RUSIEM
Всё под контролем

RuSIEM: поддерживаем организации в сложной ситуации

Чеботарев Дмитрий,
Менеджер по техническому сопровождению продаж

Актуальные кибератаки

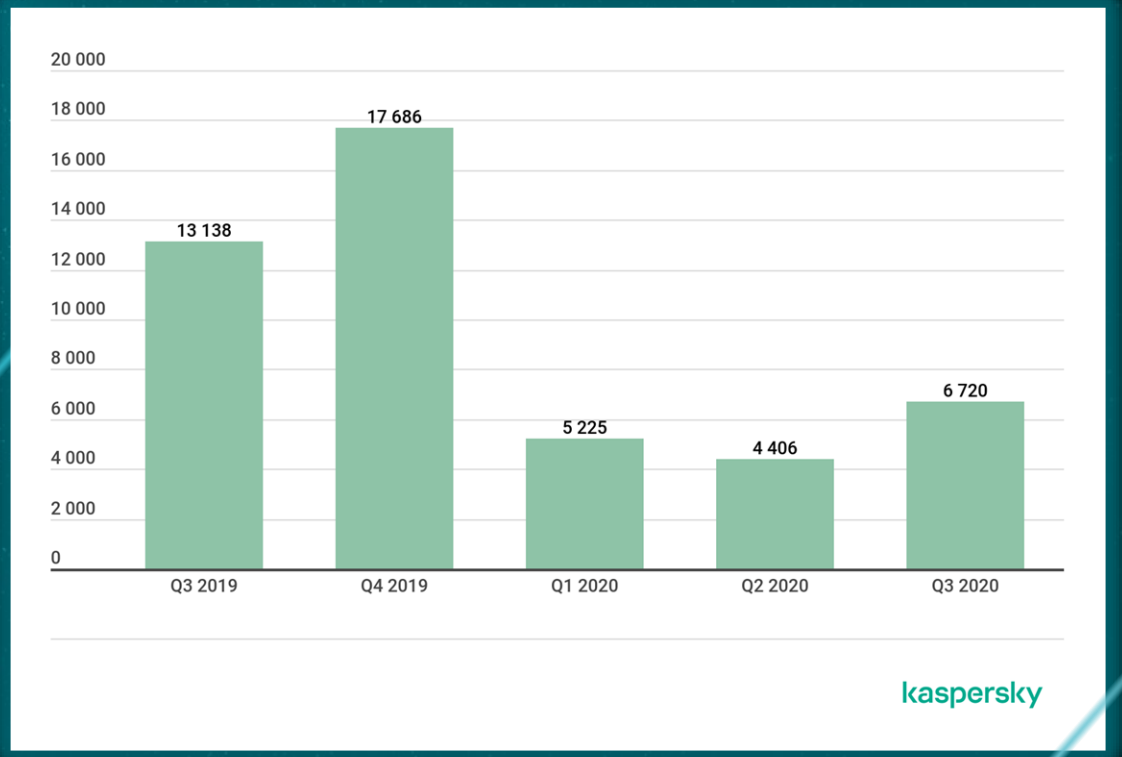
1,5 млрд

отраженных кибератак пришлось на Q3 2020 г.

