



**RUSIEM**

Всё под контролем

# ***Выявление киберугроз и реагирование на инциденты информационной безопасности***

***Екатерина Лазарева,  
менеджер по работе с ключевыми заказчиками***

# RuSIEM – это



Полностью  
русская разработка  
(с 2014 года)

Sk Сколково

Резидент  
Сколково

> 550

Партнеров в России и  
странах СНГ



Продукт включен  
в Единый реестр  
отечественного ПО



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



**Что?**

SIEM – единый экран мониторинга  
всей ИТ-инфраструктуры  
организации

**Зачем?**

Чтобы увидеть полную картину  
активности сети и  
событий безопасности

**Где?**

Везде, где из журналов событий  
можно извлечь  
полезную информацию





# Задачи SIEM



Оперативное обнаружение, реагирование и контроль обработки инцидентов



Оперативный контроль состояния инфраструктуры компании



Создание единого центра мониторинга



Определение прав, обязанностей и разграничение зон ответственности персонала компании (ИТ- и ИБ-служб)



Соответствие требованиям регуляторов  
(Федеральные законы № 152-ФЗ, 161-ФЗ, 187-ФЗ, приказы ФСТЭК России № 21, 17 и 31,  
СТО БР ИББС и РС БР ИББС-2.5-2014, международного стандарта PCI DSS, ISO 27001)



# SIEM-система RuSIEM

Более 350  
источников  
событий «из  
коробки»

Более 400  
правил  
корреляции  
для анализа  
событий

**35**  
Предустановленных  
шаблонов отчетов

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



Антивирус








Межсетевой  
экран

IPS и IDS






Почтовые  
системы

Прочее ПО

# Схема работы SIEM

-  Рабочие станции
-  Firewall
-  Роутеры
-  Сетевые коммутаторы
-  Серверы
-  Мейнфреймы
-  Системы обнаружения и предотвращения вторжений

SIEM

-  Предупреждения
-  Дашборды
-  Журнал событий
-  Отчеты
-  Мониторинг



# 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



# Где может применяться 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



# 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

# 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»



# 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

# RvSIEM Free vs RuSIEM





# RuSIEM Analytics

Модуль анализа событий, основанный на ML

- Выявление поведенческих аномалий методами машинного обучения в случаях, когда логику инцидента невозможно описать правилами корреляции
- Технологичность алгоритмов машинного обучения в процессе поиска аномалий позволяет **выявлять на ранней стадии** и **предотвращать** возможные инциденты ИБ



# RuSIEM IoC

Модуль выявления угроз для корпоративных устройств на основе индикаторов компрометации

- Автоматическая настройка
- Анализ данных из более чем 260 открытых источников
- Сбор индикаторов из социальных сетей (Telegram, Twitter), репозиториях Github, данных 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



# *RuSIEM Monitoring*

Система мониторинга ИТ-инфраструктуры с возможностью удаленного администрирования и встроенной системой HelpDesk

Позволяет контролировать работу ИТ-решений, входящих в периметр комплексной ИТ-инфраструктуры

- Мониторинг параметров всех компонентов
- Оповещение специалистов, если значения оказываются вне заданных рамок
- Детальный анализ производительности оборудования
- Оперативное устранение и предотвращение сбоев в работе

# Лицензирование

Кол-во событий в секунду  
(Event per second)

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


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

...



# Преимущества RuSIEM





# Построение Центра Мониторинга Информационной безопасности (SOC)

Примеры проектов



# 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



# SOC на RuSIEM

SOC был развернут для ряда крупных заказчиков на базе SIEM-системы RuSIEM совместно с партнерами





# *История одного инцидента*



# Хронология инцидента

## СОБЫТИЕ 1

Проникновение, зашифровали пару серверов, потребовали выкуп

## СОБЫТИЕ 2

Терминальный сервер скомпрометирован. 2 домена с Golden Ticket

## СОБЫТИЕ 3

Брутфорс с получением доступа к серверу партнеров

## 9 МАРТА 2021

Выведены из строя более 10 серверов, потребовали выкуп. Пригрозили убить все

## 9 МАРТА 2021

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

## 10 МАРТА 2021

Ограничили распространение, изолировали сеть, сняли бэкапы критичных сервисов  
Параллельно вели переговоры со злоумышленниками – затягивание времени

11 МАРТА –  
25 МАРТА 2021  
Защита сети




**RUSIEM**  
Всё под контролем



# Что происходит?

**Была вероятность захвата  
сети злоумышленниками**

*Злоумышленники обещали привести  
в действие логическую бомбу  
11 марта в 12:00*

