RUSIEM
Всё под контролем

Единая система мониторинга информационной безопасности организации

Даниил Вылегжанин,
менеджер по техническому сопровождению продаж

RuSIEM – это

Полностью российская разработка

> 1000

Пилотных внедрений

Sk Сколково

Резидент Сколково

> 150

Партнеров в РФ и странах СНГ

2014

С этого года ведется активная разработка

Продукт включен в Единый реестр отечественного ПО

Продукт имеет сертификат ФСТЭК России (4 УД), сертифицирован для использования на территории Беларуси

> 10000

Установок free-версии в мире

RUSIEM
Всё под контролем

Больше активных партнеров

Значительный рост количества компетентных и активных партнеров

rusiem.com/ru/partners

Было в 2020	Стало в 2021
25 активных партнёров 5 продающих партнёров	114 активных партнёра 24 продающих партнёра

RUSIEM
Всё под контролем

Что такое SIEM

- **SIEM** (Security Information and Event Management) — решение для мониторинга и анализа любой активности, происходящей в организации
- **SIEM** — это сложная комплексная система, позволяющая получать своевременную и всеобъемлющую информацию о состоянии ИТ-инфраструктуры предприятия

SEM
(Security Event Management) — управление событиями безопасности

Процесс централизации данных журнала компьютера из нескольких источников для улучшения обнаружения инцидентов безопасности и управления этими событиями посредством формализованного процесса реагирования

+

SIM
(Security Information Management) — управление информационной безопасностью

Процесс сбора, мониторинга и анализа данных из автоматически генерируемых компьютерных журналов

=

SIEM

SIEM – система мониторинга, которая позволит вам отслеживать состояние собственной инфраструктуры в реальном времени. Система анализа событий безопасности, исходящих от сетевых устройств и приложений, которая позволяет своевременно реагировать на инциденты безопасности

