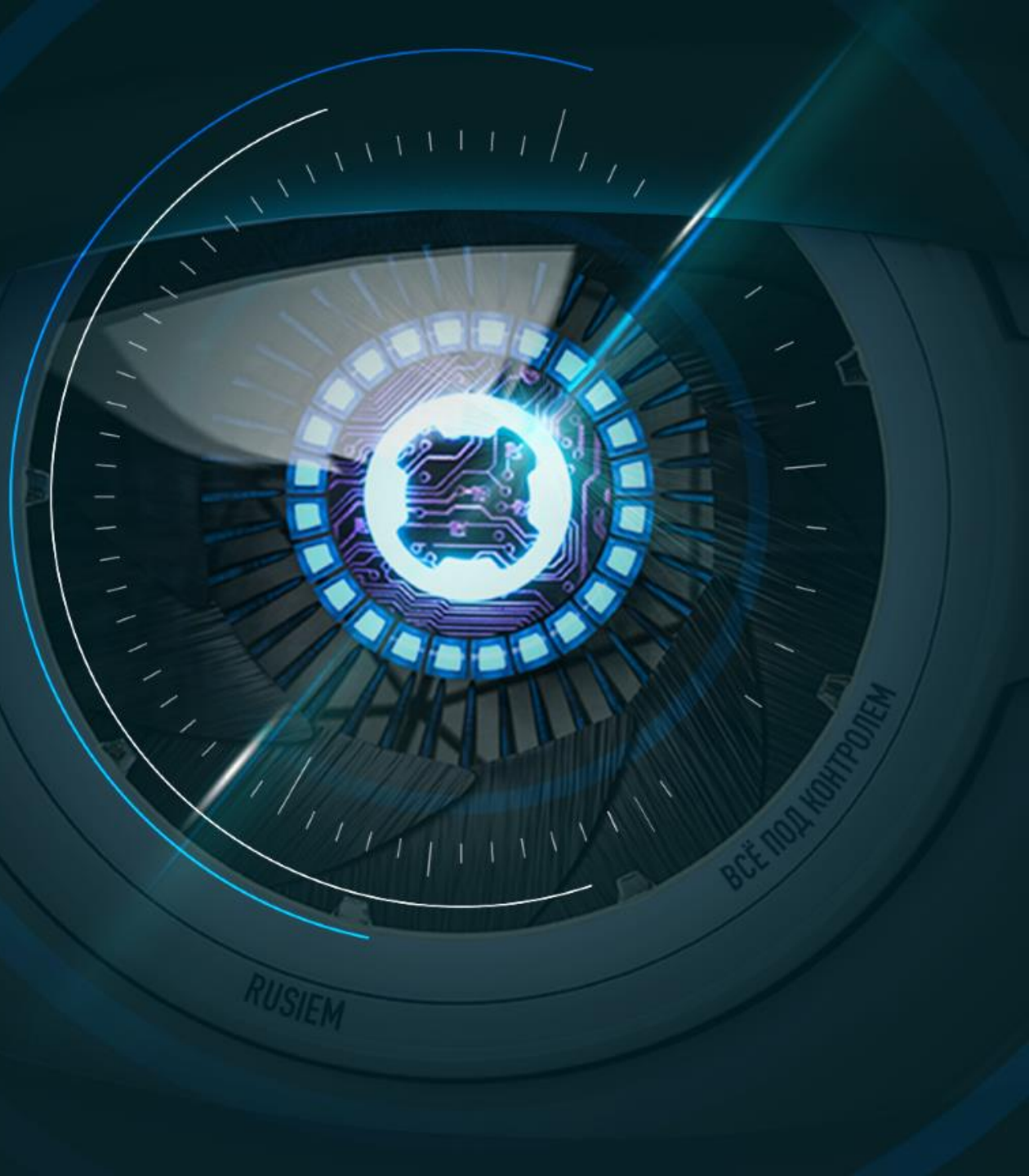
RUSIEM
Всё под контролем



RuSIEM: итоги 2021 планы 2022

Александр Булатов
Коммерческий директор
+7 916 830 75 57
a.bulatov@rusiem.com

О компании «РуСИЕМ»