2 из 3

кибератак Q3 2020 г. использовали уязвимости Microsoft Office

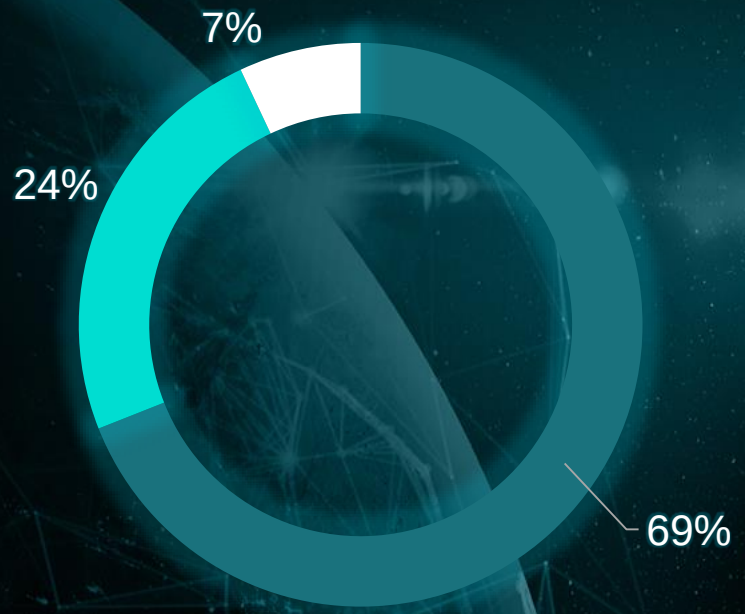
Количество модификаций шифровальщиков



RUSIEM
Всё под контролем

** По данным аналитического агентства Kaspersky*

Цели злоумышленников



Объекты атак

- Компьютеры, сервисы и сетевое оборудование
- Веб-ресурсы
- Люди

Чаще всего похищают

- Данные платежных карт
- Персональные данные
- Учетные данные
- Коммерческую тайну, ноу-хау
- Личную переписку

RUSIEM
Всё под контролем

Последствия

23%

организаций подверглись атакам, которые завершились прямыми финансовыми потерями

Возможные риски

- Фрод и мошенничество
- Нарушение непрерывности
- Несанкционированный доступ к данным
- Кибершпионаж и конкурентная разведка

Последствия

- Прямые финансовые потери
- Репутационные потери компании и ключевых лиц
- Компрометация данных
- Санкции со стороны регуляторов

Неэффективность стандартных средств защиты

7 из 10*

кибератак на организации в Q2 2020 г. совершены с применением вредоносного ПО, способного обойти антивирусную защиту

Методы атак

- Сетевые комбинированные атаки
- Социальная инженерия
- Использование вредоносного программного обеспечения
- Эксплуатация веб-уязвимостей
- Подбор учетных данных

** По данным аналитического агентства WatchGuard*

С начала 2022 года

По данным Лаборатории Касперского, наибольшая доля кибератак пришлась на

- *финансовые организации – 35%*
- *государственные органы – 33%*
- *образовательные учреждения – 9%*
- *СМИ – 3%*
- *другие сферы – 20%*

В Минцифры РФ подтвердили, что число атак на государственные органы увеличилось десятикратно

RuSIEM – это

Программный код создан российскими специалистами

> 300

Пилотных внедрений

Sk Сколково

Резидент Сколково

ГК «Программный продукт» входит в состав учредителей компании

> 100

Партнеров в России и СНГ

2014

С этого года ведется активная разработка

Продукт включен в Единый реестр отечественного ПО

Сертификат ФСТЭК России

ГОССОПКА

Интеграция с ГосСопка

> 10000

Установок free-версии в мире в 2017-18 годах

Что такое SIEM

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

SIEM

- Предупреждения
- Дашборды
- Журнал событий
- Отчеты
- Мониторинг

Зачем нужна SIEM

- **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 сопоставлении 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 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

Пример использования 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 SIEM есть даже свой внутренний функционал работы с активами)
- Система веб-фильтрации

