RUSIEM
Всё под контролем

RuSIEM

решение для оперативного обнаружения угроз и аномалий

Ксения Быкова

Менеджер по работе с ключевыми заказчиками

+7 965 010 50 80 K.Bykova@rusiem.com

+7 (495) 748-83-11

info@rusiem.com

rusiem.com

- О компании RuSIEM
- Принцип работы SIEM-системы RuSIEM
- 7 ошибок внедрения SIEM-систем

RuSIEM сейчас

ТОП
3
отечественных
SIEM-решений

полностью
российская
разработка

x 3
рост компании за
последние 3 года

> 570
партнеров в России,
странах СНГ, Азии и
Латинской Америке

10 лет
продукту
в 2024 году

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

NEW
мажорный релиз 4.0.0
с новым интерфейсом

Что такое SIEM

RUSIEM
Всё под контролем

Какие задачи решает SIEM

- Оперативное обнаружение инцидентов, контроль обработки инцидентов, сбор доказательной базы для дальнейшего расследования
- Уменьшение лага между выявленным инцидентом и реакцией
- Повышение стоимости проникновения в ИТ инфраструктуру предприятия
- Определение прав, обязанностей и разграничение зон ответственности персонала компании (ИТ- и ИБ-служб)
- Соответствие требованиям регуляторов

(ФЗ №№ 152, 161, 187, приказы ФСТЭК России №№ 21, 17, 31, ГОСТ 57580, PCI DSS, ISO 27001, подключение к ФинЦЕРТ или ГосСОПКА (опционально))

Принцип работы SIEM

Сбор событий

- Из различных источников инфраструктуры компании

Нормализация событий

- Разбивка по полям в соответствии с таксономией системы

Корреляция событий

- Анализ всех поступающих в систему событий

Выявление инцидентов

- А также уязвимостей и поведенческих аномалий

Уведомление об инцидентах

- И постановка задачи на разбор инцидента соответствующему сотруднику

7 ашипок внидрения SIEM-сыстем

RUSIEM
Всё под контролем

Ошибка № 1

Купить SIEM-систему только потому, что есть требования регулятора

RUSIEM
Всё под контролем

Соответствие требованиям

ФЗ РФ
от 27 июля 2006 г.
№ 152-ФЗ
«О персональных данных»

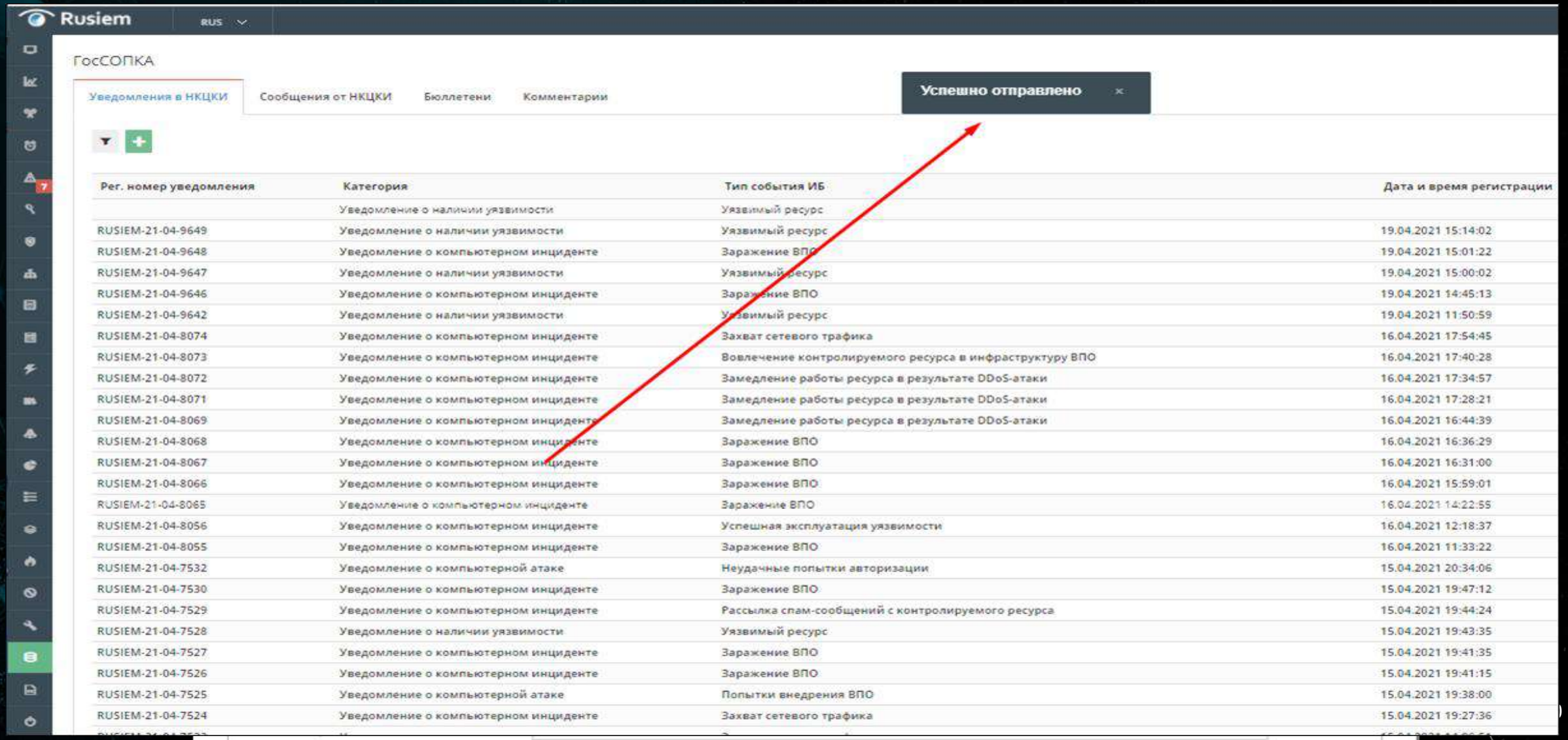
ГОСТ Р 57580.1-2017
«Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»