2014 - год старта проекта

Sk Сколково - резидент Сколково

> 10000 - установок free-версии в мире с 2017 года

rusiem.com/ru/demo/downloads

скачать RvSIEM

RvSIEM Free vs RuSIEM

RUSIEM
Всё под контролем

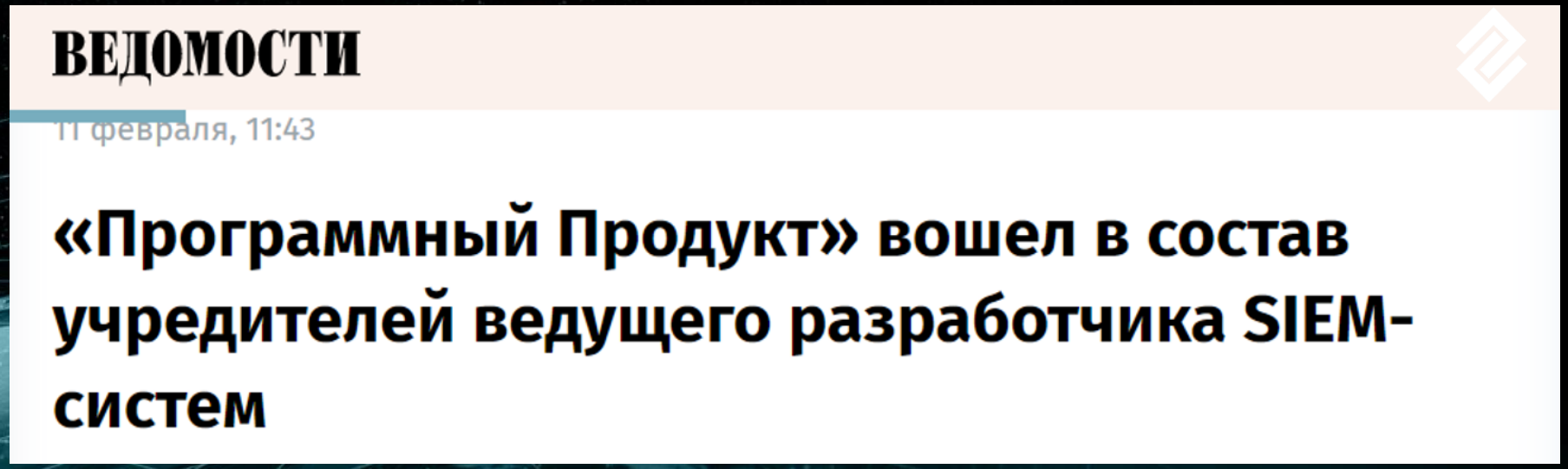
Telegram-каналы RuSIEM

https://t.me/**rusiem** - последние новости, важные события

https://t.me/**rusiemsupport** - возможность быстро связаться с технической поддержкой

О компании «РуСИЕМ»

2020



Группа компаний «Программный Продукт» работает на российском ИТ-рынке с 2002 года. Входит в список системообразующих предприятий российской экономики, ТОП-10 крупнейших российских разработчиков заказного ПО

SIEM-система RuSIEM

- Сертификат соответствия ФСТЭК России (№ 4402)
- Единый реестр отечественного ПО (№ 3808)
- Интеграция с ГосСОПКА

> 100 партнеров в России и СНГ

2020-2021 - десятки реализованных проектов для коммерческих и государственных организаций

> 150 пилотных внедрений

Некоторые КЛИЕНТЫ

Т2 ТИТАН2 холдинг

ЦОДД

Пойдём! Банк, который вам по душе

РСХБ страхование

АКСОН

КТ ГРУППА КРОНШТАДТ

МЕДСИ медицина компетенций

ФОРАБАНК

Санкт-Петербургский университет ГПС МЧС России

ГЕМОТЕСТ медицинская лаборатория

ПРИМ ТЕПЛО ЭНЕРГО

ГКУ СК «КРАЕВОЙ ЦЕНТР ИНФОРМТЕХНОЛОГИЙ»