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

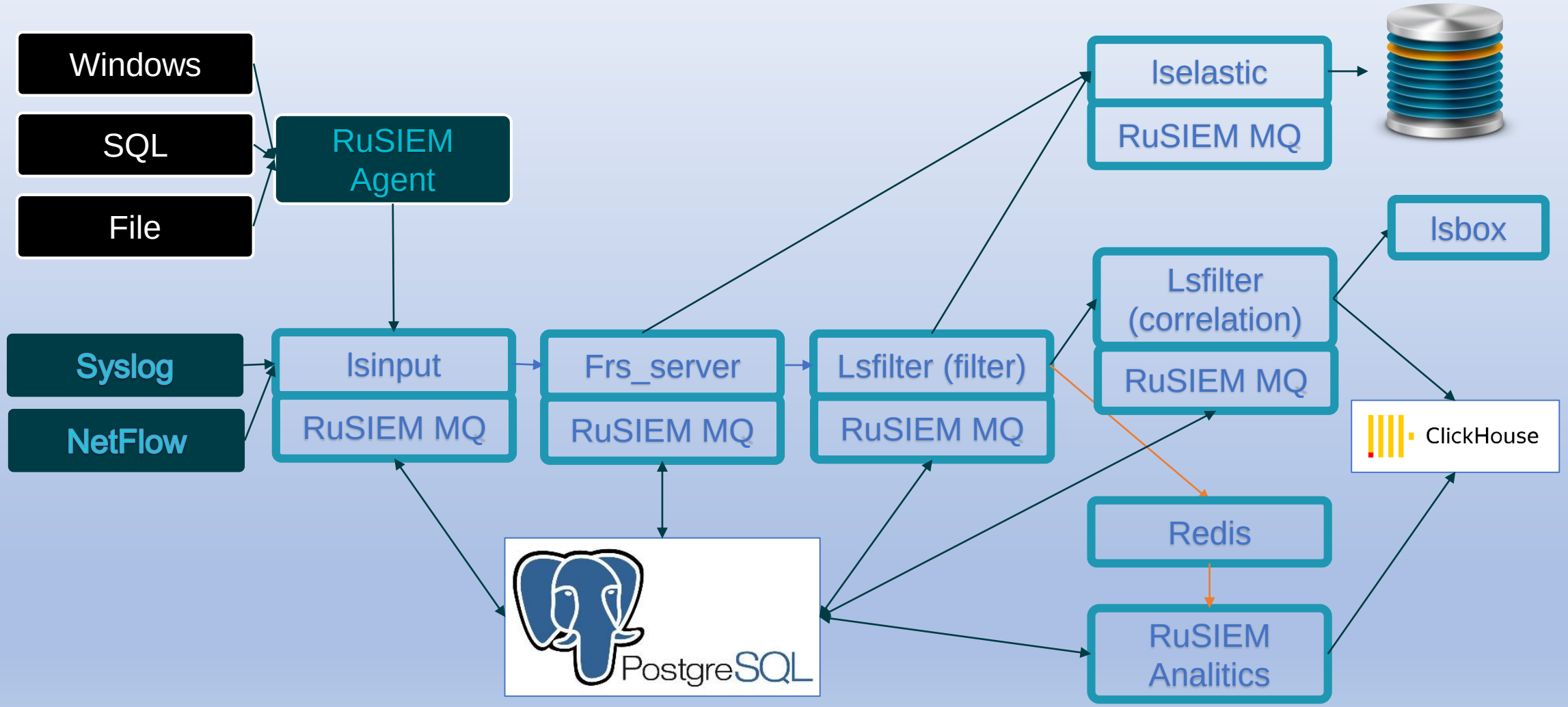
Линейка продуктов

RvSIEM (free)
– классическое решение класса LM

RuSIEM
– коммерческая версия класса SIEM

RuSIEM Analytics
– модуль для коммерческой версии, дополненный DL

АРХИТЕКТУРА



Основные микросервисы, через которые проходит каждое событие

- Сбор событий с источников
- Прием
- Нормализация
- Симптоматика
- Корреляция
- Аналитика

SOC для бизнеса – совместный проект с ЭР-Телеком

Ведущая российская телекоммуникационная компания, предоставляющая решения и услуги по информационной безопасности, широкополосного доступа в Интернет, телефонии, цифрового ТВ, доступа к сетям Wi-Fi, VPN, видеонаблюдения, IoT

Совместное решение

- *Мониторинг событий и инцидентов ИБ в режиме 24/7*
- *Подключение к ГосСОПКА*
- *Модуль реагирования*
- *Модуль аналитики*

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»

Что мы делаем, чтобы Вы соответствовали?