ФЗ РФ
от 26 июля 2017 г.
№ 187-ФЗ
«О безопасности критической информационной инфраструктуры РФ»

ISO/IEC 27001
«Системы менеджмента информационной безопасности. Требования»

ГОСТ Р 57580.2-2018
«Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия»

Интеграция с ГосСОПКА – уведомления в НКЦКИ



Рег. номер уведомления	Категория	Тип события ИБ	Дата и время регистрации
	Уведомление о наличии уязвимости	Уязвимый ресурс	
RUSIEM-21-04-9649	Уведомление о наличии уязвимости	Уязвимый ресурс	19.04.2021 15:14:02
RUSIEM-21-04-9648	Уведомление о компьютерном инциденте	Заражение ВПО	19.04.2021 15:01:22
RUSIEM-21-04-9647	Уведомление о наличии уязвимости	Уязвимый ресурс	19.04.2021 15:00:02
RUSIEM-21-04-9646	Уведомление о компьютерном инциденте	Заражение ВПО	19.04.2021 14:45:13
RUSIEM-21-04-9642	Уведомление о наличии уязвимости	Уязвимый ресурс	19.04.2021 11:50:59
RUSIEM-21-04-8074	Уведомление о компьютерном инциденте	Захват сетевого трафика	16.04.2021 17:54:45
RUSIEM-21-04-8073	Уведомление о компьютерном инциденте	Вовлечение контролируемого ресурса в инфраструктуру ВПО	16.04.2021 17:40:28
RUSIEM-21-04-8072	Уведомление о компьютерном инциденте	Замедление работы ресурса в результате DDoS-атаки	16.04.2021 17:34:57
RUSIEM-21-04-8071	Уведомление о компьютерном инциденте	Замедление работы ресурса в результате DDoS-атаки	16.04.2021 17:28:21
RUSIEM-21-04-8069	Уведомление о компьютерном инциденте	Замедление работы ресурса в результате DDoS-атаки	16.04.2021 16:44:39
RUSIEM-21-04-8068	Уведомление о компьютерном инциденте	Заражение ВПО	16.04.2021 16:36:29
RUSIEM-21-04-8067	Уведомление о компьютерном инциденте	Заражение ВПО	16.04.2021 16:31:00
RUSIEM-21-04-8066	Уведомление о компьютерном инциденте	Заражение ВПО	16.04.2021 15:59:01
RUSIEM-21-04-8065	Уведомление о компьютерном инциденте	Заражение ВПО	16.04.2021 14:22:55
RUSIEM-21-04-8056	Уведомление о компьютерном инциденте	Успешная эксплуатация уязвимости	16.04.2021 12:18:37
RUSIEM-21-04-8055	Уведомление о компьютерном инциденте	Заражение ВПО	16.04.2021 11:33:22
RUSIEM-21-04-7532	Уведомление о компьютерной атаке	Неудачные попытки авторизации	15.04.2021 20:34:06
RUSIEM-21-04-7530	Уведомление о компьютерном инциденте	Заражение ВПО	15.04.2021 19:47:12
RUSIEM-21-04-7529	Уведомление о компьютерном инциденте	Рассылка спам-сообщений с контролируемого ресурса	15.04.2021 19:44:24
RUSIEM-21-04-7528	Уведомление о наличии уязвимости	Уязвимый ресурс	15.04.2021 19:43:35
RUSIEM-21-04-7527	Уведомление о компьютерном инциденте	Заражение ВПО	15.04.2021 19:41:35
RUSIEM-21-04-7526	Уведомление о компьютерном инциденте	Заражение ВПО	15.04.2021 19:41:15
RUSIEM-21-04-7525	Уведомление о компьютерной атаке	Попытки внедрения ВПО	15.04.2021 19:38:00
RUSIEM-21-04-7524	Уведомление о компьютерном инциденте	Захват сетевого трафика	15.04.2021 19:27:36

