RUSIEM
Всё под контролем

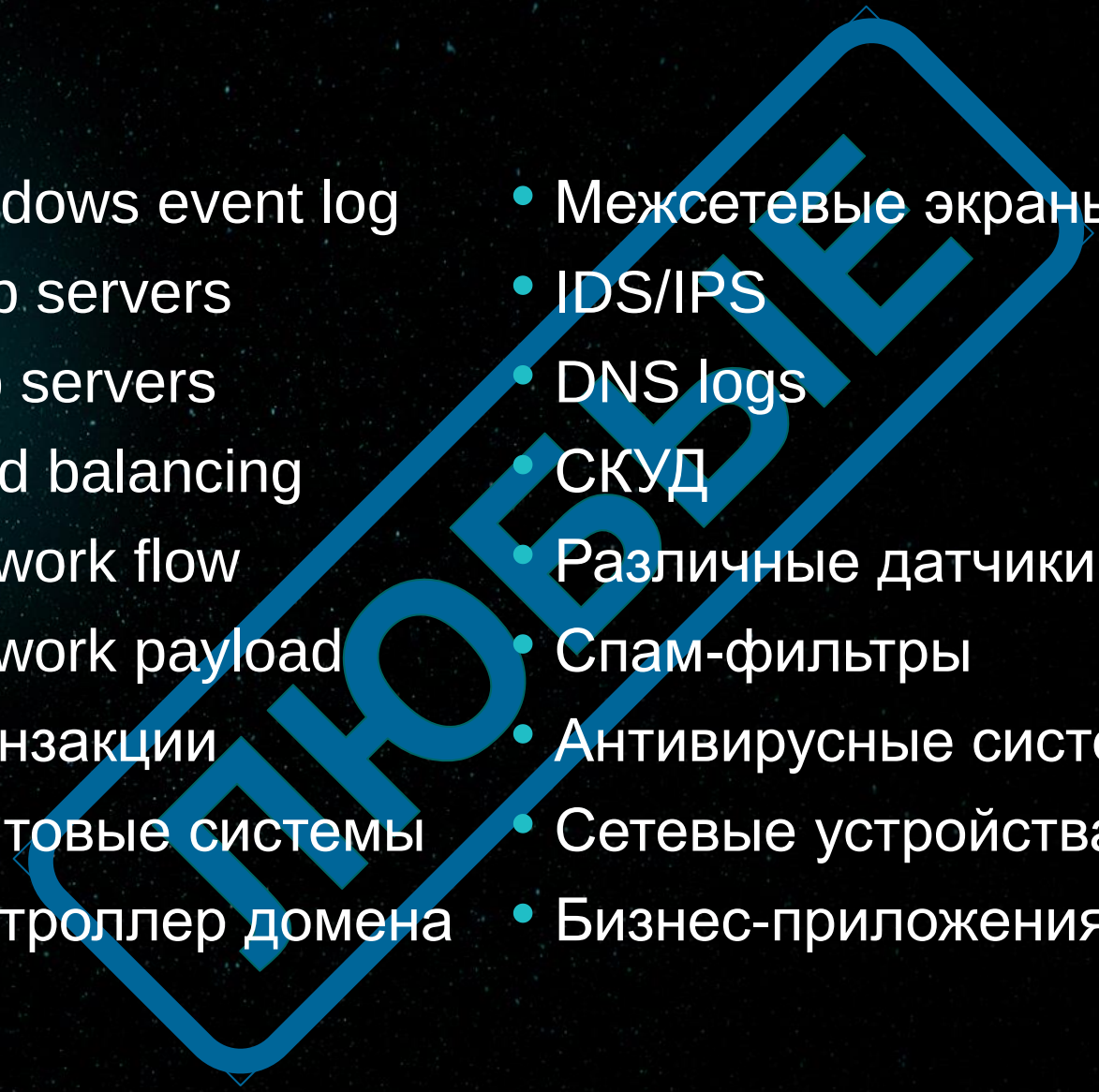
Выявление киберугроз и реагирование на инциденты информационной безопасности

Максим Степченков,
Совладелец компании

Схема работы SIEM

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

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

История одного инцидента

RUSIEM
Всё под контролем

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

RUSIEM
Всё под контролем

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?

