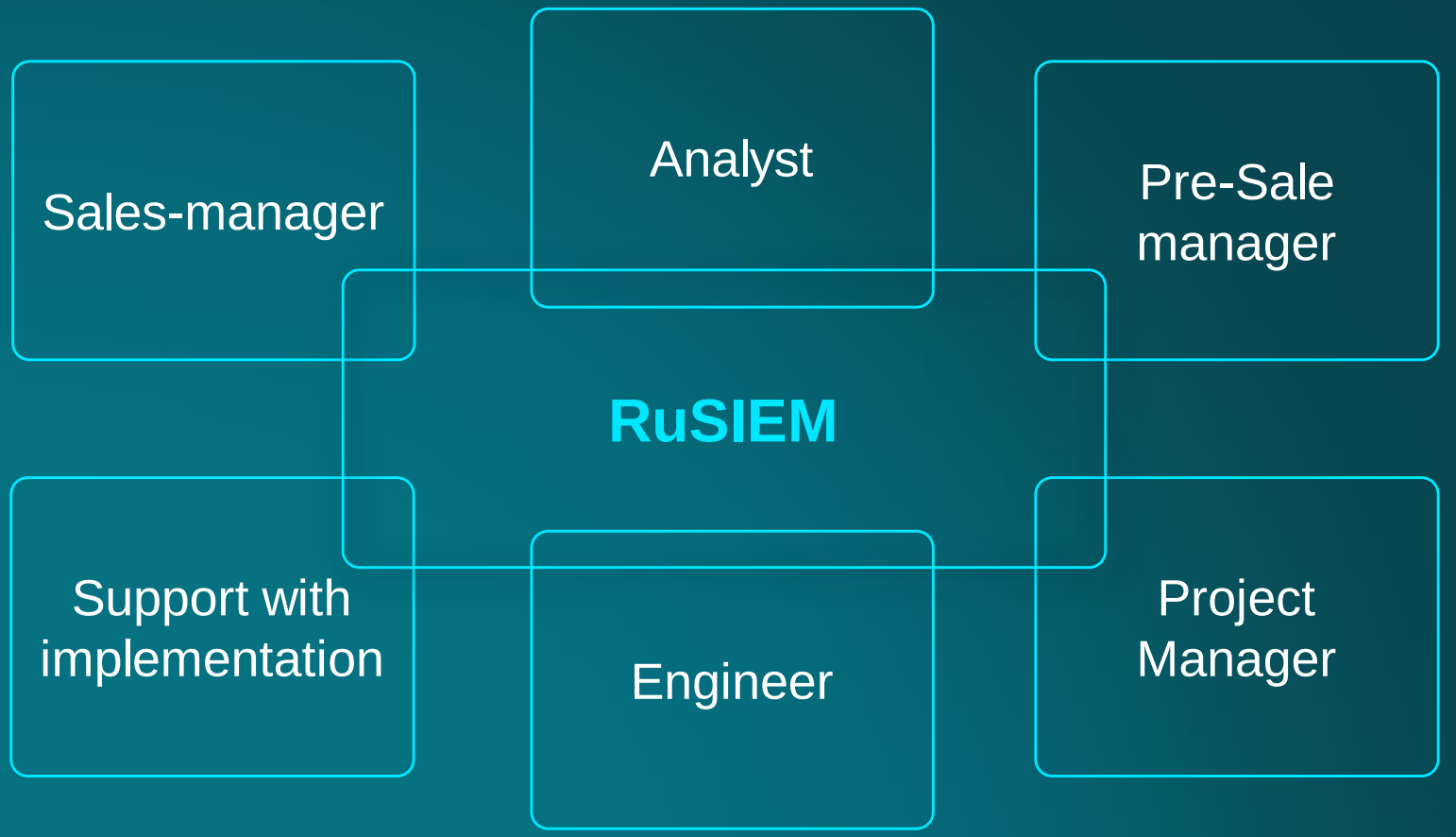
- Modular specifications
- UNLIMITED and fixed-term licenses
- Correlation rules development

Number of requests per second

Requests per second (RPS)

1
…
10 000
20 000
80 000
100 000
…

We offer support at all stages of the pilot project and during the implementation process



Some successful projects

БИЗКОММ

АКСОН

ГЕМОТЕСТ
МЕДИЦИНСКАЯ ЛАБОРАТОРИЯ

РОСЭКСИМБАНК

ЦОДД

ГКУ СК «КРАЕВОЙ ЦЕНТР ИНФОРМТЕХНОЛОГИЙ»

