RUSIEM

Всё под контролем

Практика Использования SIEM Кейс из жизни

Максим Николаевич Степченков, совладелец RuSIEM

ЧТО ТАКОЕ SIEM И ЗАЧЕМ ОНА НУЖНА

SIEM представляет собой улучшенную систему обнаружения вредоносной активности и различных системных аномалий. Работа SIEM позволяет увидеть более полную картину активности сети и событий безопасности. Когда обычные средства обнаружения по-отдельности не видят атаки, но она может быть обнаружена при тщательном анализе и корреляции информации из различных источников.

Сотни и тысячи устройств живут своей жизнью и генерируют миллионы событий, сообщая о том, что происходит с ними и вокруг. При этом необходимо реагировать только на часть из них

Отдельные устройства, операционные системы только предоставляют события без детального анализа

Для полной картины происходящего необходимо собрать воедино состояния с отдельных устройств

Для этого и нужна SIEM-система

SIEM – система, которая собирает, анализирует и представляет информацию из сетевых устройств, средств защиты информации и информационных систем

Также в систему входят приложения для контроля идентификацией и доступом, инструменты управления уязвимостями

Инцидент. Хронология

RUSIEM
Всё под контролем

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

Что происходит?

RUSIEM
Всё под контролем

Была вероятность захвата сети злоумышленниками

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

Инцидент. Расследование

RUSIEM
Всё под контролем

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?