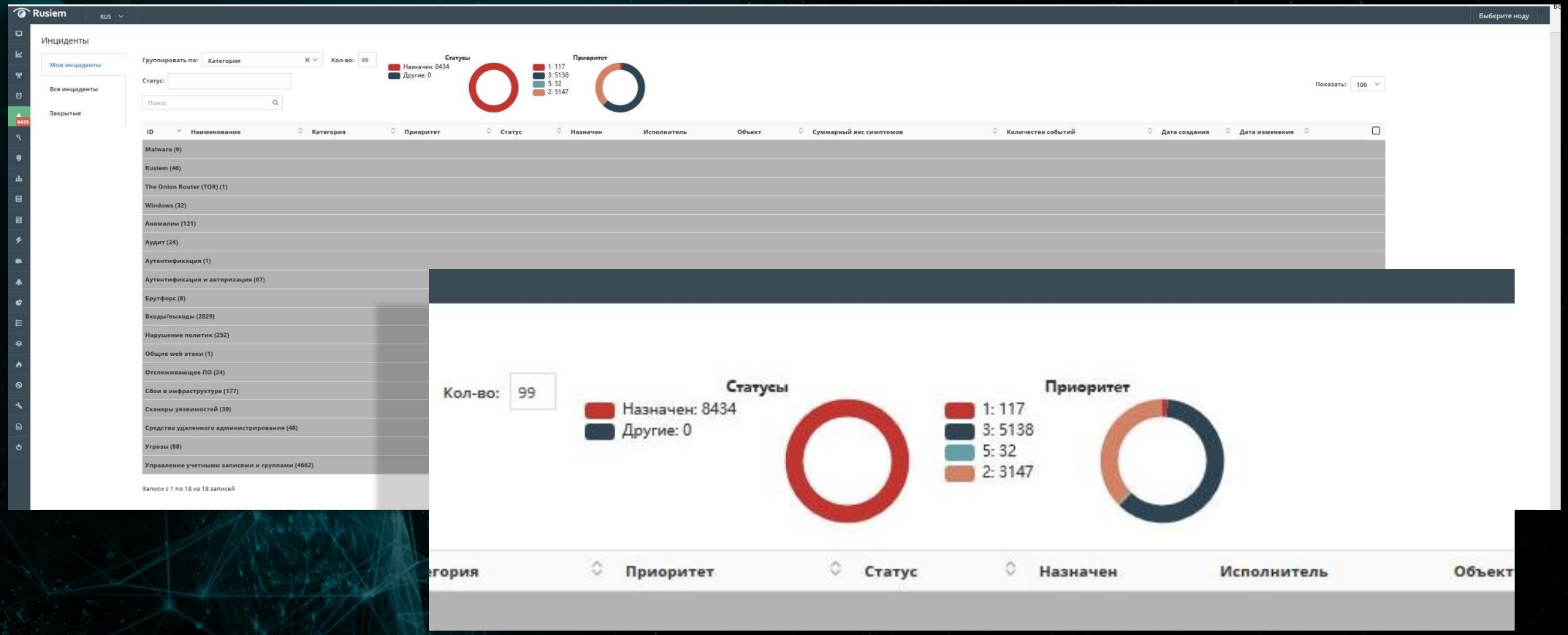
Следующим шагом за ручным анализом после подключения основных источников был анализ с помощью SIEM

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



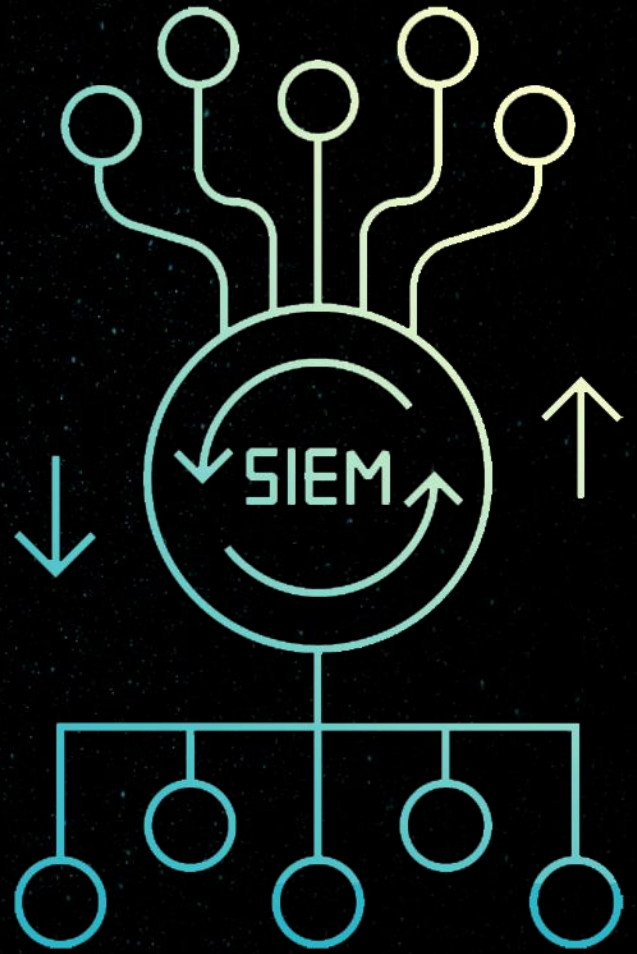
RUSIEM
Всё под контролем

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



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:

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)

ЭР-ТЕЛЕКОМ

Комплексное решение, которое обеспечивает проактивную защиту компаний от всех типов современных киберрисков и позволяет своевременно реагировать на инциденты, которые потенциально могут нанести финансовый или репутационный вред. Программные средства мониторинга можно развернуть как на инфраструктуре заказчика, так и по облачной модели, если клиент не готов тратить дополнительные серверные ресурсы

МегаФон МОБИЛЬНЫЙ ОПЕРАТОР №1 ПО СКОРОСТИ И ПОКРЫТИЮ by OOKLA 2022

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

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

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!

Максим Степченков
m.stepchenkov@rusiem.com
+7 (903) 164-31-31