РСХБ
страхование

КРИПТОНИТ

DataSpace

УРАЛСИБ
СТРАХОВАНИЕ

ПРОФЕССИОНАЛЬНЫЙ
негосударственный пенсионный фонд

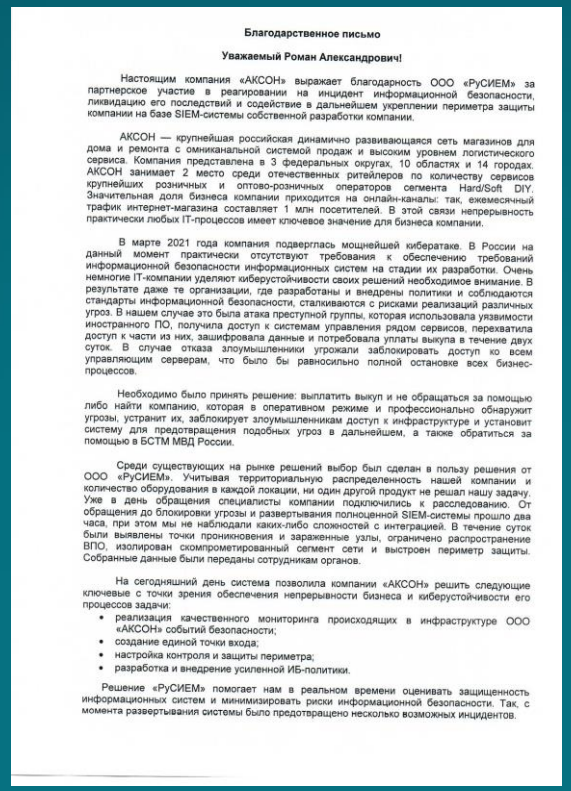
ПРИМ ТЕПЛО ЭНЕРГО

ЭР·ТЕЛЕКОМ

МегаФон

Other successful projects

АКСОН



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 омниканальной 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 Hard/Soft DIY. Значительная доля бизнеса компании приходится на онлайн-каналы: так, ежемесячный трафик интернет-магазина составляет 1 млн посетителей. В этой связи непрерывность практически 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 реализаций 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.

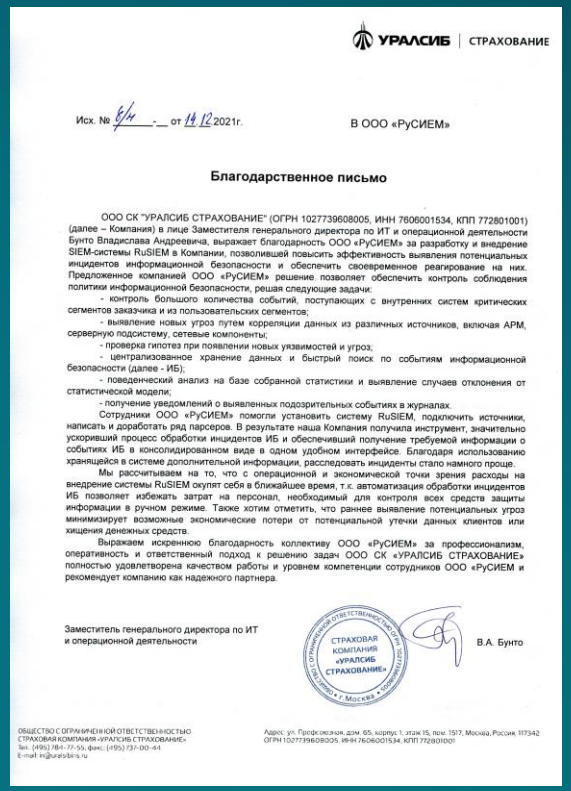
Среди существующих на рынке решений выбор был сделан в пользу решения от ООО «РуСИЕМ». Учитывая территориальную распределенность нашей компании и количество оборудования в каждой локации, ни один другой продукт не решал нашу задачу. Уже в день обращения специалисты компании подключились к расследованию. От обращения до блокировки угрозы и развертывания 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 киберустойчивости 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.

УРАЛСИБ



УРАЛСИБ | СТРАХОВАНИЕ

Исх. № 6/4 от 14.12.2021г.

В ООО «РуСИЕМ»

Благодарственное письмо

ООО СК "УРАЛСИБ СТРАХОВАНИЕ" (ОГРН 1027739608005, ИНН 7606001534, КПП 772801001) (далее – Компания) в лице Заместителя генерального директора по ИТ и операционной деятельности Бунто 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 уязвимостей 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 журналах.