RUSIEM
Всё под контролем

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

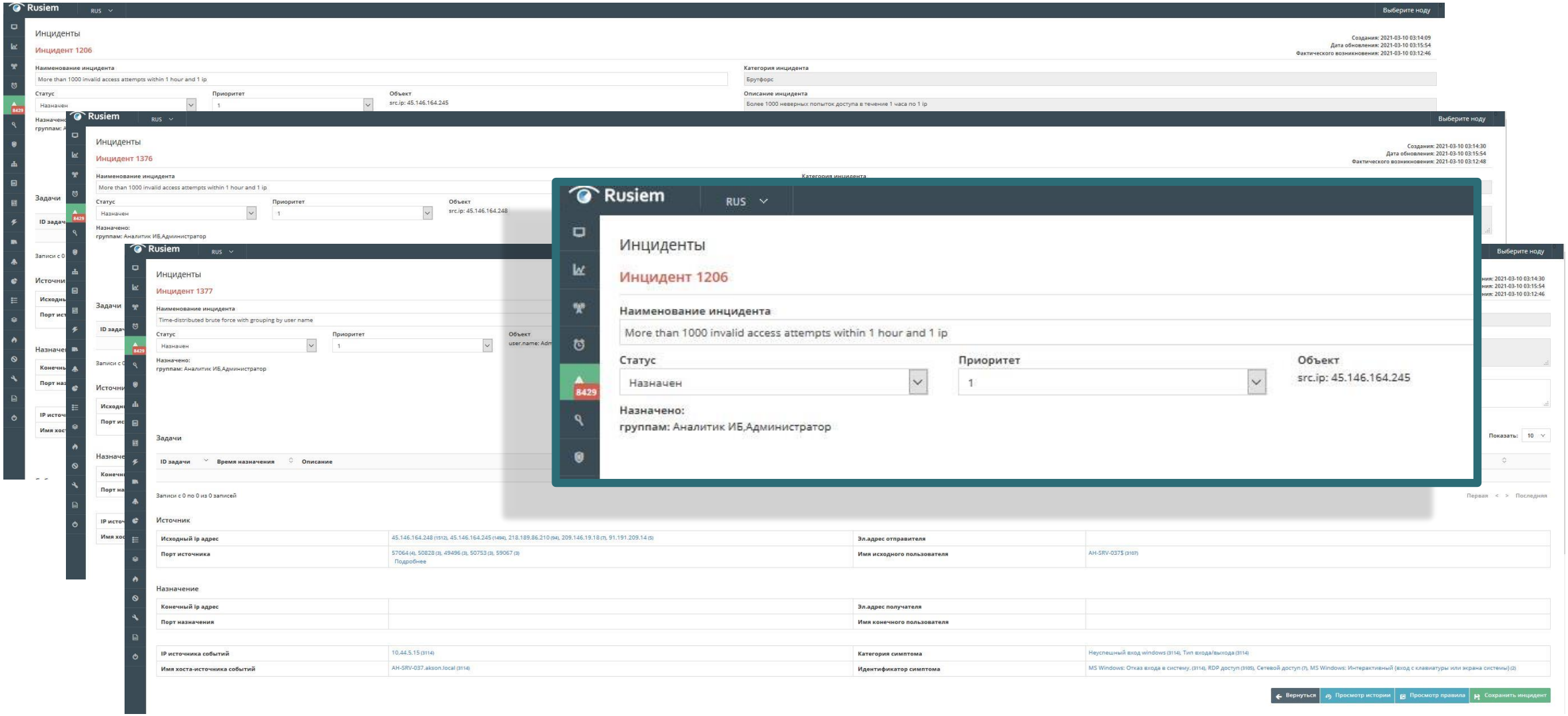
– Golden Ticket

– Скомпрометированный сервер партнеров

И множество иных, менее значимых инцидентов

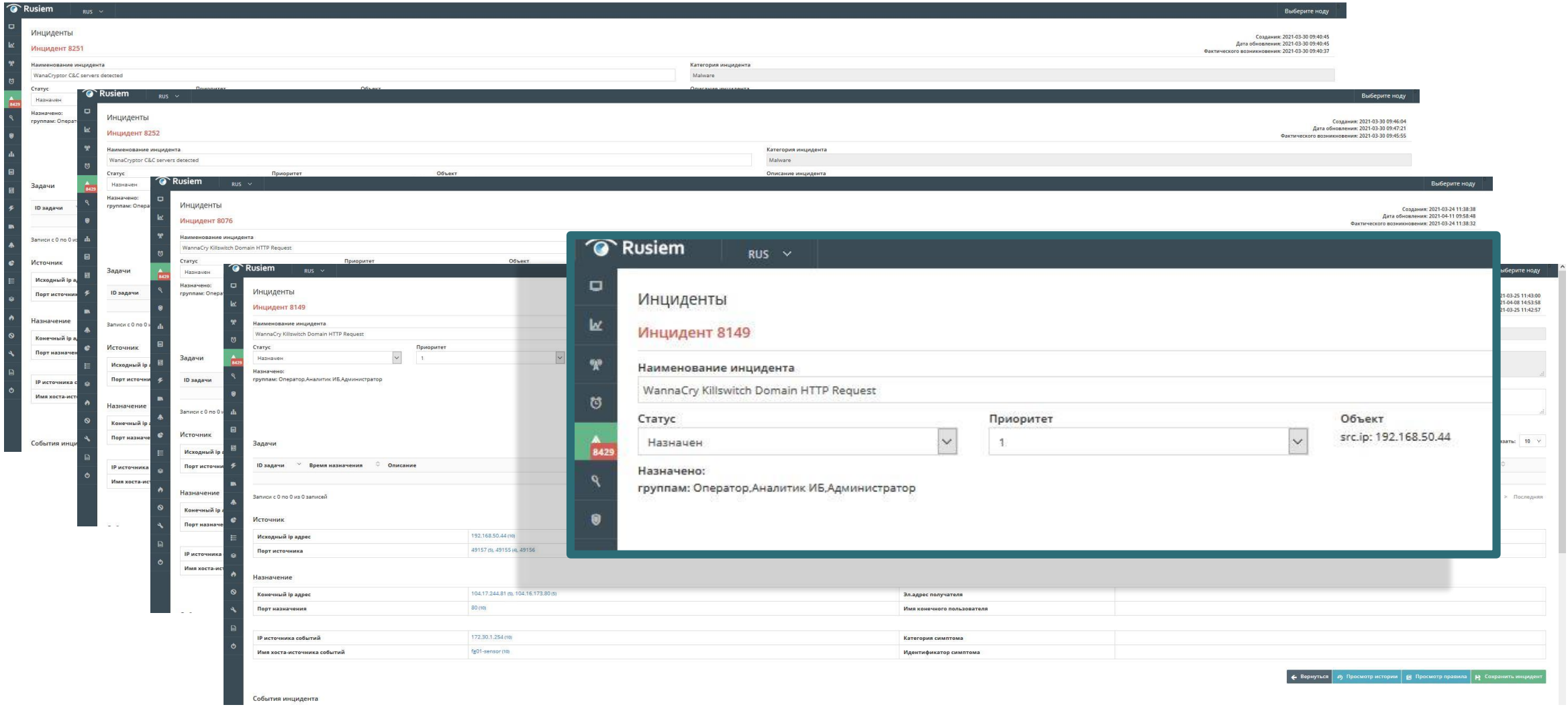
RuSIEM | Brute-Force

RUSIEM
Всё под контролем



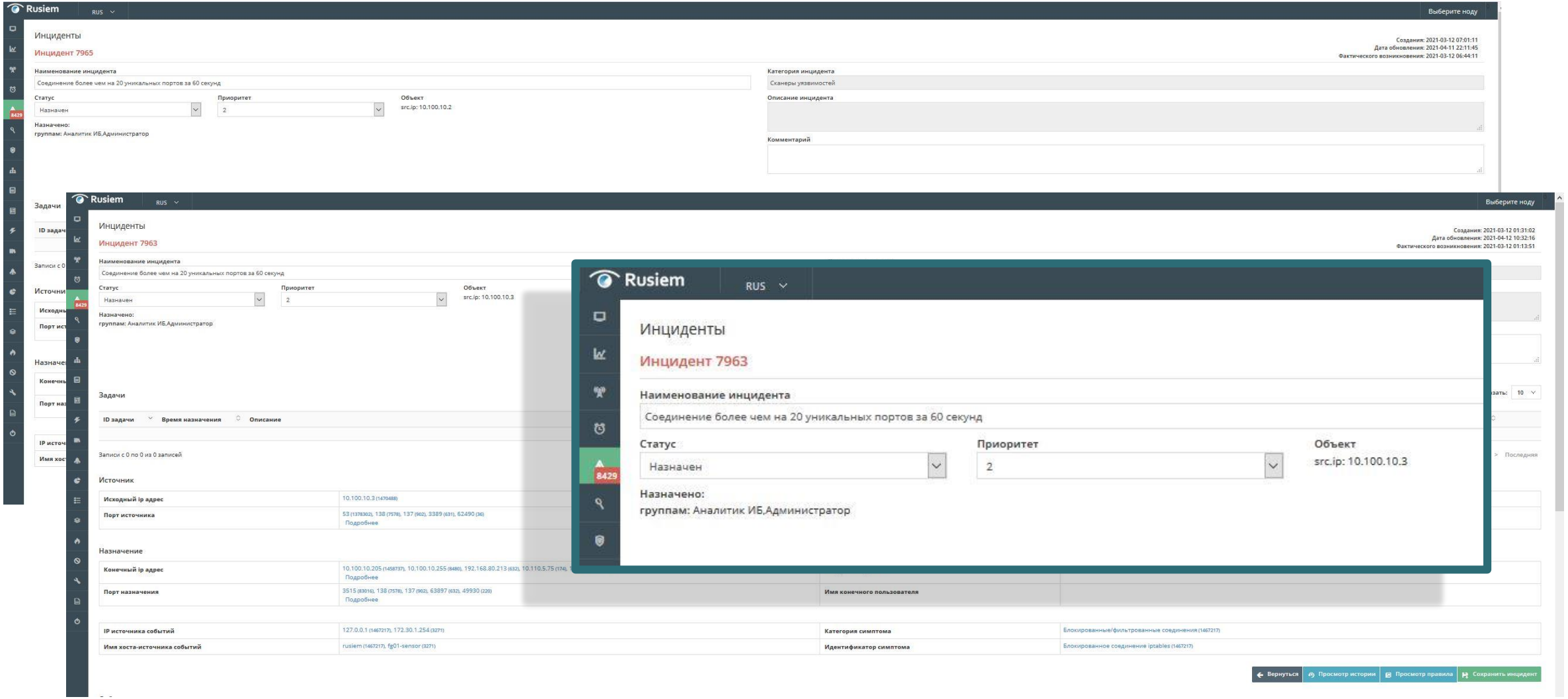
RuSIEM | WannaCryptor

RUSIEM
Всё под контролем



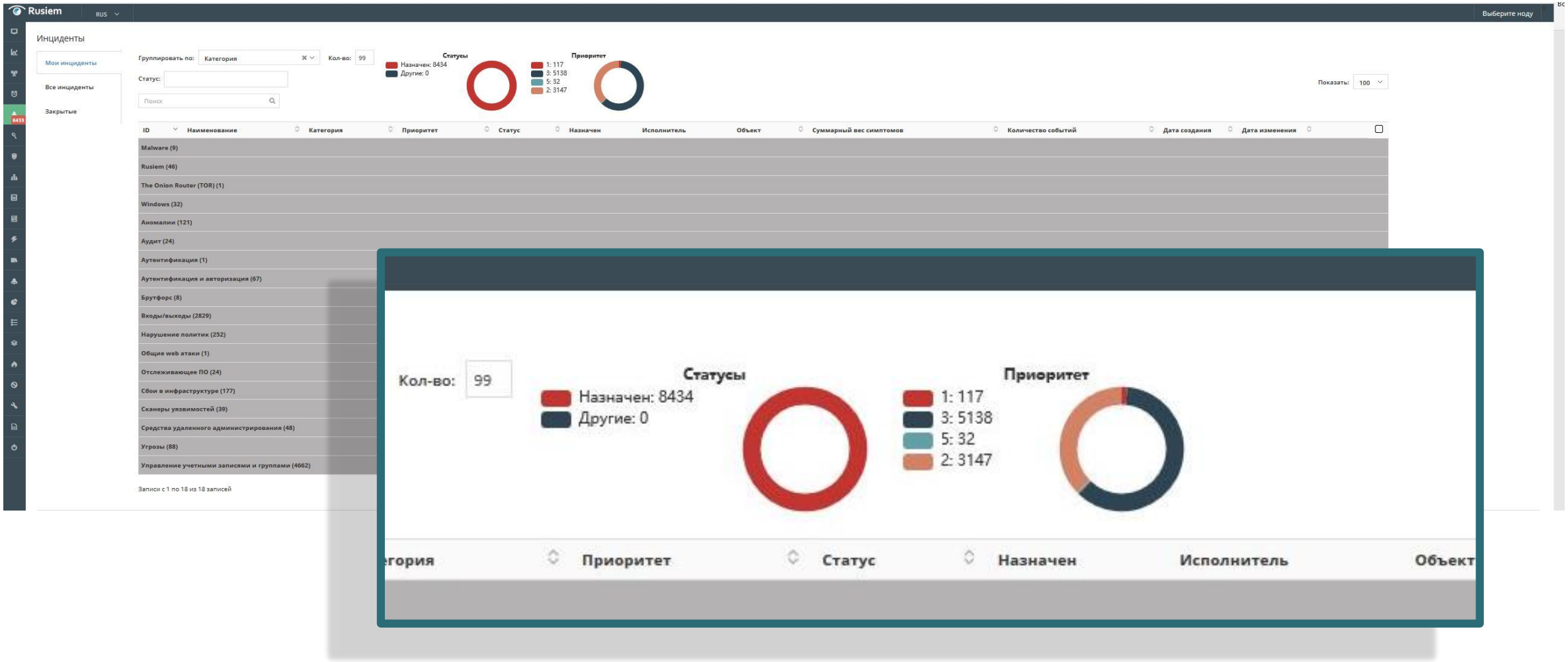
RuSIEM | Сканеры уязвимостей

RUSIEM