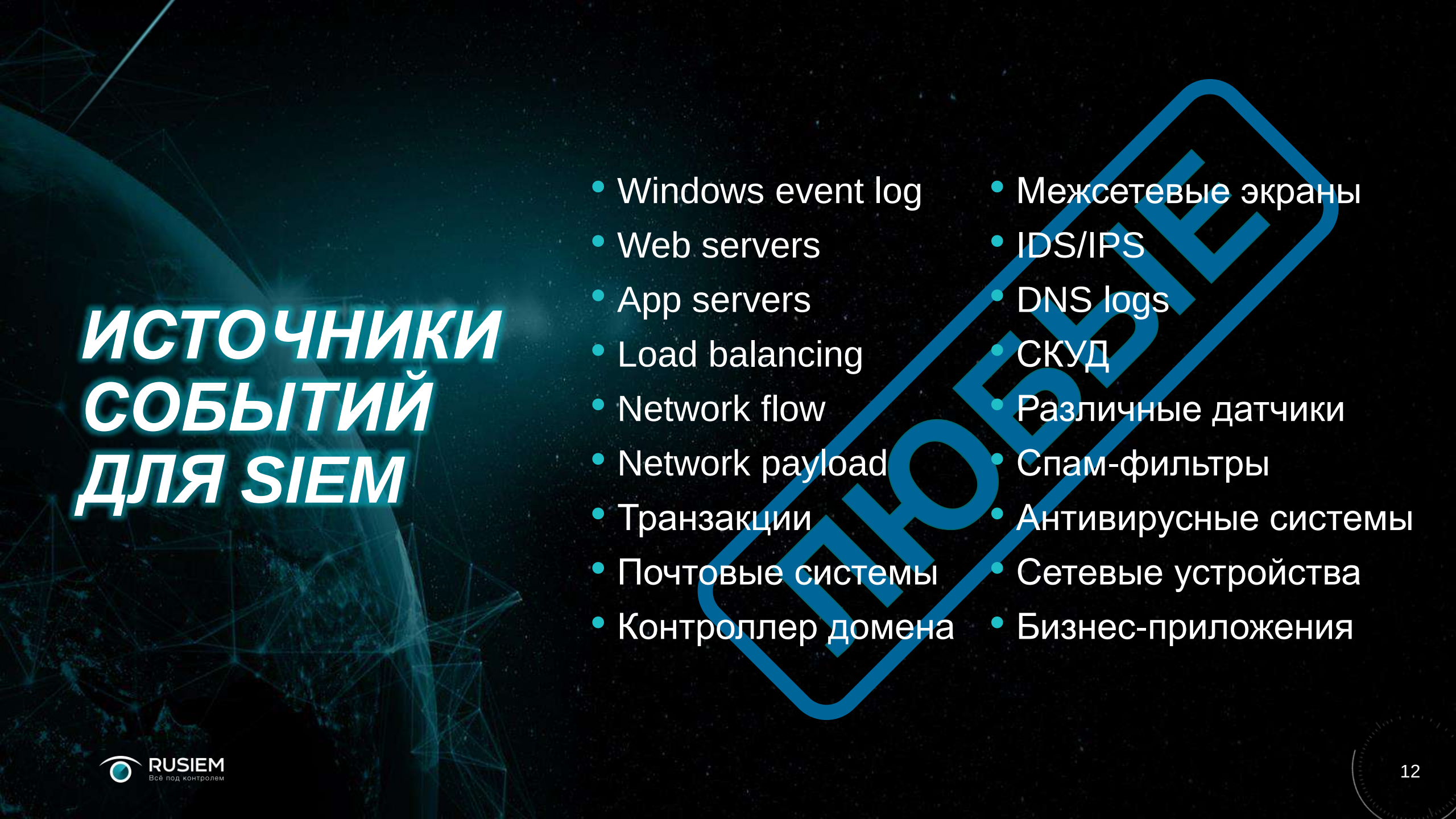
Ошибка № 2

Ограничиться малым функционалом или покупать излишний функционал

RUSIEM
Всё под контролем

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



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

RUSIEM
Всё под контролем