Схема работы SIEM

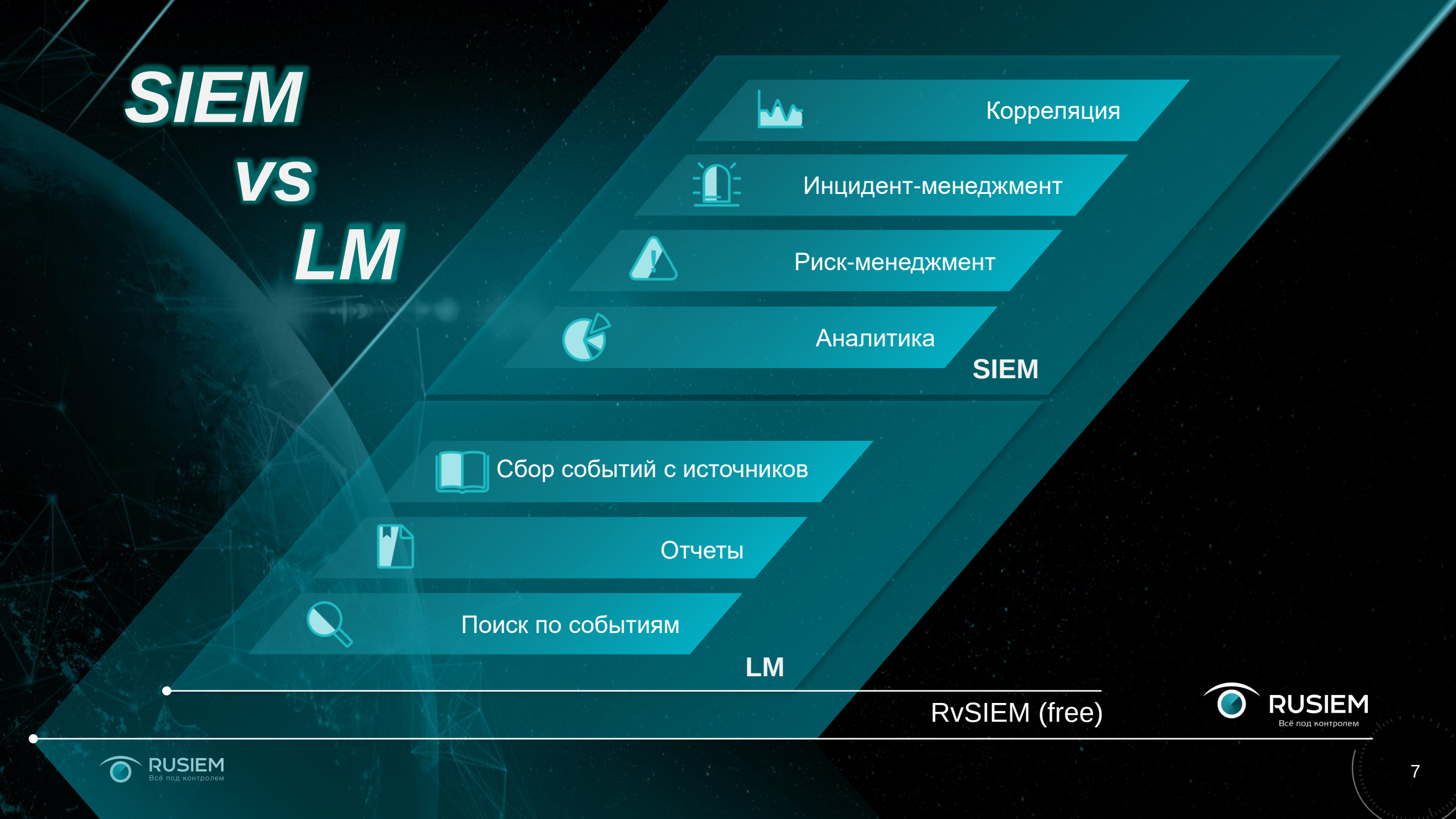
Внедрение SIEM

- Access Control, Authentication
- DLP-системы
- IDS/IPS-системы
- Антивирусные приложения

- Журналы событий серверов и рабочих станций
- Межсетевые экраны
- Сетевое активное оборудование
- Сканеры уязвимостей

- Система инвентаризации и asset-management (а у некоторых СИЕМ есть даже свой внутренний функционал работы с активами)
- Система веб-фильтрации

SIEM vs LM



RUSIEM
Всё под контролем

RUSIEM
Всё под контролем

RuSIEM – это

Более 350 источников событий «из коробки»

Более **400** правил корреляции **для анализа событий**

75 Предустановленных шаблонов **отчетов**

Собственная технология анализа событий, основанная на лучших практиках и собранном опыте

RUSIEM
Всё под контролем

Антивирус | **Межсетевой экран** | **IPS и IDS** | **Почтовые системы** | **Прочее ПО**

RuSIEM – стандарты

- **ФСТЭК России**
  - на систему получен сертификат ФСТЭК России по 4 УД

- **Интеграция с ФинЦЕРТ**
  - получение актуальных индикаторов компрометаций для участников обмена с ЦБ и кредитно-финансовой сферой

- **Модуль НКЦКИ**
  - полноценная интеграция с ГосСОПКА в части отправки инцидентов и обмена информацией

Решение

Линейка продуктов

RvSIEM (free)
– классическое решение класса LM

RuSIEM
– коммерческая версия класса SIEM

RuSIEM Analytics
– модуль анализа событий, учета активов, дополненный DL

Сравнение функционала линейки RuSIEM

	RuSIEM	RuSIEM Analytics	RvSIEM (free)
Дашборды (набор виджетов для оценки показателей в режиме реального времени)	✓	✓	✓
Поиск по событиям	✓	✓	✓
Сохраненные запросы	✓	✓	✓
RBR (rule-based) корреляция	✓	✓	
Инцидент-менеджмент по ITIL	✓	✓	
Симптоматика для тегирования событий понятным описанием	✓	✓	✓
Риск-метрики	✓	✓	
Отчеты	✓	✓	✓
Отчеты соответствия стандартам и политикам	✓	✓	
Аналитика (агрегация событий) для обнаружения инцидентов без корреляции		✓	
Аналитика (baseline) для обнаружения инцидентов без корреляции		✓	
Обновляемые ленты угроз (feeds: потенциально опасные ip, hash, url, fqdn, mail)		✓	
Аналитика (сложные отчеты с расчетами)		✓	
ИТ-активы с обновлением в режиме реального времени		✓	
Агент с универсальными коннекторами к источникам	✓	✓	✓
Масштабируемость	✓	✓	limited
Обновление базы знаний (правила корреляции, отчеты, симптомы)	✓	✓	✓
Поддержка	24x7	24x7	limited
Обновление версий	✓	✓	✓