- **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

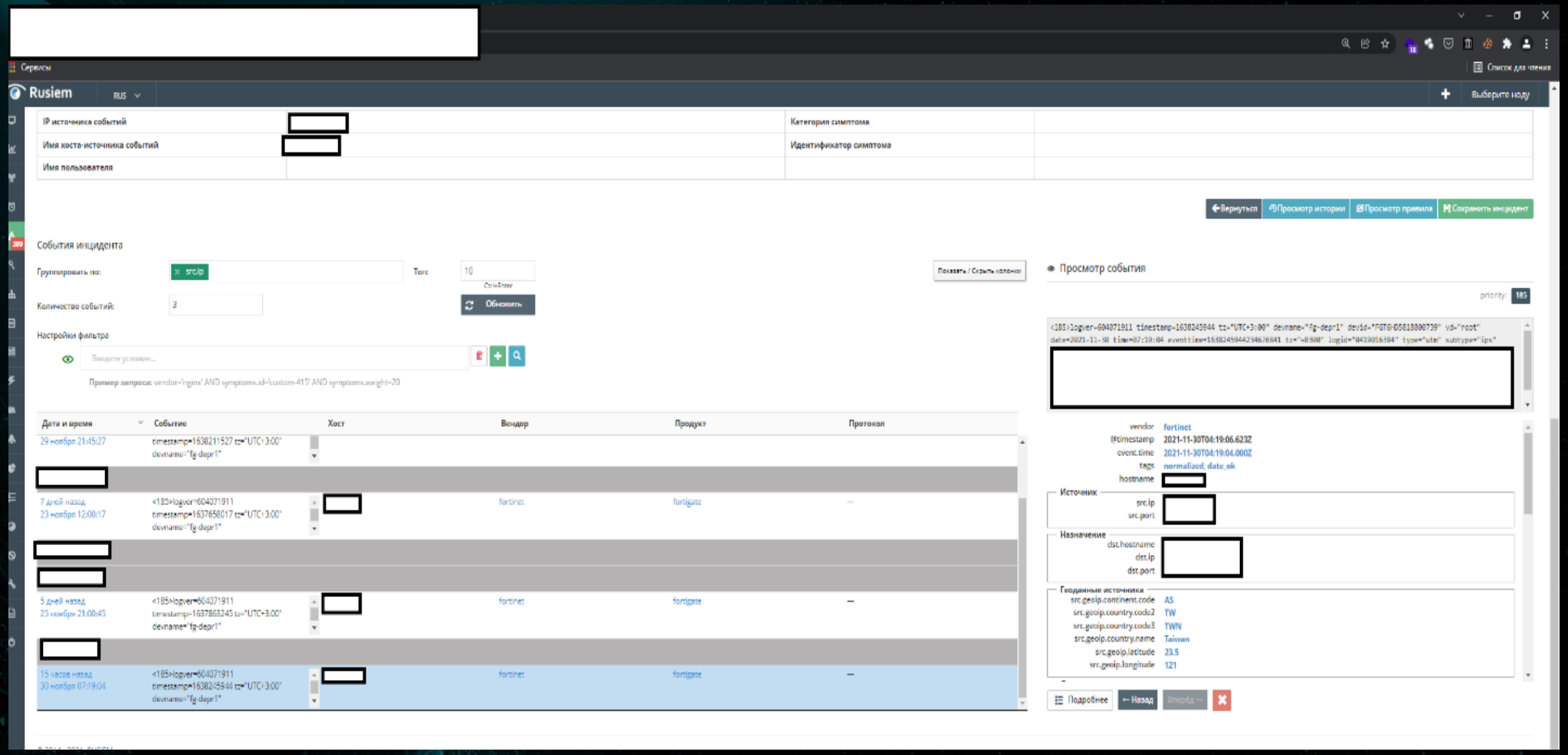
RUSIEM
Всё под контролем