Ошибка № 3

Руководство компании НЕ понимает, что такое SIEM

RUSIEM
Всё под контролем

Выгоды внедрения RuSIEM

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

Ошибка № 4

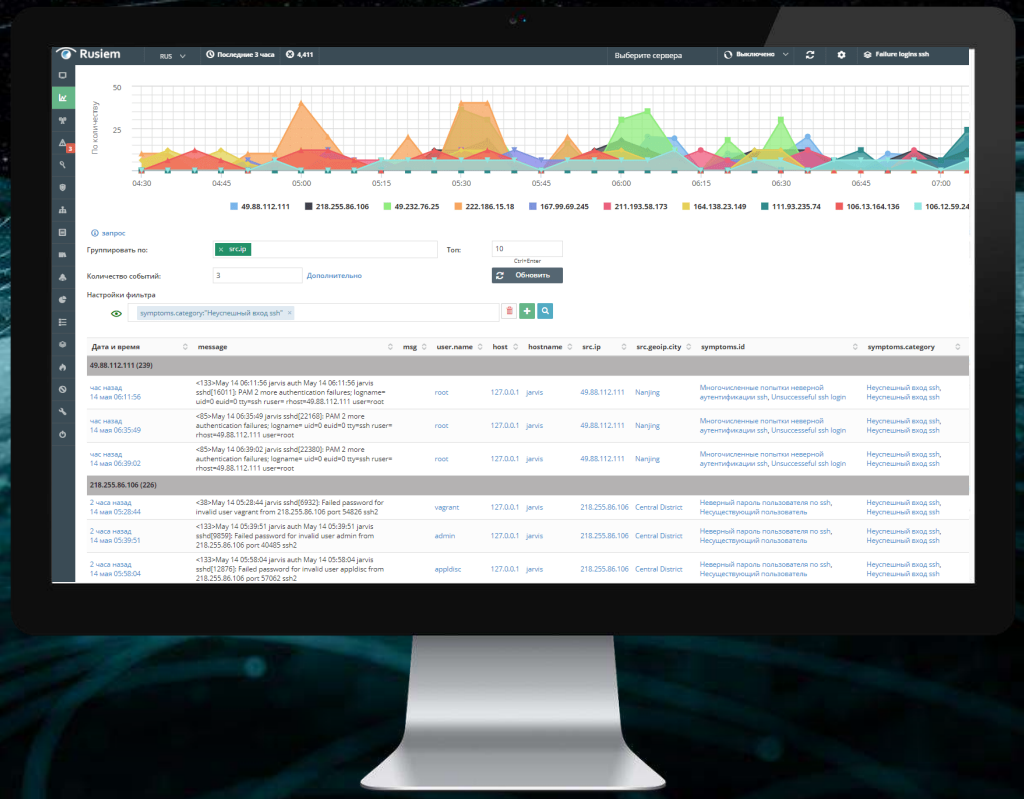
Пусть работу с SIEM совместит системный администратор