Масштабируемость

- Вертикальная (филиалы) и горизонтальная (производительность)
- «Горячее» расширение без остановки сбора
- Поддержка слабых каналов между удаленными объектами
- Корреляция в центральном офисе без необходимости передачи всех событий «наверх»
- Распределенный поиск по событиям без необходимости «единого хранилища»
- Построение отказоустойчивой системы

Лицензирование

- *Проектные цены*
- *Модульные спецификации*
- *Бессрочные и срочные лицензии*
- *Разработка сложных парсеров*
- *Разработка правил корреляции*

Кол-во событий в секунду (Event per second)

2000 eps
3000 eps
4000 eps
5000 eps
7500 eps
10000 eps
12500 eps
15000 eps
20000 eps
...

RUSIEM
Всё под контролем

Конкурентные преимущества

- Интеграция с ГосСОПКА и сертификация ФСТЭК России
- Полная поддержка русского языка
- Приведенная к общем формату объектная нормализация
- Встроенная управляемая и редактируемая корреляция
- Высокая производительность (Свыше 90000 событий на одну ноду)
- Нет ограничений по количеству событий и источникам
- Вертикальная масштабируемость
- Горизонтальная масштабируемость
- Разделение нагрузки на несколько серверов или виртуальных машин
- Наличие собственных модульных агентов
- Real-time и историческая корреляция
- Коннекторы от производителя
- Нет ограничений по размеру архивного хранилища
- Сохранение исходных RAW-событий

Задачи

Что умеет RuSIEM

RUSIEM
Всё под контролем

Централизованное управление ИБ

- Централизованное управление позволяет **создавать правила для контроля** систем и пользователей
- Оперативное **выявление и реагирование на инциденты** информационной безопасности

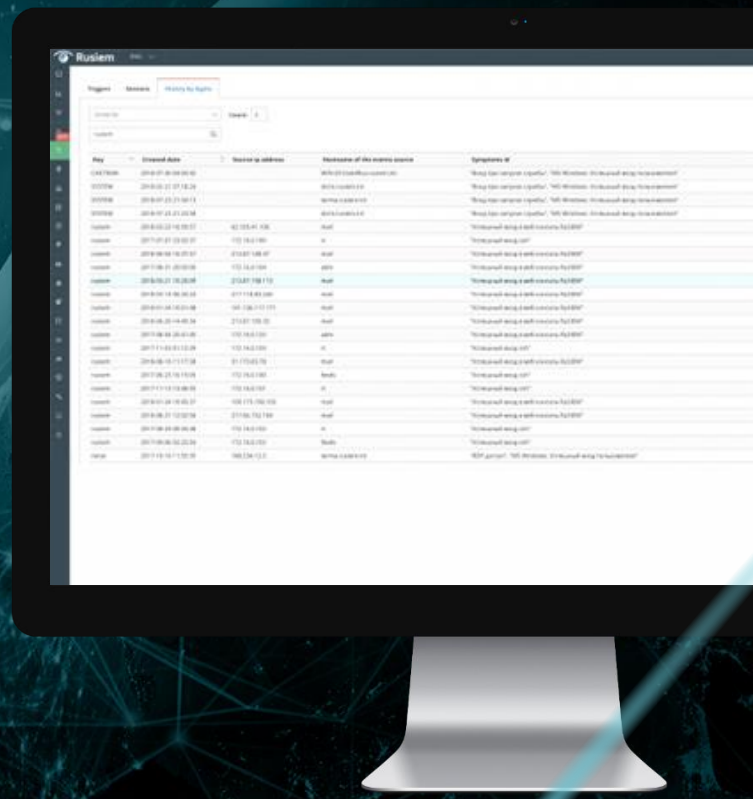
RUSIEM
Всё под контролем

Создание SOC-центра

- **Автоматизация процессов** информационной безопасности
- **Комплексный подход** к управлению информационной безопасностью
- Применение **экспертизы** специалистов **RuSIEM**