Сотрудники ООО «РуСИЕМ» помогли установить систему RuSIEM, подключить источники, написать и доработать ряд парсеров. В результате наша Компания получила инструмент, значительно ускоривший процесс обработки инцидентов ИБ и обеспечивший получение требуемой информации о событиях ИБ в консолидированном виде в одном удобном интерфейсе. Благодаря использованию хранящейся 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

СТРАХОВАЯ КОМПАНИЯ «УРАЛСИБ СТРАХОВАНИЕ»

В.А. Бунто

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ СТРАХОВАЯ КОМПАНИЯ «УРАЛСИБ СТРАХОВАНИЕ»
Тел.: (495) 784-77-55, факс: (495) 737-00-44
E-mail: in@uralsibins.ru

Адрес: ул. Профсоюзная, дом 65, корпус 1, этаж 15, пом. 1517, Москва, Россия, 117342
ОГРН 1027739608005, ИНН 7606001534, КПП 772801001

ПРОФЕССИОНАЛЬНЫЙ
негосударственный пенсионный фонд

Негосударственный пенсионный фонд
Профессиональный

Адрес:
101000, г. Москва, ул. Чаплыгина, д. 11, эт. 5
Тел.: +7 (495) 003-36-75

ОГРН 1147799010325
ИНН/КПП 7701109908/770101001
р/с 40701810895000001960
Банк ГПБ (АО), г. Москва
к/с 30101810200000000823
БИК 044525823

исх. № ИСХ202206011
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».

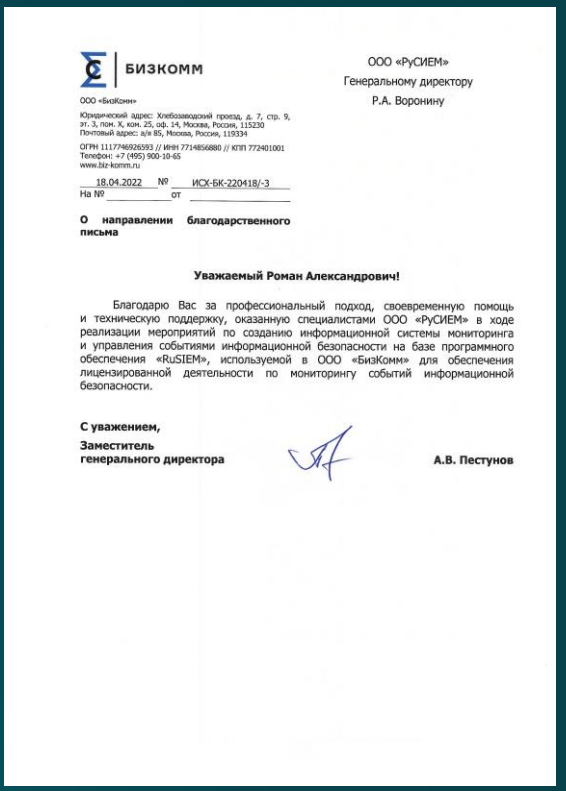
Отдельно хотелось бы отметить профессионализм, оперативность и ответственный подход сотрудников ООО «РуСИЕМ» по обеспечению информационной безопасности.

Рекомендуем участникам финансового сектора рынка обратить внимание на SIEM-систему RuSIEM при решении задач, связанных с выполнениями 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**

БИЗКОМ



БИЗКОМ

ООО «РуСИЕМ»
Генеральному директору
Р.А. Воронину

ООО «БизКомм»

Юридический адрес: Хлебозаводский проезд, д. 7, стр. 9, эт. 3, пом. X, ком. 25, оф. 14, Москва, Россия, 115230
Почтовый адрес: а/я 85, Москва, Россия, 119334

ОГРН 1117746926593 // ИНН 7714856880 // КПП 772401001
Телефон: +7 (495) 900-10-65
www.biz-komm.ru

18.04.2022 № ИСХ-БК-220418/-3
На № от

О направлении благодарственного письма

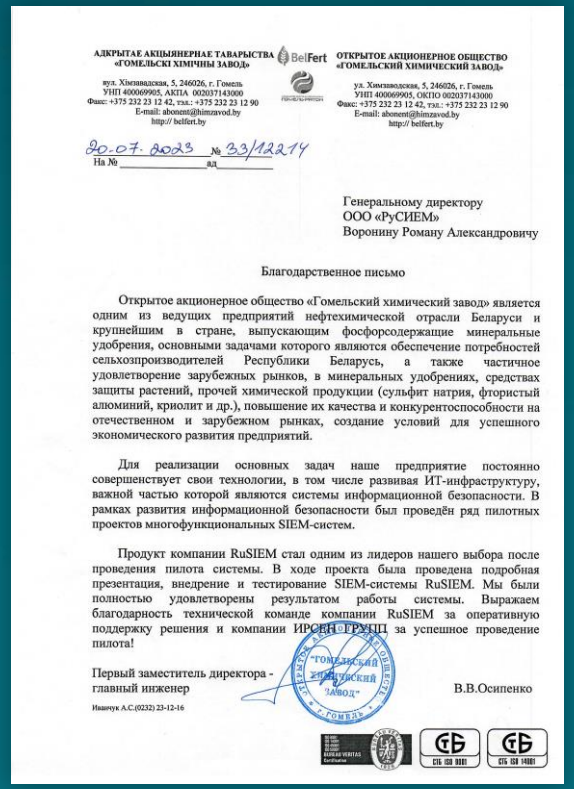
Уважаемый Роман Александрович!