РЕШЕНИЕ

RUSIEM

Всё под контролем

система мониторинга и управления событиями информационной безопасности на основе симптомов и анализа данных в реальном времени, для крупных и средних компаний

Линейка продуктов

RvSIEM (free)
– классическое решение класса LM

RuSIEM
– коммерческая версия класса SIEM

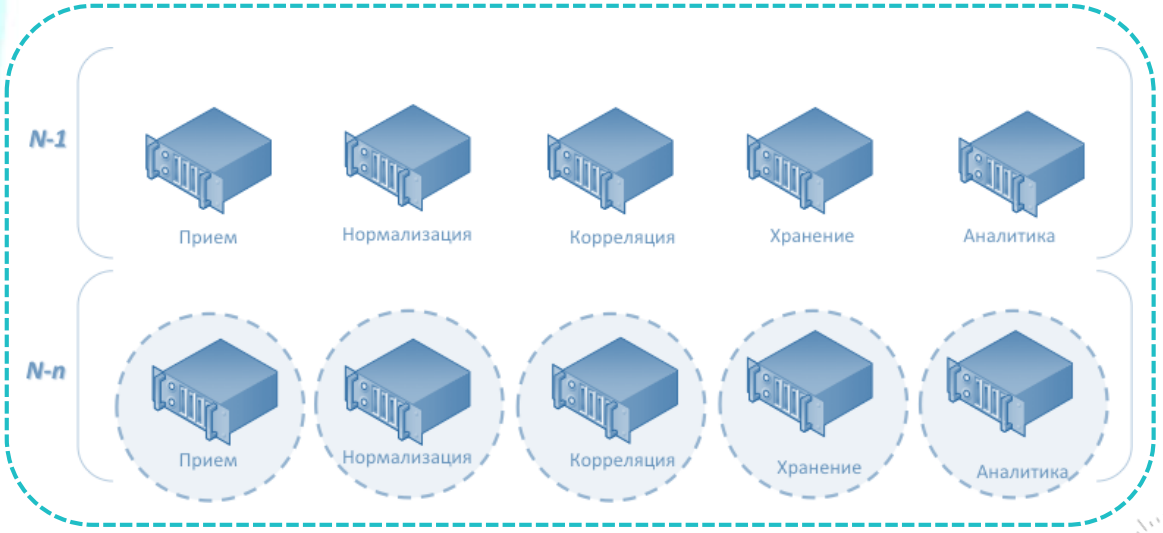
RuSIEM Analytics
– модуль для коммерческой версии, дополненный ML

ИСТОЧНИКИ СОБЫТИЙ

- Сервера Linux
- Сервера Windows
- Network flow
- Сетевые устройства
- Рабочие станции
- Сервера приложений
- Веб-сервера
- Антивирусные системы
- Контроллер домена
- СКУД
- IPS/IDS
- Межсетевые экраны
- Сервера БД
- Прочие источники

МАСШТАБИРУЕМОСТЬ

- Вертикальное расширение (подключение филиалов)
- Горизонтальное расширение (производительность)
- Горячее расширение без остановки сбора событий
- Разделение нагрузки на несколько серверов или ВМ



ЛИЦЕНЗИРОВАНИЕ

- Лицензирование по интенсивности потока событий (EPS – events per second);
- Срок лицензии;
- Техническая поддержка;
- Дополнительные модули;
- Дополнительная разработка нетиповых парсеров и коннекторов.

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

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

- Приказы ФСТЭК России №№ 17, 21, 31, 239
- 152-ФЗ, 161-ФЗ, 187-ФЗ
- ГОСТ 57580
- Приказ ФСБ России № 282
- СТО БР ИББС и РС БР ИББС-2.5-2014
- Международный стандарт ISO 27001

Влияние регуляторов на рынок крайне ценно, так как многие СЗИ начинают использовать в приказном порядке и лишь потом осознают их пользу

ФЗ и другие нормативные документы создают благоприятную среду для массового изучения и применения более сложных ИБ-продуктов, таких, как SIEM (EDR, XDR, PAM)

RUSIEM
Всё под контролем

Соответствовать требованиям регуляторов

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

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

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

RUSIEM
Всё под контролем

Быть удобнее для пользователя

- **Документация**
  - ➢ система перешла на удобную актуализируемую online-документацию в формате Wiki