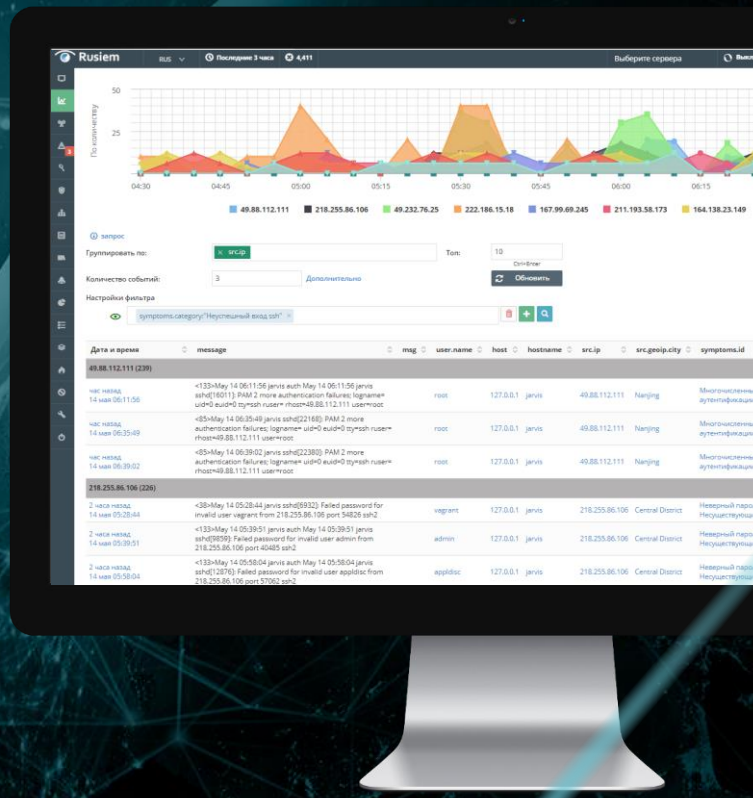
Выявление НСД

- **Отслеживание аутентификации** позволяет создавать правила корреляции для любой системы и контролировать параметры входа пользователей через единую консоль RuSIEM



Машинное обучение

- Технологичность и внедрение алгоритмов машинного обучения в процессе поиска аномалий позволит **выявлять на ранней стадии** и **предотвращать** возможные инциденты ИБ

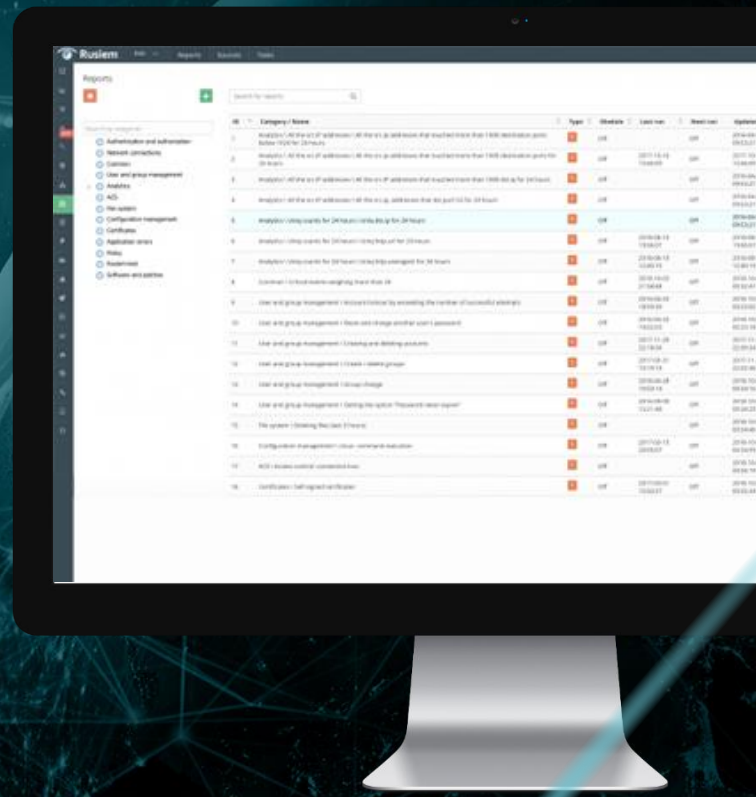


Учет активов

- Выявление **потенциальных рисков** и угроз с целью оценки имеющихся и внедряемых средств безопасности
- Единый реестр актуальных угроз и уязвимостей компании с подробным описанием **мер защиты и способов противодействия**