Всё под контролем



RuSIEM | Всего найдено

RUSIEM
Всё под контролем



Реагирование и защита

RUSIEM
Всё под контролем

– 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

RUSIEM
Всё под контролем

Сегодня 22 апреля

– Благодаря проделанной работе удалось полностью отразить атаку злоумышленников

– Составлен план последующих действий

– Новая доменная инфраструктура с чистыми хостами

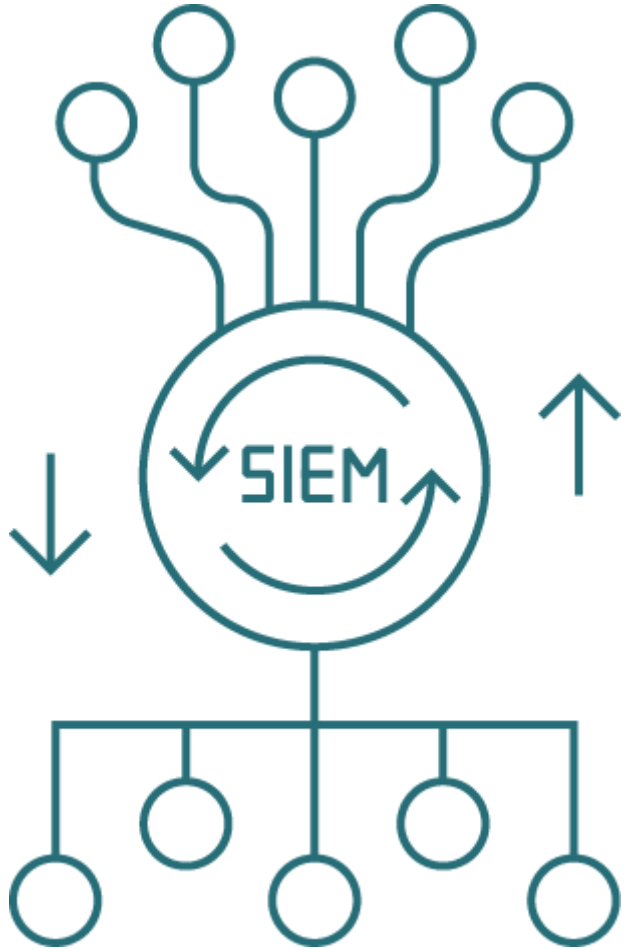
– Процедура архивации

– Единая точка входа

– NGFW для контроля периметра

– Все источники в SIEM и инциденты мониторятся

– Усиленная политика ИБ и парольная политика



Где может применяться SIEM?

RUSIEM
Всё под контролем

Везде, где из журналов событий можно извлечь полезную информацию

ПРИМЕРЫ СОБЫТИЙ

- Сетевые атаки
- Шифрование файлов
- Откуда и когда блокировались учетные записи
- Изменение конфигураций «не администраторами»
- Выявление несанкционированных сервисов
- Отсутствие антивирусной защиты на новом установленном компьютере
- Контроль выполняемых команд на серверах и сетевом оборудовании
- Аудит изменений конфигураций (сетевых устройств, приложений, ОС)
- Повышение привилегий
- Аномальная активность пользователя (массовое удаление/копирование)
- Обнаружение вирусной эпидемии
- Обнаружение уязвимости по событию об установке софта
- Оповещение об активной уязвимости по запуску ранее отключенной службы
- Обнаружение распределенных по времени атаках
- Влияние отказа в инфраструктуре на бизнес-процессы

