RUSIEM
Всё под контролем

Единая система мониторинга информационной безопасности организации

Альбина Бухарова
Менеджер по работе с ключевыми заказчиками

Какие задачи решает SIEM

- Оперативное обнаружение инцидентов, контроль обработки инцидентов, сбор доказательной базы для дальнейшего расследования
- Контроль состояния инфраструктуры компании
- Создание единого центра мониторинга
- Определение прав, обязанностей и разграничение зон ответственности персонала компании (ИТ- и ИБ-служб)
- Соответствие требованиям регуляторов

О компании «РуСИЕМ»

2014 — Старт разработки

Sk Сколково — Резидент Сколково

> 20000 — Установок free-версии в мире с 2017 года

SIEM-система RuSIEM

- Сертификат соответствия ФСТЭК России (№ 4402)
- Единый реестр российского ПО (№ 3808)
- Сертификат ОАЦ при Президенте Республики Беларусь (партиями)

>550 партнёров в России и СНГ

>150 реализованных проектов для коммерческих и государственных организаций

Почему RuSIEM?

Российская разработка, техническая поддержка на русском языке

Решение подойдет **компаниям любого масштаба**

Система быстро разворачивается, **проста в освоении**

Технологичность алгоритмов машинного обучения **в процессе поиска аномалий**

Оптимальное соотношение цена/качество **на рынке России и СНГ**

100% гарантия доставки событий в SIEM **благодаря особенностям микросервисной архитектуры**

Более 400 правил корреляции для **анализа событий**

Удобство написания правил корреляции и парсеров

Линейка продуктов

RvSIEM (free)
– классическое решение класса LM

RuSIEM
– коммерческая версия класса SIEM

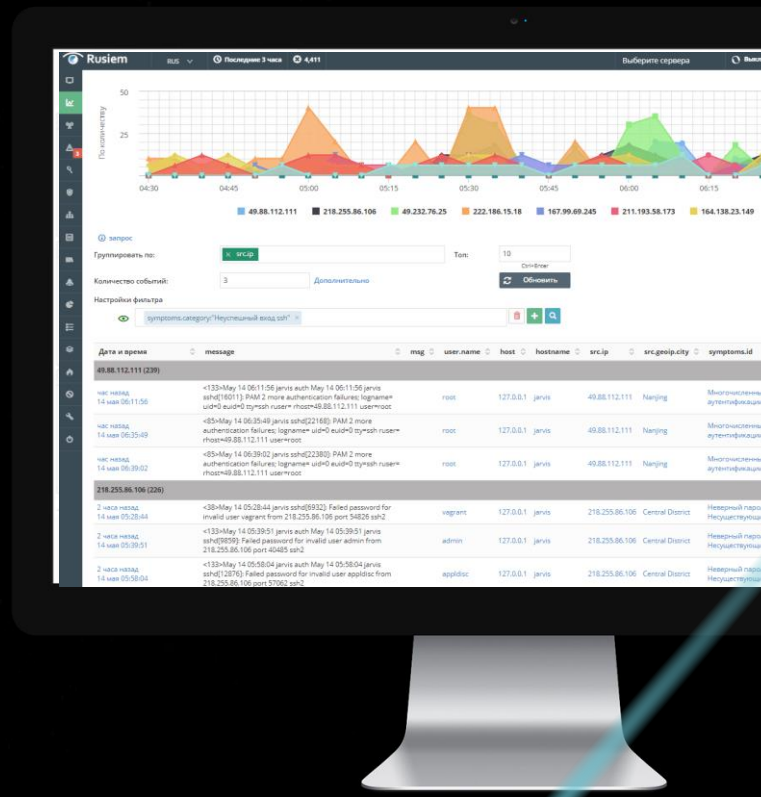
RuSIEM Analytics
– модуль для анализа событий, основанный на ML