Выявление мошеннических схем

- Полностью **автоматизированный** процесс **сбора и анализа событий**
- Пользователи могут **создавать как** свои **собственные шаблоны** для выявления аномальных событий, так и использовать лучшие практики компании RuSIEM




Для кого

Государственные учреждения

Возможности RuSIEM

- Снизит санкционные риски за счет внедрения отечественного ПО
- Позволит соответствовать требованиям регуляторов
- Поможет выявить потенциальные утечки персональных данных госслужащих и граждан РФ

Финансовый сектор

Возможности RuSIEM

- Позволит соответствовать требованиям регуляторов, отраслевым и международным стандартам
- Поможет обеспечить доступность ресурсов и непрерывность процессов организации за счет раннего обнаружения внешних атак
- Способствует выявлению фрода и мошеннических схем

Промышленность

Возможности RuSIEM

- Обеспечит интеграцию с ГосСОПКА, позволит соответствовать требованиям законодательства в области КИИ
- Способствует выявлению сложных внешних атак на ранней стадии
- Обеспечит централизованное управление активами как в рамках отдельного предприятия, так и в масштабах холдинга

Выгоды ИБ-службы

SIEM-система RuSIEM **позволяет оперативно реагировать на инциденты** информационной безопасности на ранней стадии, предоставляет возможность сбора доказательной базы для дальнейшего расследования

Выгоды ИТ-службы

SIEM-система RuSIEM позволяет **централизовано управлять и контролировать** ИТ-активы, получать актуальную информацию о хранящихся данных и оценивать возможные риски и уязвимости

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»

Построение Центра Мониторинга Информационной безопасности (SOC)

Примеры проектов

RUSIEM
Всё под контролем

Задачи SOC

Центр мониторинга информационной безопасности (Security Operations Center, SOC) — структурное подразделение организации, отвечающее за оперативный мониторинг IT-среды и предотвращение киберинцидентов. Специалисты SOC собирают и анализируют данные с различных объектов инфраструктуры организации и при обнаружении подозрительной активности принимают меры для предотвращения атаки

- Постоянный поиск, мониторинг и анализ вторжений
- Проактивное предотвращение угроз
- Проверка сетей компании на уязвимость и анализ инцидентов безопасности
- Фильтрация ложных срабатываний и быстрая реакция на подтвержденные инциденты
- Подготовка отчетов об актуальном состоянии ИТ-инфраструктуры, зарегистрированных инцидентах и действиях потенциальных злоумышленников

Примеры проектов

SOC был развернут для ряда крупных заказчиков на SIEM-системе RuSIEM совместно с партнерами:

Многопрофильный системный интегратор ИБ полного цикла, более 15 лет обеспечивает безопасность информационных систем различного уровня сложности. Обеспечивает безопасность государственных информационных систем, объектов критической информационной инфраструктуры, информационных систем персональных данных. Участвует в государственной программе по импортозамещению