Линейка продуктов RuSIEM

RUSIEM
Всё под контролем

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

RvSIEM (free) – классическое решение класса LM

RuSIEM коммерческая версия

RuSIEM Analytics

RuSIEM Agent – агент под Windows OS

SIEM vs LM

RUSIEM
Всё под контролем

LM | RvSIEM (free)

Сбор событий с источников

Отчеты

Поиск по событиям

Корреляция LM

Инцидент-менеджмент

Риск-менеджмент

Аналитика

SIEM | RuSIEM

Конкурентные преимущества

RUSIEM
Всё под контролем

Полная поддержка русского языка

Сохранение исходных RAW-событий

Приведенная к общем формату объектная нормализация

Нет ограничений по размеру архивного хранилища

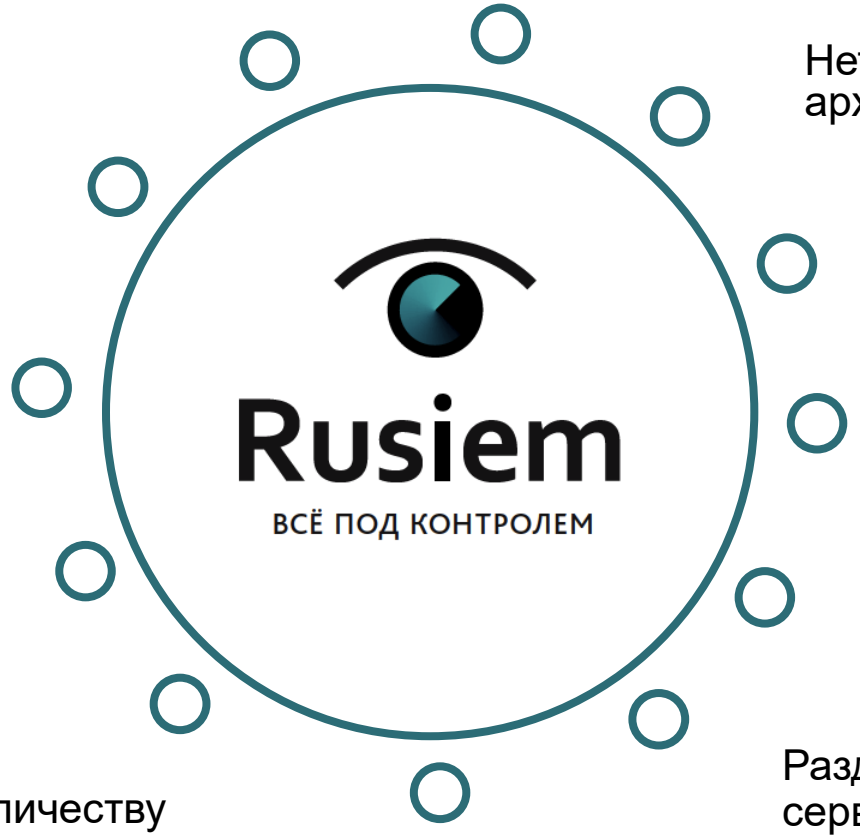
Коннекторы от производителя

Встроенная управляемая и редактируемая корреляция

Real-time и историческая корреляция

Высокая производительность (Свыше 90000 событий на одну ноду)

Наличие собственных модульных агентов



Разделение нагрузки на несколько серверов или виртуальных машин

Нет ограничений по количеству событий и источникам

Легкая вертикальная масштабируемость

О компании RuSIEM

RUSIEM
Всё под контролем

Программный код создан российскими программистами

>300

пилотных внедрений

Резидент Сколково

>50

партнеров в странах СНГ

2014

с этого года ведется активная разработка

Продукт включен в реестр отечественного ПО

10000

установок free-версии в мире в 2017-18 годах

Клиенты

RUSIEM
Всё под контролем

RUSIEM

Всё под контролем

Спасибо за внимание!

Ответим на все вопросы
Обращайтесь!

Контактная информация:

Сайт : www.rusiem.com

Почта: info@rusiem.com

Телефон: +7(495)748-83-11