RuSIEM IoC
– модуль индикаторов компрометации

RuSIEM Monitoring
– модуль мониторинга информационных систем, узлов, приложений

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

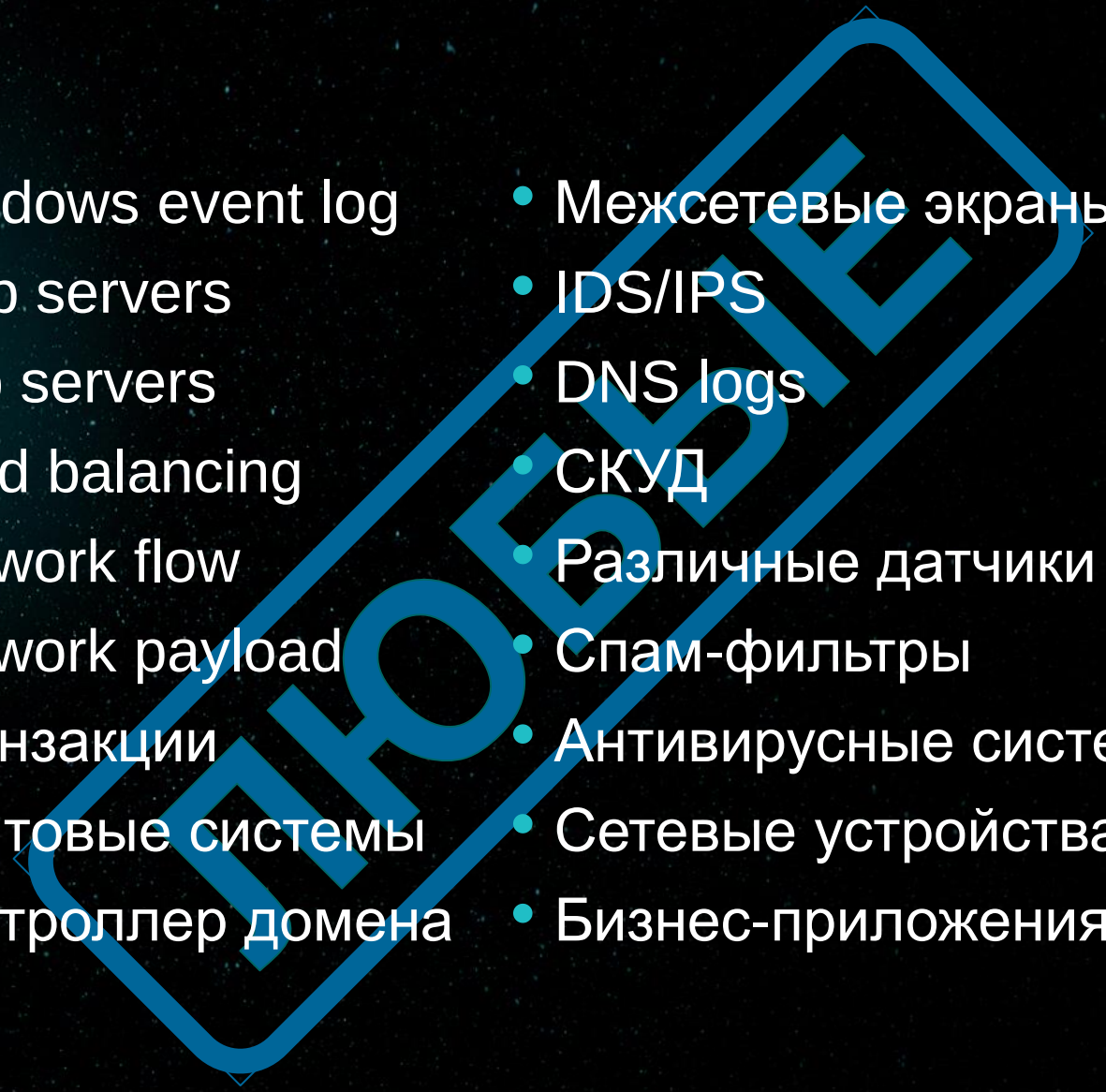


Модуль RuSIEM IoC

- Автоматическая настройка
- Анализ данных из более чем **260** открытых источников
- Сбор индикаторов из социальных сетей (Telegram, Twitter), репозиториев Github, публичных TI-отчетов
- **Более 250 тысяч** уникальных индикаторов в сутки, **30 тысяч** из которых имеют **наивысший уровень опасности**
- Интеллектуальная нормализация, очистка, обогащение индикаторов
- Определение степени опасности каждого индикатора на базе уникальной математической модели ранжирования

ИСТОЧНИКИ СОБЫТИЙ ДЛЯ SIEM

- Windows event log
- Web servers
- App servers
- Load balancing
- Network flow
- Network payload
- Транзакции
- Почтовые системы
- Контроллер домена
- Межсетевые экраны
- IDS/IPS
- DNS logs
- СКУД
- Различные датчики
- Спам-фильтры
- Антивирусные системы
- Сетевые устройства
- Бизнес-приложения