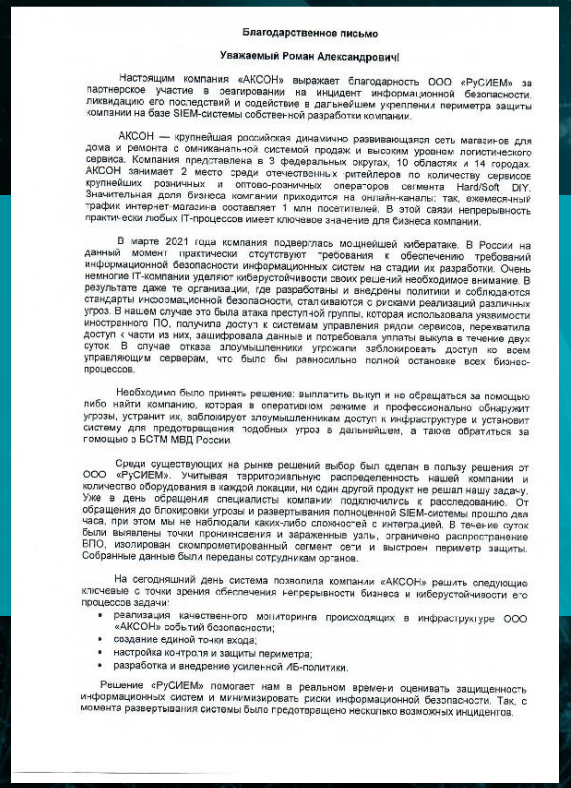
Предоставляет услуги широкополосного доступа в Интернет, телефонии, цифрового ТВ, доступа к сетям Wi-Fi, VPN, LoRaWAN, видеонаблюдения и комплексных решений на базе технологий промышленного Интернета вещей (IoT)

Оказывает полный спектр услуг по защите информации — от проектирования информационных систем в защищенном исполнении, внедрения средств защиты информации ведущих российских и зарубежных производителей до аттестации объектов информатизации и оказания последующего информационно-технического сопровождения, в том числе обработки сведений, составляющих государственную тайну

Референсы

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.

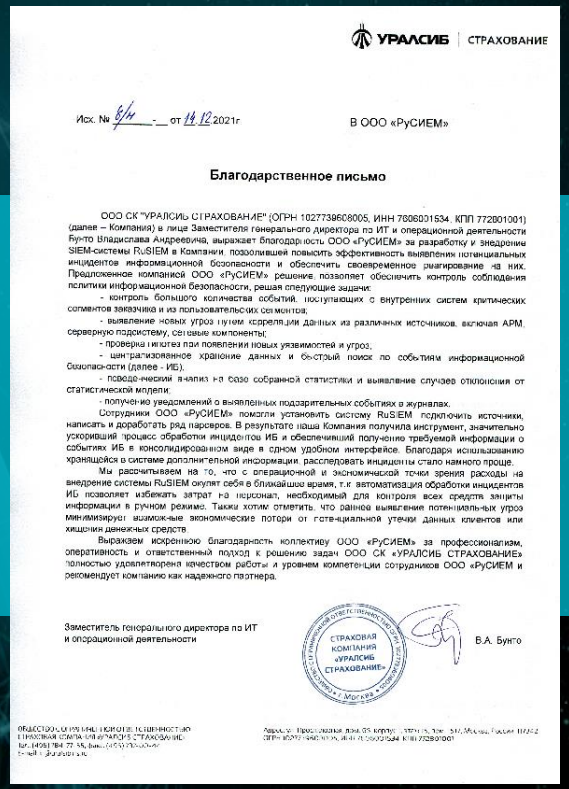
Необходимо было принять решение: выплатить выкуп и не обращаться за помощью либо найти компанию, которая в оперативном режиме и профессионально обнаружит угрозы, устранит их, заблокирует злоумышленникам доступ к инфраструктуре и установит систему для предотвращения подобных угроз в дальнейшем, а также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

СТРАХОВАЯ КОМПАНИЯ «УРАЛСИБ СТРАХОВАНИЕ»

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.