Мониторинг продолжительного брутфорса

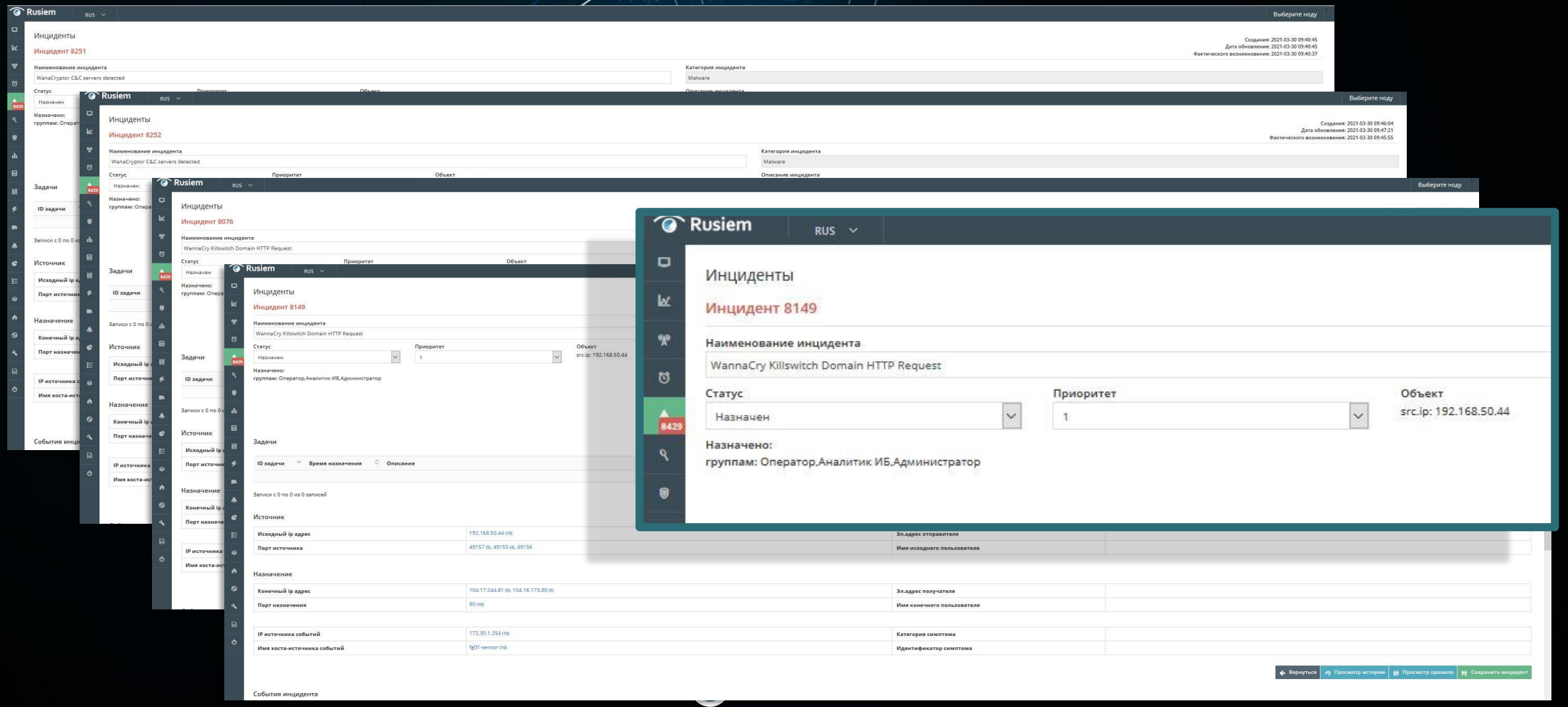
При условии *30* неуспешных попыток входа в течение *900* секунд