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**

Other successful projects



АДКРЫТАЕ АКЦЫЯНЕРНАЕ ТАВАРЫСТВА «ГОМЕЛЬСКІ ХІМІЧНЫ ЗАВОД»
вул. Хімзавадская, 5, 246026, г. Гомель
УНП 400069005, 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 400069005, 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

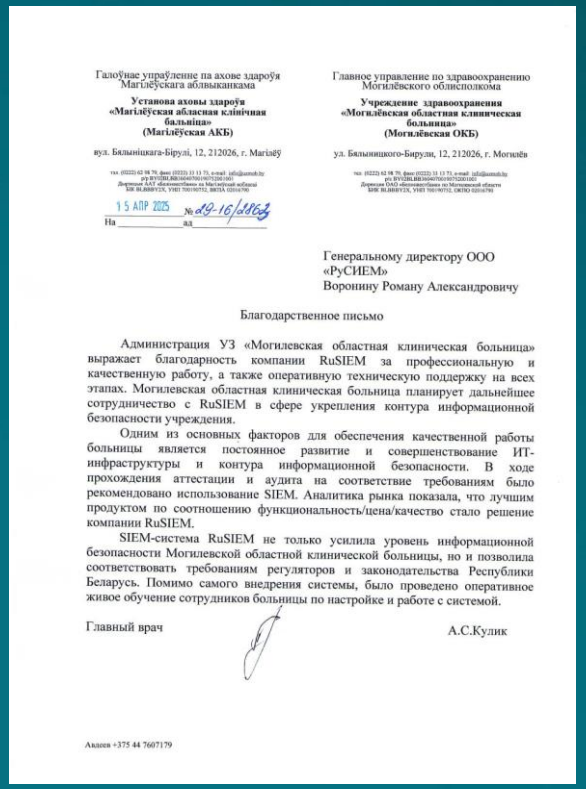
Открытое акционерное общество «Гомельский химический завод» является одним из ведущих предприятий нефтехимической отрасли Беларуси и крупнейшим в стране, выпускающим фосфорсодержащие минеральные удобрения, основными задачами которого являются обеспечение потребностей сельхозпроизводителей Республики 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 ИРСВ ГРУПП за успешное проведение пилота!

Первый заместитель директора - главный инженер В.В.Осипенко

Иванчук А.С.(0232) 23-12-16



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

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

15 АПР 2025 № 29-16/2863
На _____ ад _____

Генеральному директору ООО «РуСИЕМ»
Воронину Роману Александровичу

Благодарственное письмо

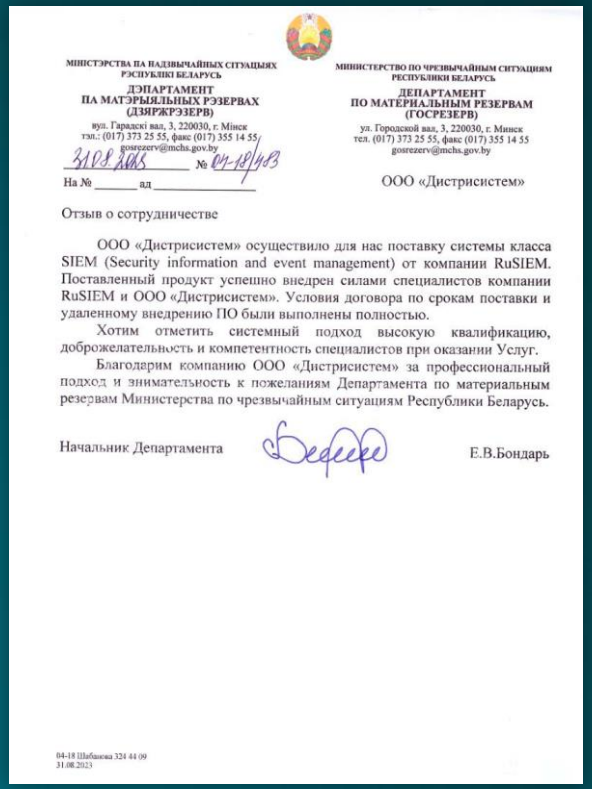
Администрация УЗ «Могилевская областная клиническая больница» выражает благодарность компании RuSIEM за профессиональную и качественную работу, а также оперативную техническую поддержку на всех этапах. Могилевская областная клиническая больница планирует дальнейшее сотрудничество с RuSIEM в сфере укрепления 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 № 07-18/483
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 Шабашова 324 44 09
31.08.2023