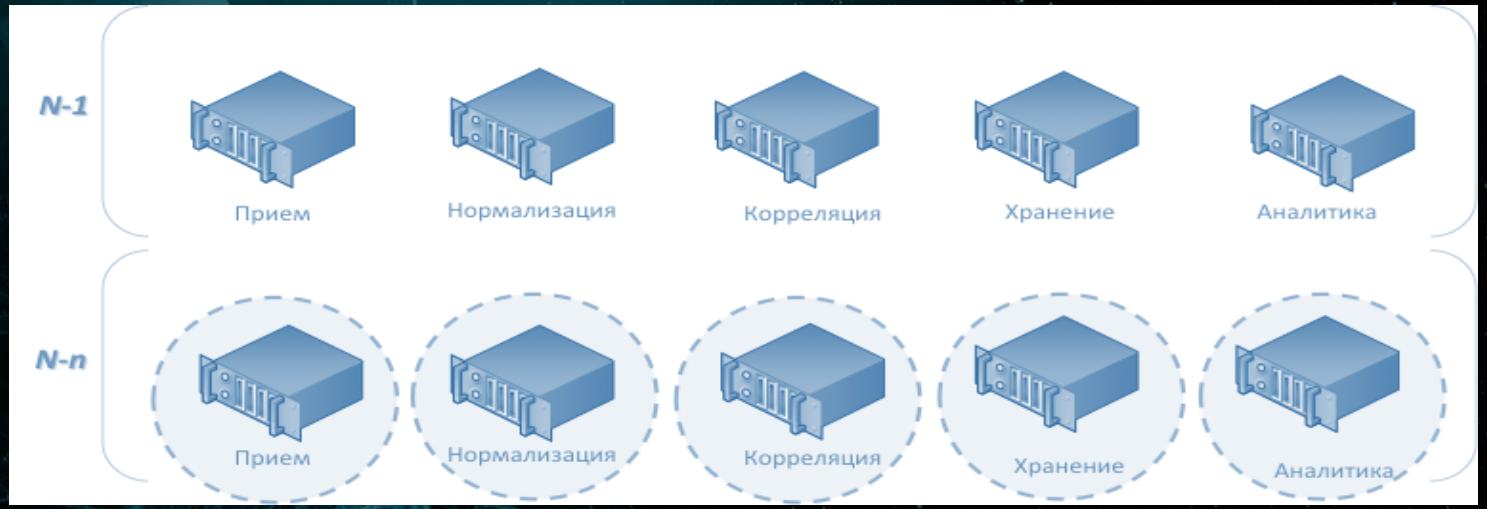
Сценарии применения SIEM

Примеры событий:

- Сетевые атаки
- Фрод и мошенничество
- Откуда и когда блокировались учётные записи
- Изменение конфигураций «не админами»
- Повышение привилегий
- Выявление несанкционированных сервисов
- Обнаружение НСД (вход под учётной 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 (сетевых устройств, приложений, ОС)
- 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 распределённых по времени атаках
- Влияние отказа в инфраструктуре на бизнес-процессы