ID	Наименование	Категория	Приоритет	Статус	Назначен	Исполнитель	Объект	Mitre ID	Количество событий	Дата создания	Дата изменения	
21747	Брутофорс owa (agressive)	[redacted]	1	Назначен	Группы: Оператор, Аналитик ИБ, Аналитик ИТ, Аудитор, Администратор Пользователи: admin	Группы: Оператор, Аналитик ИБ, Аналитик ИТ, Аудитор, Администратор Пользователи: admin	user.name: src.ip:		30	2022-01-19 12:19:59	2022-01-19 12:19:59	
21714	Брутофорс owa (agressive)	[redacted]	1	Назначен	Группы: Оператор, Аналитик ИБ, Аналитик ИТ, Аудитор, Администратор Пользователи: admin	Группы: Оператор, Аналитик ИБ, Аналитик ИТ, Аудитор, Администратор Пользователи: admin	user.name: src.ip:		31	2022-01-17 11:10:04	2022-01-17 11:10:04	
21702	Брутофорс owa (agressive)	[redacted]	1	Назначен	Группы: Оператор, Аналитик ИБ, Аналитик ИТ, Аудитор, Администратор Пользователи: admin	Группы: Оператор, Аналитик ИБ, Аналитик ИТ, Аудитор, Администратор Пользователи: admin	user.name: src.ip:		3517	2022-01-16 15:14:58	2022-01-19 14:23:58	
21701	Брутофорс owa (agressive)	[redacted]	1	Назначен	Группы: Оператор, Аналитик ИБ, Аналитик ИТ, Аудитор, Администратор Пользователи: admin	Группы: Оператор, Аналитик ИБ, Аналитик ИТ, Аудитор, Администратор Пользователи: admin	user.name: src.ip:		538	2022-01-16 11:28:04	2022-01-18 13:40:31	
21698	Брутофорс owa (agressive)	[redacted]	1	Назначен	Группы: Оператор, Аналитик ИБ, Аналитик ИТ, Аудитор, Администратор Пользователи: admin	Группы: Оператор, Аналитик ИБ, Аналитик ИТ, Аудитор, Администратор Пользователи: admin	user.name: src.ip:		44	2022-01-15 16:35:53	2022-01-15 16:36:23	

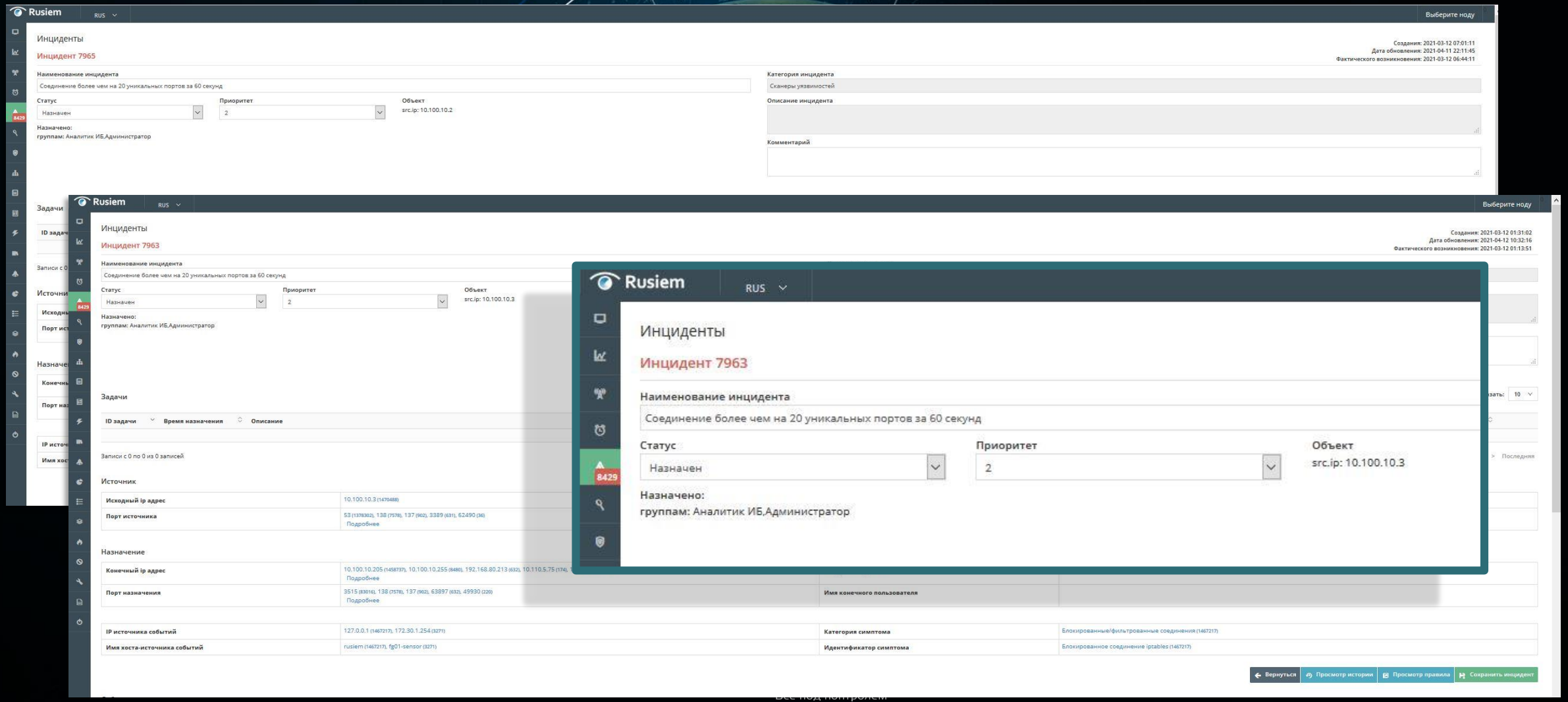
С IP-адреса xx.xx.xx.xx шла вредоносная активность, связанная с зловредом Moon malware