- **Горячее/Холодное хранение**
  - ➢ разделение зоны хранения на участки для оперативного и неоперативного использования с разным выделением ресурсов

- **Оптимизация производительности**
  - ➢ уменьшение требуемых ресурсов под установку системы и увеличение её стабильности

- **Модуль активов**
  - ➢ введение актуальной информации об активах компаний в удобном интерфейсе, справочник уязвимостей

RUSIEM
Всё под контролем

Обнаруживать сложные угрозы

- **Динамические списки**
  - списки в памяти, используемые в правилах корреляции, для выявления более сложных современных угроз

- **Динамические таблицы**
  - создание таблиц в памяти для работы с ними в корреляции и симптоматике – для выявления более сложных угроз

- **RuSIEM IoC**
  - собственный список индикаторов компрометации – IP, домены для выявления актуальных угроз

RUSIEM
Всё под контролем

Мониторинг распределенной инфраструктуры

- **Филиальная структура**

➢ полноценная возможность создавать иерархические структуры SOC-ов с подчиненными SIEM-системами
  - ➢ обмен инцидентами
  - ➢ управление всеми настройками через интерфейс
  - ➢ разграничение прав доступа к информации

RUSIEM
Всё под контролем

Вектор развития

- Машинное обучение и нейросети
- Решение задач ИТ в дополнение к задачам ИБ
- Простота использования системы при сохранении производительности

ОБУЧЕНИЕ

https://www.infosystems.ru/

АИС
АКАДЕМИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

Код - IS085 • Вендор: RuSIEM

Эксплуатация системы мониторинга, сбора и анализа событий RuSIEM

06 Декабря — **25 000 ₽**

Код - IS086 • Вендор: RuSIEM

Внедрение и развертывание системы мониторинга, сбора и анализа событий RuSIEM

07 - 08 Декабря — **45 000 ₽**

ОБУЧЕНИЕ

Запись мастер-класса КОД ИБ

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АКАДЕМИЯ

ИСПОЛЬЗОВАНИЕ SIEM-СИСТЕМЫ RUSIEM

АЛЕКСЕЙ НИКИТИН

Начальник отдела внедрения и сопровождения ПО RuSIEM

https://codeib.ru/

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. Например, 10 попыток неудачного входа и потом 1 удачный. Назначение инцидента, закрытие инцидента
- *Ответы на вопросы*

Блок 4

- Аналитика
- Ролевая модель
- Иерархия
- *Ответы на вопросы*

От теории к практике

RUSIEM
Всё под контролем

ИНЦИДЕНТ. Хронология. Событие №1

Проникновение злоумышленника в ИТ-инфраструктуру, зашифрованы два сервера

ИНЦИДЕНТ. Хронология Событие №2

Терминальный сервер скомпрометирован. 2 домена с Golden Ticket. Потребован выкуп.

ИНЦИДЕНТ. Хронология Событие №3

Брутфорс с получением доступа к серверу партнеров

СОБЫТИЕ 1
Проникновение, зашифровали пару серверов, потребовали выкуп

СОБЫТИЕ 2
Терминальный сервер скомпрометирован. 2 домена с Golden Ticket

ИНЦИДЕНТ. Хронология

9 МАРТА 2021

Выведены из строя более 10 серверов, потребовали выкуп. Угроза остановки инфраструктуры

9 МАРТА 2021

Подключение специалистов к расследованию, развернули SIEM, выявили точки проникновения и зараженные узлы

ИНЦИДЕНТ. Реагирование и защита

Развернули SIEM

- *30 минут на установку системы*
- *2 часа на подключение основных источников*

Форензика зараженных узлов и сети

- *Таймлайн и атрибуция атак*

Настройка логирования с дополнительных источников в SIEM

Планирование блокировки заражения и защиты

В результате обнаружено:

- Зараженные узлы и точки проникновения
- Много закладок с внешним доступом, WannaCryptor и др.
- Syn-flood в сети
- Golden Ticket
- Brute-Force и компрометация сервера партнеров

ИНЦИДЕНТ. Реагирование и защита

- Контроль всех инцидентов в SIEM
- Закрыли все точки входа, оставили 1 – центральную
- Была перенастроена сеть по правилу: все, что не разрешено, то запрещено
- Доступ только к процессинговой системе банка – как бизнес-критичному сервису
- Бэкап всех критичных сервисов на внешнее хранилище
- Новая, защищенная доменная инфраструктура
- Изолированная инфраструктура, куда переносятся узлы после тщательной проверки
- Зараженные узлы выводятся из сети и обнуляются

Что было обнаружено?