Галоўнае ўпраўленне па ахове здароўя Магілёўскага аблвыканкама выканаўчага камітэта
Установа аховы здароўя «МАГІЛЁЎСКАЯ АБЛАСНАЯ ДЗІЦЯЧАЯ БАЛЬНІЦА» (Установа аховы здароўя «МАДБ»)
вул. Бальнічная-Бірулі, 9, 212025, г.Магілёў
тэл. (0222) 41-85-65, факс (0222) 41-74-69
E-mail: modb@modb.by
р/с BY22BLBB36040700198143001001
Дирекция ААТ«Беларусбанк»,БІК BLBBBY2X
УНН 700198143 ОКПО 05566143

Главное управление по здравоохранению Могилевского областного исполнительного комитета
Учреждение здравоохранения «МОГИЛЕВСКАЯ ОБЛАСТНАЯ ДЕТСКАЯ БОЛЬНИЦА» (Учреждение здравоохранения «МОДБ»)
ул. Больничного-Бирули, 9, 212025, г.Могилев
тел.(0222) 41-85-65, факс (0222) 41-74-69
E-mail: modb@modb.by
р/с BY22BLBB36040700198143001001
Дирекция ОАО«Белгазпромбанк»,БІК 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 беспрерывно 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

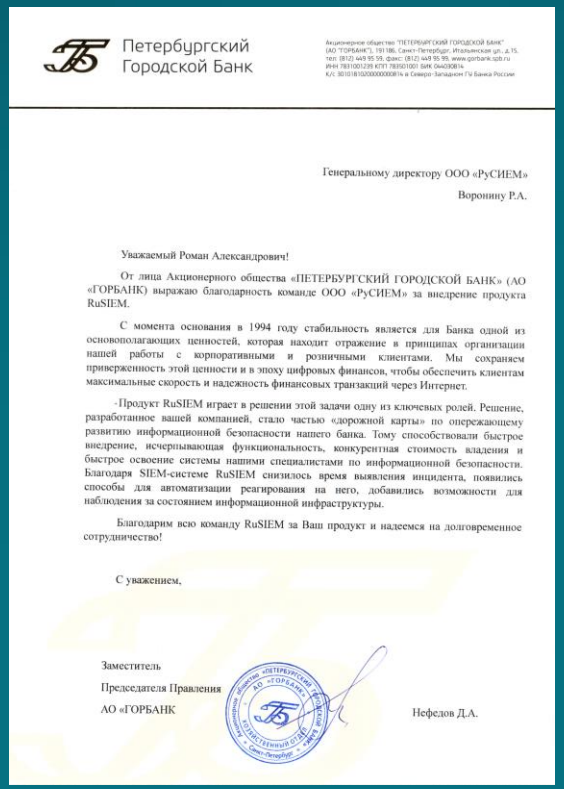
Other successful projects

Петербургский Городской Банк

Коммерческий Индо Банк

ИНСТИТУТ АЭРОНАВИГАЦИИ

ДЕРЖАВА БАНК



Петербургский Городской Банк

Акционерное общество "ПЕТЕРБУРГСКИЙ ГОРОДСКОЙ БАНК"
(АО "ГОРБАНК"), 191186, Санкт-Петербург, Итальянская ул., д.15,
тел: (812) 449 95 55, факс: (812) 449 95 99, www.gorbank.spb.ru
ИНН 7831001235 КПП 783501001 БИК 044030814
К/с 30101810200000000814 в Северо-Западном ГУ Банка России

Генеральному директору ООО «РуСИЕМ»
Воронину Р.А.

Уважаемый Роман Александрович!

От лица Акционерного общества «ПЕТЕРБУРГСКИЙ ГОРОДСКОЙ БАНК» (АО «ГОРБАНК») выражаю благодарность команде ООО «РуСИЕМ» за внедрение продукта RuSIEM.

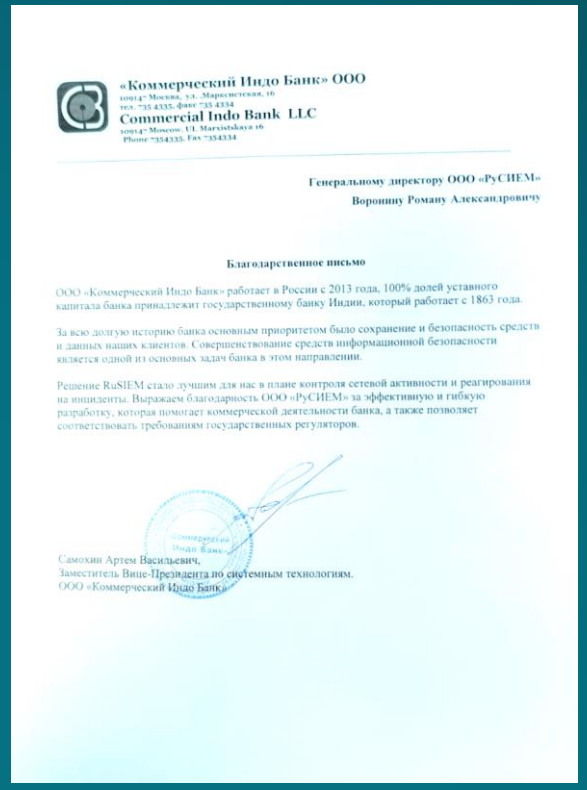
С момента основания в 1994 году стабильность является для Банка одной из основополагающих ценностей, которая находит отражение в принципах организации нашей работы с корпоративными и розничными клиентами. Мы сохраняем приверженность этой ценности и в эпоху цифровых финансов, чтобы обеспечить клиентам максимальные скорость и надежность финансовых транзакций через Интернет.