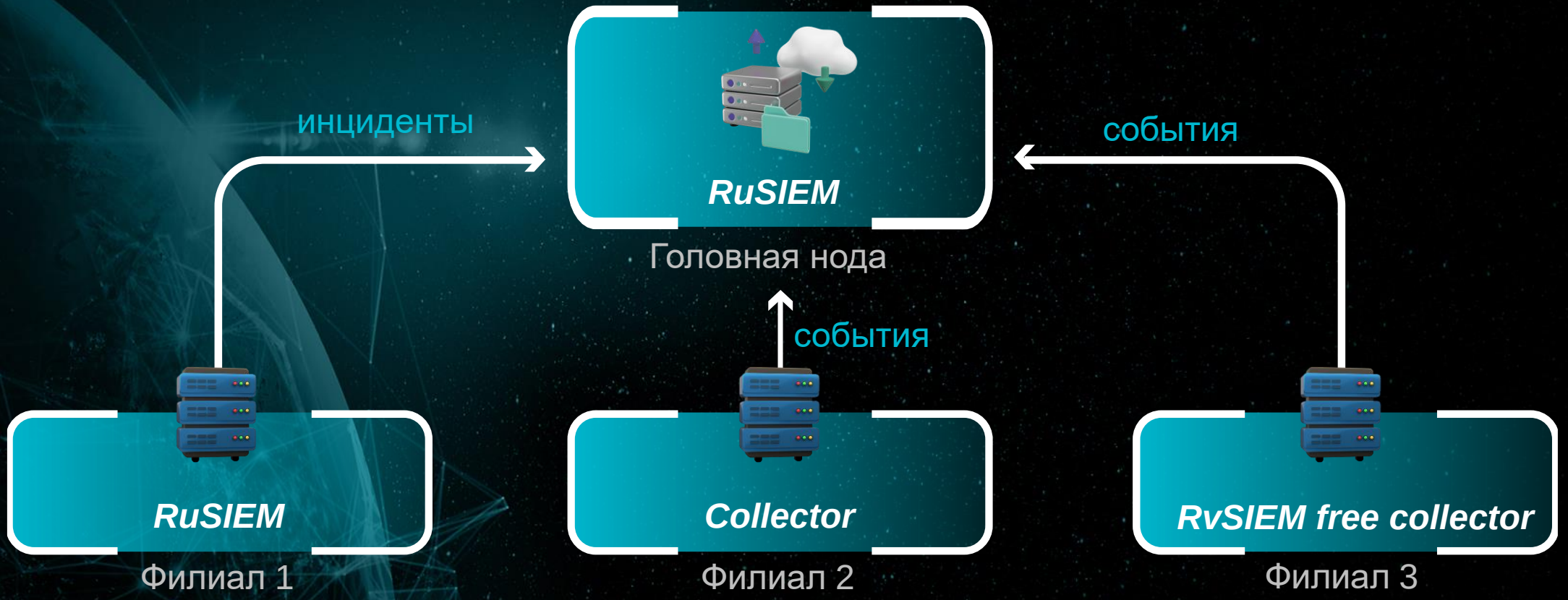
Гибкость масштабирования

- Вертикальное расширение (подключение филиалов)
- Горизонтальное расширение (производительность)



- Горячее расширение без остановки сбора событий

Варианты развертывания системы



RUSIEM
Всё под контролем

Обновление 3.11

RuSIEM Q4 2023

RUSIEM
Всё под контролем

1

Оптимизация производительности RuAgent

- повышена стабильность работы при высоких нагрузках, в т.ч. у модуля PostgreSQL
- оптимизирован модуль FTP Log
- доработан модуль АПКШ Континент

2

Отчёты

- доработаны отчёты по задачам инцидентов
- доработаны отчёты по инцидентам

3

Доработана авторизация по LDAP

4

Микросервисы

- оптимизирован коррелятор
- повышена стабильность нормализатора
- добавлена возможность удаления конфигураций

5

Парсеры

- улучшены более 40 существующих парсеров
- разработаны новые парсеры:
  - SolidSoft
  - Bolid Orion
  - Exim
  - Courier-mta
  - CyberProtego
  - Echelon (Scaner-VS)
  - Tripwire (enterprise)
  - DejaVU (engine)
  - Isimplelab
  - Qnap (nas)
  - F5 (ASM)
  - NSD (Transit 2.0)
  - Proxmox (PVE)

Лицензирование

- Лицензирование по интенсивности потока событий (EPS – events per second);
- Особенности филиальной структуры организации;
- Срочные и бессрочные лицензии;
- Модульные спецификации;
- Разработка нетиповых парсеров;
- Разработка правил корреляции.

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

Выгоды внедрения SIEM

Экономические

- **Предотвращение** на ранней стадии угроз и рисков ИБ
- **Оптимизация** ресурсов отдела информационной безопасности
- **Снижение** влияние человеческого фактора при предотвращении инцидентов

Качественные

- **Соответствие** требованиям регуляторов
- Проведение **расследований** инцидентов «по горячим следам»
- Создание **единого окна** управления информационной безопасностью

Отзывы

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 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 полнофункциональной 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 | СТРАХОВАНИЕ

Исх. № 6/н от 14.12.2021г

В ООО «РуСИЕМ»

Благодарственное письмо

ООО СК "УРАЛСИБ СТРАХОВАНИЕ" (ОГРН 1027739608005, ИНН 7606031534, 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 ускоряющий 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 — В.А. Бунто