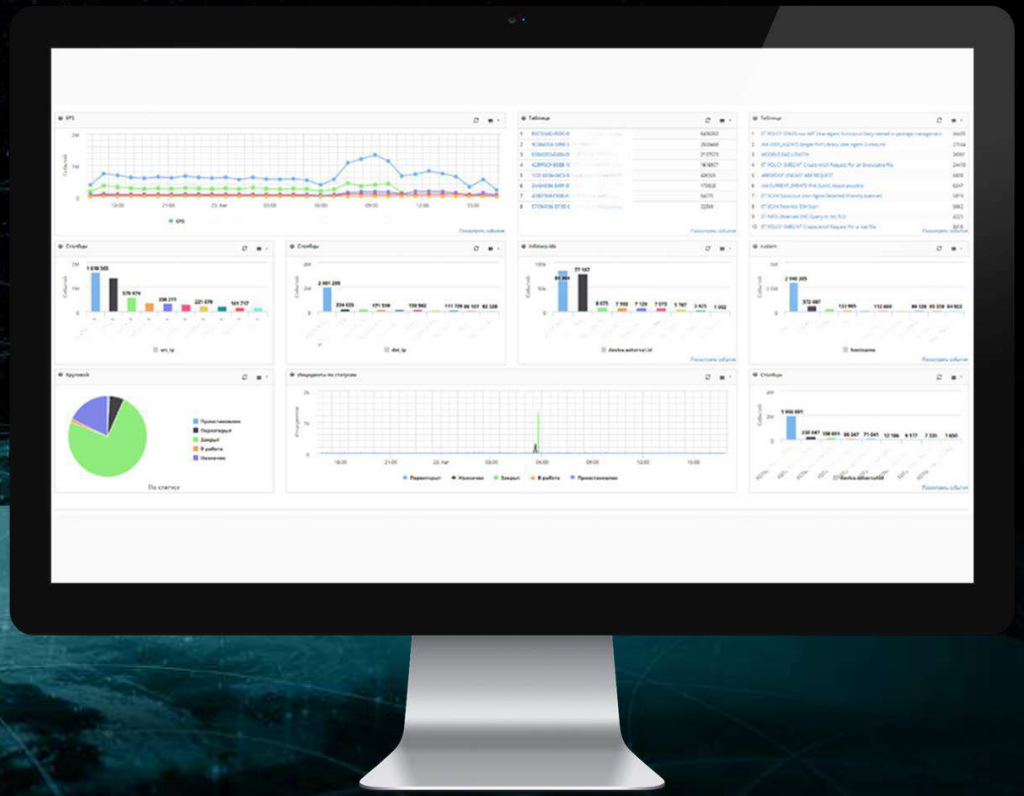
RUSIEM
Всё под контролем

Ошибка № 5

Я не знаю, что я хочу, но мне нужен красивый отчет для Руководства

RUSIEM
Всё под контролем





RUSIEM
Всё под контролем

Ошибка № 6

Работа с правилами (корреляции, нормализации и парсерами) – это сугубо прерогатива вендора и интегратора

RUSIEM
Всё под контролем

Ошибка № 7

Использовать SIEM только как инструмент ИБ

RUSIEM
Всё под контролем

Сценарии применения SIEM

Примеры событий:

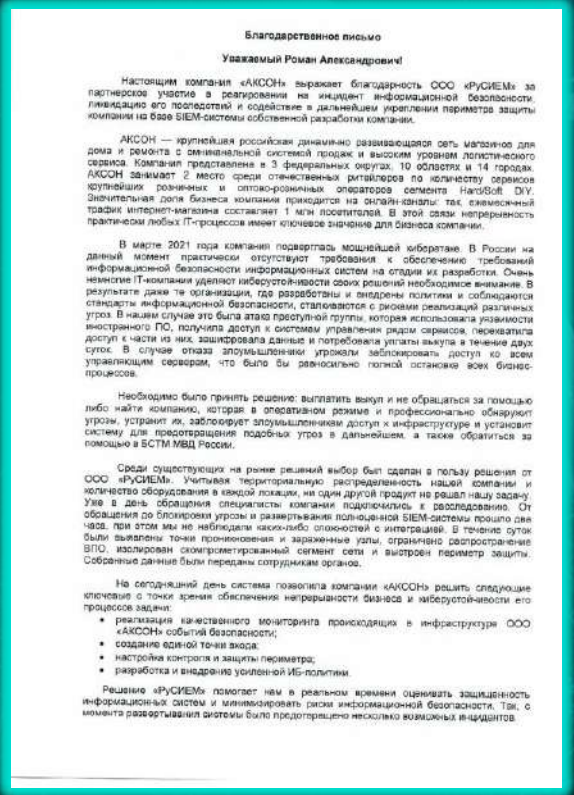
- Сетевые атаки
- Блокирование учётных записей с информацией откуда и когда
- Изменение конфигураций не админами
- Повышение привилегий
- Выявление несанкционированных сервисов
- Обнаружение НСД (вход под учётной записью уволенного сотрудника)
- Отсутствие антивирусной защиты на новом установленном компьютере
- 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