Продукт RuSIEM играет в решении этой задачи одну из ключевых ролей. Решение, разработанное вашей компанией, стало частью «дорожной карты» по опережающему развитию информационной безопасности нашего банка. Тому способствовали быстрое внедрение, исчерпывающая функциональность, конкурентная стоимость владения и быстрое освоение системы нашими специалистами по информационной безопасности. Благодаря SIEM-системе RuSIEM снизилось время выявления инцидента, появились способы для автоматизации реагирования на него, добавились возможности для наблюдения за состоянием информационной инфраструктуры.

Благодарим всю команду RuSIEM за Ваш продукт и надеемся на долговременное сотрудничество!

С уважением,

Заместитель
Председателя Правления
АО «ГОРБАНК» Нефедов Д.А.



«Коммерческий Индо Банк» ООО
109147 Москва, ул. Марксистская, 16
тел. 735 4335, факс 735 4334
Commercial Indo Bank LLC
109147 Moscow, Ul. Marxistskaya 16
Phone 735 4335, Fax 735 4334

Генеральному директору ООО «РуСИЕМ»
Воронину Роману Александровичу

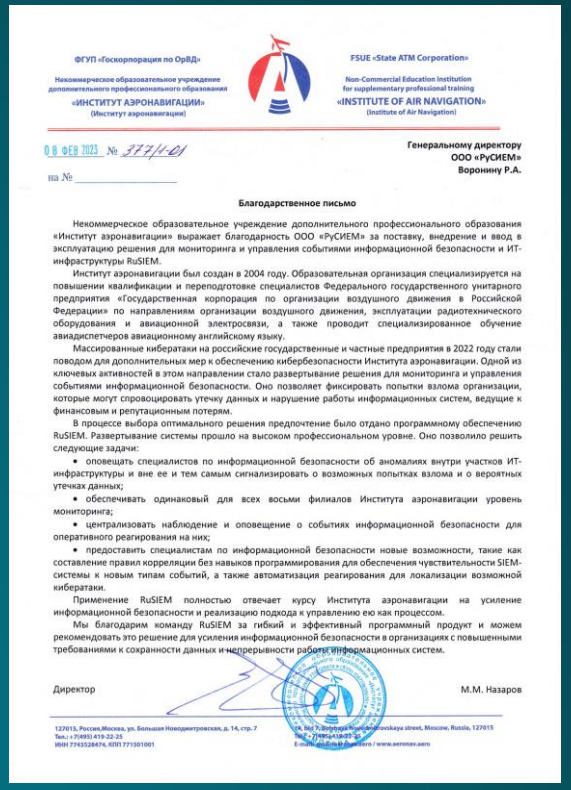
Благодарственное письмо

ООО «Коммерческий Индо Банк» работает в России с 2013 года, 100% долей уставного капитала банка принадлежит государственному банку Индии, который работает с 1863 года.

За всю долгую историю банка основным приоритетом было сохранение и безопасность средств и данных наших клиентов. Совершенствование средств информационной безопасности является одной из основных задач банка в этом направлении.

Решение RuSIEM стало лучшим для нас в плане контроля сетевой активности и реагирования на инциденты. Выражаем благодарность ООО «РуСИЕМ» за эффективную и гибкую разработку, которая помогает коммерческой деятельности банка, а также позволяет соответствовать требованиям государственных регуляторов.

Самохин Артем Васильевич,
Заместитель Вице-Президента по системным технологиям.
ООО «Коммерческий Индо Банк»



ФГУП «Госкорпорация по ОрВД»
Некоммерческое образовательное учреждение дополнительного профессионального образования
«ИНСТИТУТ АЭРОНАВИГАЦИИ»
(Институт аэронавигации)

FSUE «State ATM Corporation»
Non-Commercial Education Institution for supplementary professional training
«INSTITUTE OF AIR NAVIGATION»
(Institute of Air Navigation)

06 ФЕВ 2023 № 377/1-01
на №

Генеральному директору
ООО «РуСИЕМ»
Воронину Р.А.

Благодарственное письмо

Некоммерческое образовательное учреждение дополнительного профессионального образования «Институт аэронавигации» выражает благодарность ООО «РуСИЕМ» за поставку, внедрение и ввод в эксплуатацию решения для мониторинга и управления событиями информационной безопасности и ИТ-инфраструктуры RuSIEM.