A large, stylized thought bubble with a white outline and a light blue fill. Inside the bubble, there are three lines of binary code (0s and 1s) arranged in a slightly curved, descending pattern. The background of the slide is dark blue with a network of glowing lines and nodes, suggesting a digital or cyber environment.

```
10101101110011110010111  
01101100000111000011010  
01111101011001001100001
```



# Расследование инцидента

## 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

## Результат

- 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



# Что было обнаружено?

Следующим шагом за ручным анализом после подключения основных источников был анализ с помощью SIEM

## 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

# RuSIEM | Всего найдено

The screenshot displays the RuSIEM interface with the following components:

- Header:** "RuSIEM" logo and "RUS" language selector.
- Left Sidebar:** Navigation menu with categories like "Инциденты", "Мои инциденты", "Все инциденты", and "Закрываемые".
- Filtering and Summary:** "Группировать по: Категория", "Ж", "Кол-во: 99", and "Поиск" field.
- Donut Charts:** "Статусы" (Assigned: 8434, Other: 0) and "Приоритет" (1: 117, 3: 5138, 5: 32, 2: 3147).
- Table:** Table with columns: ID, Наименование, Категория, Приоритет, Статус, Назначен, Исполнитель, Объект, Суммарный вес симптомов, Количество событий, Дата создания, Дата изменения.
- Table Content:** Malware (9), RuSIEM (46), The Onion Router (TOR) (1), Windows (32), Аномалии (121), Аудит (24), Аутентификация (1), Аутентификация и авторизация (67), Брутфорс (8), Входы/выходы (2829), Нарушение политик (252), Общие веб атаки (1), Отслеживание ПО (24), Сбои в инфраструктуре (177), Сканы уязвимостей (39), Средства удаленного администрирования (48), Угрозы (88), Управление учетными записями и группами (4662).
- Footer:** "Записи с 1 по 18 из 18 записей".



# Реагирование и защита

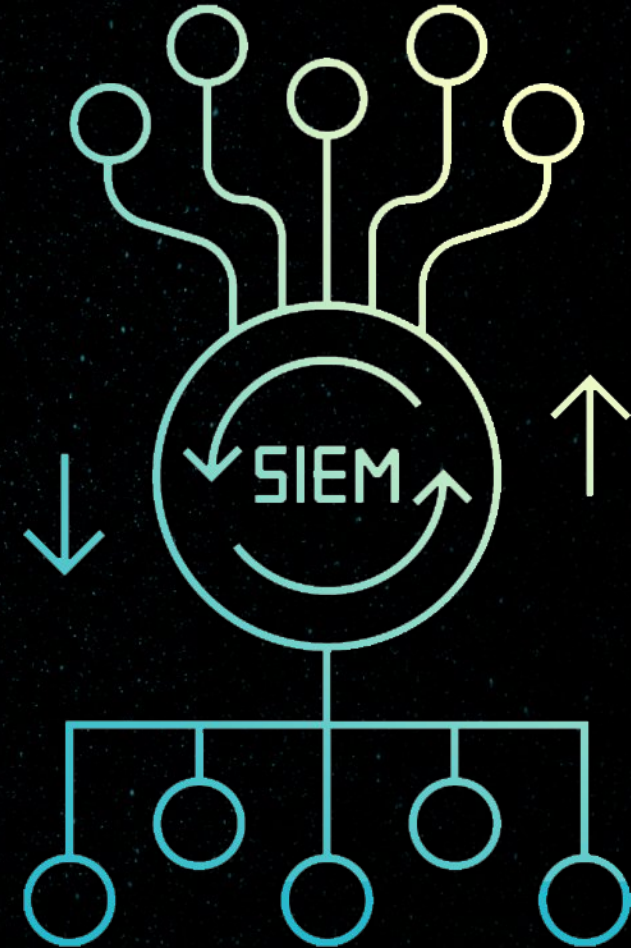
- Контроль всех инцидентов в SIEM
- Закрыли все точки входа, оставили 1 – центральную
- Была перенастроена сеть по правилу: все, что не разрешено, то запрещено
- Доступ только к бизнес-критичному сервису
- Бэкап всех критичных сервисов на внешнее хранилище
- Новая, защищенная доменная инфраструктура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





# Текущая ситуация

- 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





# Telegram-каналы RuSIEM

<https://t.me/rusiem>

*последние новости, важные события*






<https://t.me/rusiemsupport>

*возможность быстро связаться с технической поддержкой*



***Спасибо за внимание!***

-  Екатерина Лазарева
-  [e.lazareva@rusiem.com](mailto:e.lazareva@rusiem.com)
-  +7 (985) 714-07-71