Негосударственный пенсионный фонд
Профессиональный

Адрес: 101000, г. Москва, ул. Чаплыгина, д. 17, стр. 5
Тел.: +7 (495) 003-26-75

ОГРН 1147799018525
ИНН/КПП 7701069067/770101001
р/с 40701810895000001900
банк ПАО «...», г. Москва
к/с 30101810200000000825
БИК 044-525825

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**

БИЗКОММ

ООО «БизКомм»
Юридический адрес: Хлебозаводский проезд, д. 7, стр. 9, эт. 3, пом. X, ком. 23, оф. 14, Москва, Россия, 115230
Почтовый адрес: а/я 85, Москва, Россия, 119334
ОГРН 1137746926493 // ИНН 7714856180 // КПП 773401001
Телефон: +7 (495) 300-10-05
www.bizkomm.ru

ООО «РуСИЕМ»
Генеральному директору
Р.А. Воронину

28.04.2022 № ИСХ-БК-220418/-3
На № от

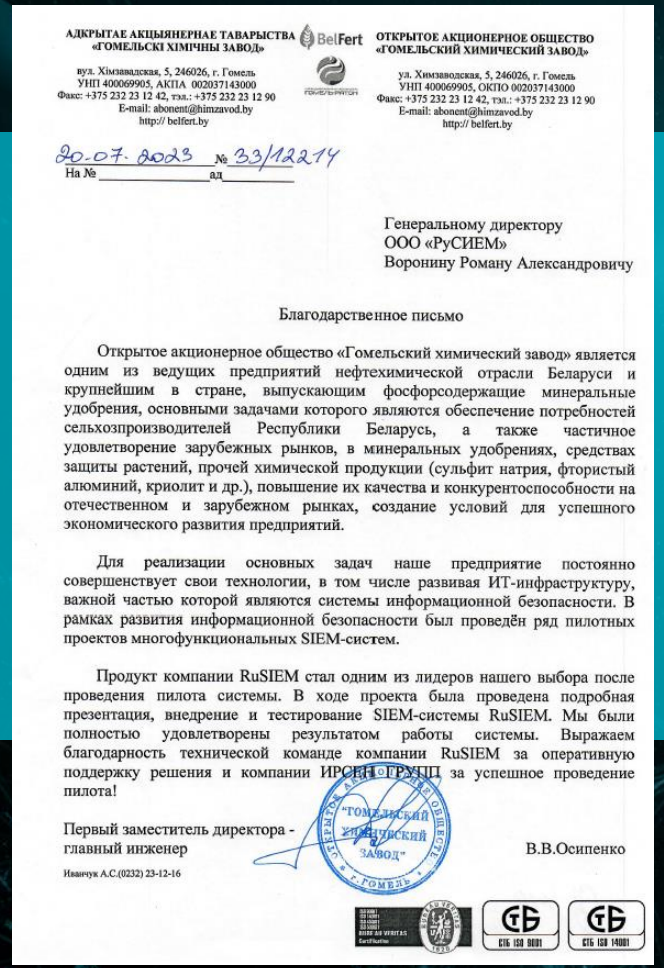
О направлении благодарственного письма

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**

Отзывы белорусских заказчиков



АДКРЫТАЕ АКЦЫЯНЕРНАЕ ТАВАРЫСТВА
«ГОМЕЛЬСКІ ХІМІЧНЫ ЗАВОД»

вул. Хімзаводская, 5, 246026, г. Гомель
УНП 400069905, АКПА 00203714300
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 00203714300
Факс: +375 232 23 12 42, тэл.: +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 ИРСИН ГРУПП за успешное проведение пилота!

Первый заместитель директора - главный инженер В.В.Осипенко

Иванчук А.С.(0232) 23-12-16

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

31.08.2015 № 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

Telegram-каналы RuSIEM

t.me/rusiem
последние новости,
важные события

t.me/rusiemsupport
возможность быстро связаться
с технической поддержкой

Поддержка

Поддерживаем заказчиков и партнёров на всех этапах проекта

RUSIEM
Всё под контролем

Спасибо за внимание!

Появились вопросы?
ОБРАЩАЙТЕСЬ!

Альбина Бухарова
Менеджер по работе с ключевыми заказчиками

a.bukharova@rusiem.com
www.rusiem.com
+7(495)748-83-11
+7(968)478-94-35