Преимущества решения RuSIEM

- Не теряем события
- No-code
- Полностью подходит под критерии импортозамещения
- Максимальный предустановленный функционал
- Гибкость масштабирования
- Подключение любых источников данных
- Взаимодействие с ФинЦЕРТ
- Интеграция с ГосСОПКА «из коробки»
- Система быстро разворачивается, проста в освоении
- Разработка и поддержка от вендора
- Централизованное управление
- 570 правил корреляции для анализа событий

Референсы

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 1027739606605, 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 заказчиков 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 обеспечивающий 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 ранее 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

ПРОФЕССИОНАЛЬНЫЙ
негосударственный пенсионный фонд

Негосударственный пенсионный фонд Профессиональный

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 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

бизкомм

БИЗКОМм

ООО «РуСИЕМ»
Генеральному директору
Р.А. Воронину

18.04.2022 № ИСХ-БК-2204187-3
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

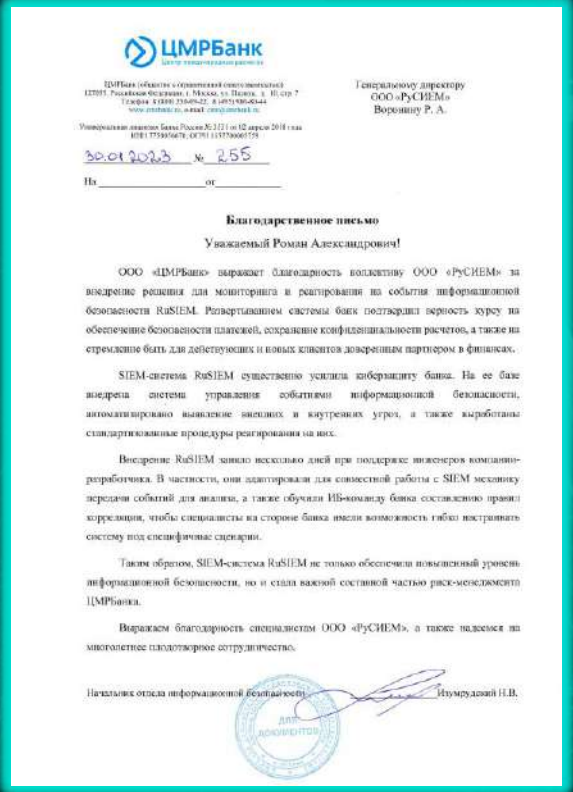
Референсы

ЦМРБанк
Центр международных расчетов

ДЕРЖАВА
БАНК

Петербургский
Городской Банк

Коммерческий
Индо Банк



ЦМРБанк
Центр международных расчетов

Генеральному директору
ООО «РуСИЕМ»
Воронину Р. А.

30.01.2023 № 255

Благодарственное письмо

Уважаемый Роман Александрович!

ООО «ЦМРБанк» выражает благодарность коллективу ООО «РуСИЕМ» за внедрение решения для мониторинга и реагирования на события информационной безопасности RuSIEM. Развертывание системы банк подтвердил верность курсу на обеспечение безопасности платежей, сохранение конфиденциальности расчетов, а также на стремление быть для действующих и новых клиентов доверенным партнером в финансах.

SIEM-система RuSIEM существенно усилила кибербезопасность банка. На ее базе внедрена система управления событиями информационной безопасности, автоматизировано выявление внешних и внутренних угроз, а также выработаны стандартизированные процедуры реагирования на них.

Внедрение RuSIEM заняло несколько дней при поддержке инженеров компании-разработчика. В частности, они адаптировали для совместной работы с SIEM механику передачи событий для анализа, а также обучили ИБ-команду банка составлению правил корреляции, чтобы специалисты на стороне банка имели возможность гибко настраивать систему под специфичные сценарии.