Институт аэронавигации был создан в 2004 году. Образовательная организация специализируется на повышении квалификации и переподготовке специалистов Федерального государственного унитарного предприятия «Государственная корпорация по организации воздушного движения в Российской Федерации» по направлениям организации воздушного движения, эксплуатации радиотехнического оборудования и авиационной электросвязи, а также проводит специализированное обучение авиадиспетчеров авиационному английскому языку.

Массированные кибератаки на российские государственные и частные предприятия в 2022 году стали поводом для дополнительных мер к обеспечению кибербезопасности Института аэронавигации. Одной из ключевых активностей в этом направлении стало развертывание решения для мониторинга и управления событиями информационной безопасности. Оно позволяет фиксировать попытки взлома организации, которые могут спровоцировать утечку данных и нарушение работы информационных систем, ведущие к финансовым и репутационным потерям.

В процессе выбора оптимального решения предпочтение было отдано программному обеспечению RuSIEM. Развертывание системы прошло на высоком профессиональном уровне. Оно позволило решить следующие задачи:

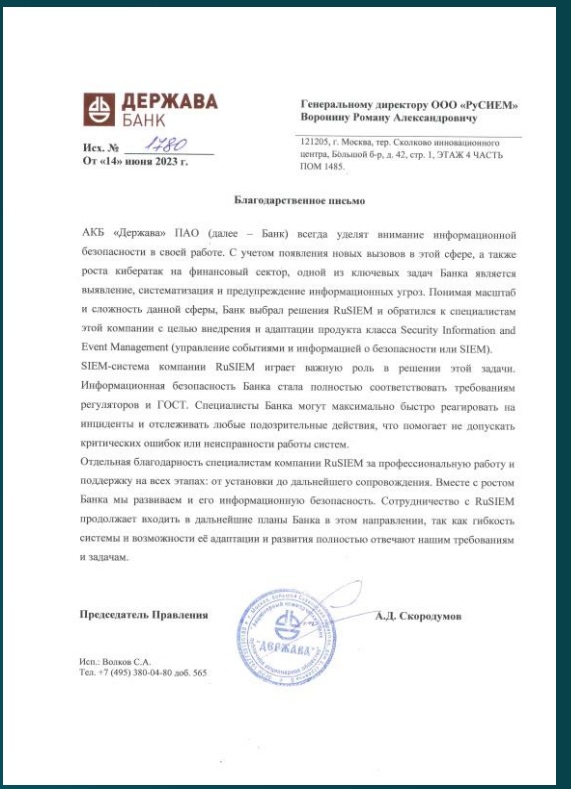
- оповещать специалистов по информационной безопасности об аномалиях внутри участков ИТ-инфраструктуры и вне ее и тем самым сигнализировать о возможных попытках взлома и о вероятных утечках данных;
- обеспечивать одинаковый для всех восьми филиалов Института аэронавигации уровень мониторинга;
- централизовать наблюдение и оповещение о событиях информационной безопасности для оперативного реагирования на них;
- предоставить специалистам по информационной безопасности новые возможности, такие как составление правил корреляции без навыков программирования для обеспечения чувствительности SIEM-системы к новым типам событий, а также автоматизация реагирования для локализации возможной кибератаки.

Применение RuSIEM полностью отвечает курсу Института аэронавигации на усиление информационной безопасности и реализацию подхода к управлению ею как процессом.

Мы благодарим команду RuSIEM за гибкий и эффективный программный продукт и можем рекомендовать это решение для усиления информационной безопасности в организациях с повышенными требованиями к сохранности данных и непрерывности работы информационных систем.

Директор М.М. Назаров

127015, Россия, Москва, ул. Большая Новодмитровская, д. 14, стр. 7
Тел.: +7(495) 419-22-25
ИНН 7743528474, КПП 771501001



ДЕРЖАВА БАНК

Исх. № 1480
От «14» июня 2023 г.

Генеральному директору ООО «РуСИЕМ»
Воронину Роману Александровичу

121205, г. Москва, тер. Сколково инновационного центра, Большой б-р, д. 42, стр. 1, ЭТАЖ 4 ЧАСТЬ ПОМ 1485.

Благодарственное письмо

АКБ «Держава» ПАО (далее – Банк) всегда уделял внимание информационной безопасности в своей работе. С учетом появления новых вызовов в этой сфере, а также роста кибератак на финансовый сектор, одной из ключевых задач Банка является выявление, систематизация и предупреждение информационных угроз. Понимая масштаб и сложность данной сферы, Банк выбрал решения RuSIEM и обратился к специалистам этой компании с целью внедрения и адаптации продукта класса Security Information and Event Management (управление событиями и информацией о безопасности или SIEM).