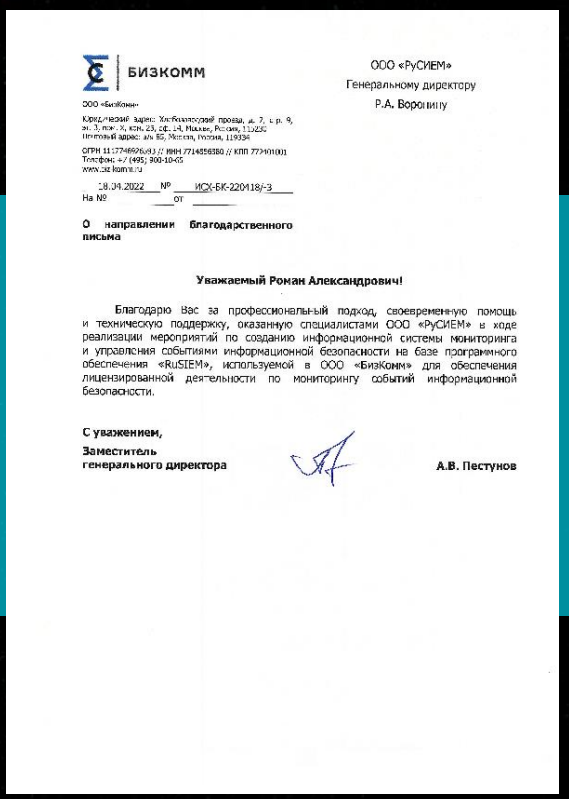
SIEM-система RuSIEM позволила НПФ «Профессиональный» (АО) обеспечить соответствие требованиям Положения Банка России от 20.04.2021 № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых 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 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 «РуСИЕМ»
Генеральному директору
Р.А. Воронину

ООО «БизКомм»
Юридический адрес: Хлебозаводский проезд, д. 7, с.р. 9, эт. 3, пом. X, ком. 23, сф. 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.ce.bizkom.ru

28.04.2022 № ИСХ-БК-220418/-3
На № от

О направлении благодарственного письма

Уважаемый Роман Александрович!

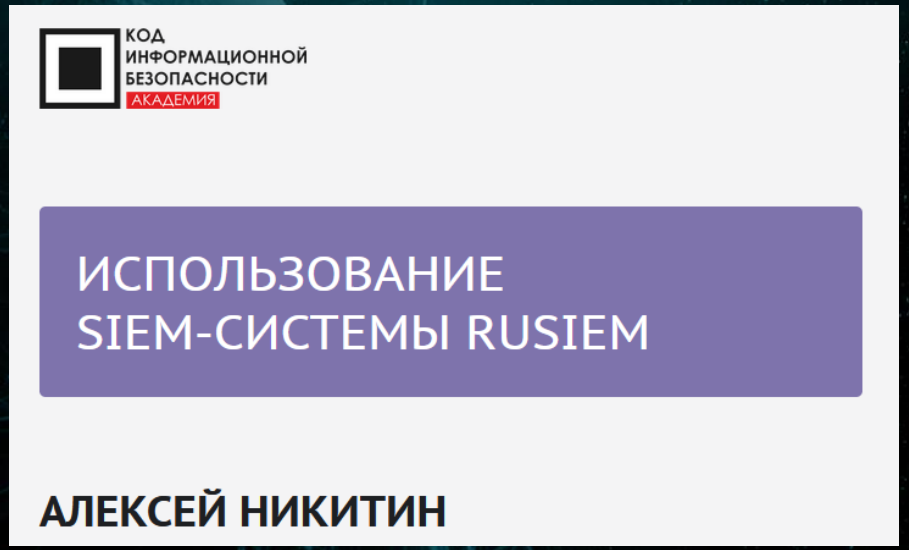
Благодарю Вас за профессиональный подход, своевременную помощь и техническую поддержку, оказанную специалистами ООО «РуСИЕМ» в ходе реализации мероприятий по созданию информационной системы мониторинга и управления событиями информационной безопасности на базе программного обеспечения «RuSIEM», используемой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

С уважением,
Заместитель генерального директора — **А.В. Пестунов**

RUSIEM
Всё под контролем

Обучение и мастер-классы от вендора

Онлайн- и оффлайн-форматы, эксперты-практики



Блок 1
- Архитектура системы
- Работа с событиями и поиск
- Симптоматика
- Ответы на вопросы

Блок 2
- Принцип работы с источниками, подключение источника
- Парсеры
- Дашборды, создание нового дашборда
- Отчеты и пример создания отчета
- Ответы на вопросы

Блок 3
- Корреляция, создание нового правила, редактирование правила
- Инциденты, имитация инцидента
- Ответы на вопросы

Блок 4
- Аналитика
- Ролевая модель
- Иерархия
- Ответы на вопросы

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

RUSIEM
Всё под контролем

Спасибо за внимание!

Даниил Вылегжанин
d.vylegzhanin@rusiem.com
+7 (926) 840 84 10