Таким образом, SIEM-система RuSIEM не только обеспечила повышенный уровень информационной безопасности, но и стала важной составной частью риск-менеджмента ЦМРБанка.

Выражаем благодарность специалистам ООО «РуСИЕМ», а также надеемся на многолетнее плодотворное сотрудничество.

Начальник отдела информационной безопасности Изумрудский Н.В.

ДЕРЖАВА
БАНК

Исх. № 1480
От «14» июня 2023 г.

Генеральному директору ООО «РуСИЕМ»
Воронину Роману Александровичу

121205, г. Москва, тер. Сколково инновационного центра, Большой бр, д. 42, стр. 1, ЭТАЖ 4 ЧАСТЬ ПОМ 3483.

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. Скорадумов

Исп.: Волков С.А.
Тел.: +7 (495) 398-04-80 доб. 565

Петербургский
Городской Банк

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 трансакций 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.

Благодарю 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
Commercial Indo Bank LLC

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 главных 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»

RUSIEM
Всё под контролем

Референсы

BelFert
ОАО «Гомельский химический завод»

Алкогольная Сибирская группа

ИНСТИТУТ АЭРОНАВИГАЦИИ

АКЦЫЯНЕРНАЯ ТАВАРЫСТВА «ГОМЕЛЬСКІ ХІМІЧНЫ ЗАВОД»

ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО «ГОМЕЛЬСКИЙ ХИМИЧЕСКИЙ ЗАВОД»

30.07.2023 № 33/12214

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 ИРОНИ ГРУПП за успешное проведение пилота!

Первый заместитель директора - главный инженер В.В.Осипенко

Генеральному директору ООО «РуСИЕМ»
Воронину Роману Александровичу

Благодарственное письмо

«Алкогольная Сибирская Группа» (АСГ) является одним из крупнейших производителей алкоголя. По итогам 2021 года объем производства продукции под брендами компании составил 8,3 млн. дал.

Сложность производственных процессов, их бесперебойность, автоматизация и цифровизация производства предполагают постоянный контроль и усиление информационной безопасности, чтобы не допустить сбоев на всех этапах.

Для решения этой задачи АСГ выбрала продукт компании RuSIEM. SIEM-система российского производства RuSIEM полностью соответствует требованиям АСГ по контролю и аналитике сетевой активности (благодаря дополнительному модулю RuSIEM Analytics), обнаружению и реагированию на инциденты.

Благодарим ООО «РуСИЕМ» за профессиональную работу, качественную поддержку при установке системы и своевременную обратную связь в по сей день. Можем рекомендовать данное решение для организаций с повышенными требованиями по сохранности данных и безопасности производственных процессов.

Ивлиев Виталий Александрович
Ведущий специалист по информационной безопасности
ООО «Алкогольная Сибирская Группа»

МІНІСТЭРСТВА ПА НАДЗВЫЧАЙНЫХ СІТУАЦЫЯХ РЭСПУБЛІКІ БЕЛАРУСЬ
ДЭПАРТАМЕНТ ПА МАТЭРЫЯЛЬНЫХ РЭЗЕРВАХ (ДЗЯРЖРЭЗЕРВ)

МИНИСТЕРСТВО ПО ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ РЕСПУБЛИКИ БЕЛАРУСЬ
ДЕПАРТАМЕНТ ПО МАТЕРИАЛЬНЫМ РЕЗЕРВАМ (ГОСРЕЗЕРВ)

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

ФГУП «Госкорпорация по ОрВД»
Некоммерческое образовательное учреждение дополнительного профессионального образования
«ИНСТИТУТ АЭРОНАВИГАЦИИ»

FSUE «State ATM Corporation»
Non-Commercial Education Institution for supplementary professional training
«INSTITUTE OF AIR NAVIGATION»

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 и 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

RUSIEM
Всё под контролем

Telegram-каналы RuSIEM

*https://t.me/**rusiem***

последние новости, важные события

*https://t.me/**rusiemsupport***

возможность быстро связаться с технической поддержкой

RUSIEM
Всё под контролем

Запросите бесплатную версию RuSIEM

Быкова Ксения
Менеджер по работе с ключевыми заказчиками

k.bykova@rusiem.com

www.rusiem.com

+7(495) 748-83-11

+7(965) 010-50-80