SIEM-система компании RuSIEM играет важную роль в решении этой задачи. Информационная безопасность Банка стала полностью соответствовать требованиям регуляторов и ГОСТ. Специалисты Банка могут максимально быстро реагировать на инциденты и отслеживать любые подозрительные действия, что помогает не допускать критических ошибок или неисправности работы систем.

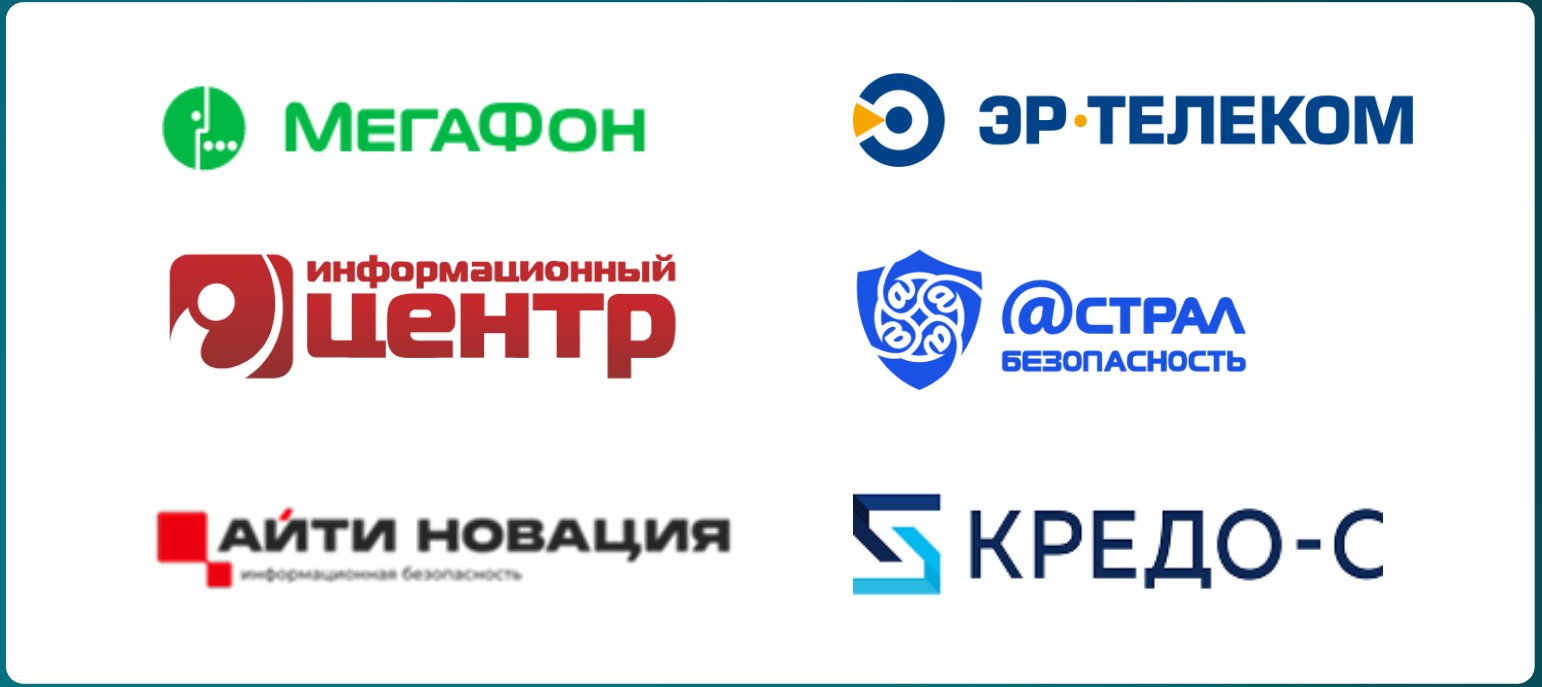
Отдельная благодарность специалистам компании RuSIEM за профессиональную работу и поддержку на всех этапах: от установки до дальнейшего сопровождения. Вместе с ростом Банка мы развиваем и его информационную безопасность. Сотрудничество с RuSIEM продолжает входить в дальнейшие планы Банка в этом направлении, так как гибкость системы и возможности её адаптации и развития полностью отвечают нашим требованиям и задачам.

Председатель Правления А.Д. Скородумов

Исп.: Волков С.А.
Тел. +7 (495) 380-04-80 доб. 565

SOC based on RuSIEM

The Information Security Monitoring Center (Security Operations Center, SOC) based on RuSIEM was deployed for a number of large customers together with the following partners



The main thing for us is

to hear our clients and understand their needs,
as well as actively participate in the operational implementation of the requests

Join us in Telegram

RuSIEM **@rusiem**

our latest news, important events

https://t.me/rusiem

RuSIEM Support **@rusiemsupport**

quick contact our technical support

https://t.me/rusiemsupport