После подключения основных источников –

автоматический анализ событий SIEM-системой

Было обнаружено

- Malware 9 шт.
- The onion router 1 шт.
- WanaCryptor 3 шт.
- WannaCry Killswitch Domain HTTP Request 4 шт.
- Сканеры уязвимостей 33 шт.
- Брутфорс 8 шт.
- Syn Flood в сети
- Golden Ticket
- Скомпрометированный сервер партнеров

И множество иных, менее значимых инцидентов

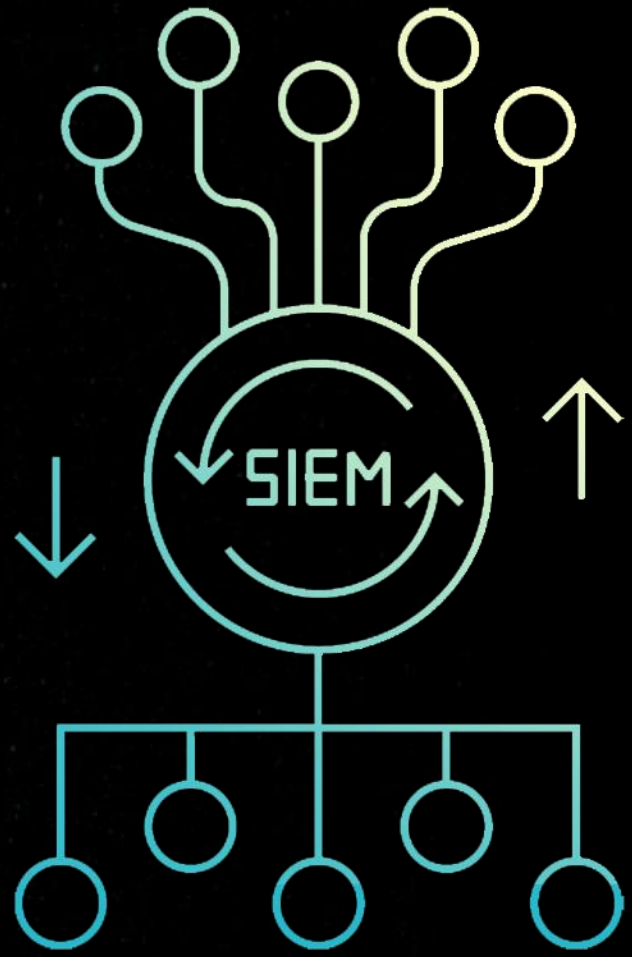
ИНЦИДЕНТ. Хронология

10 МАРТА 2021
Ограничили распространение, изолировали сеть, сняли бэкапы критичных сервисов

11 МАРТА – 25 МАРТА 2021
Защита сети

Инцидент. Реагирование. Итоги

- Благодаря проделанной работе удалось полностью отразить атаку злоумышленников
- Составлен план последующих действий
- Новая доменная инфраструктура с чистыми хостами
- Процедура архивации
- Единая точка входа
- NGFW для контроля периметра
- Все источники в SIEM и инциденты мониторятся
- Усиленная политика ИБ и парольная политика



Предложение

- Демонстрация решения RuSIEM
- Расширенный пилотный проект
- Аналитический отчет по результатам пилотного проекта

RUSIEM
Всё под контролем

RUSIEM
Всё под контролем

Спасибо за внимание!

Появились вопросы?
ОБРАЩАЙТЕСЬ!

Александр Булатов
Коммерческий директор

a.bulatov@rusiem.com
www.rusiem.com
+7(495)748-83-11
+7 916 830 75 57