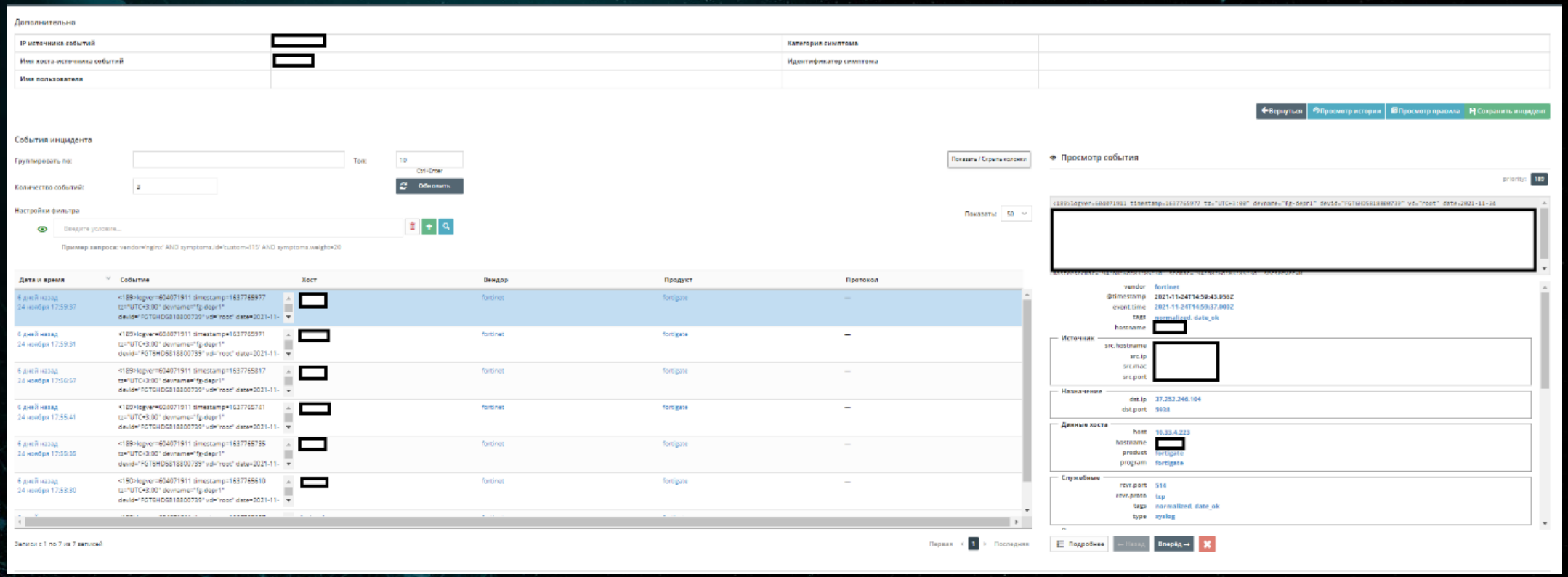
WannaCryptor



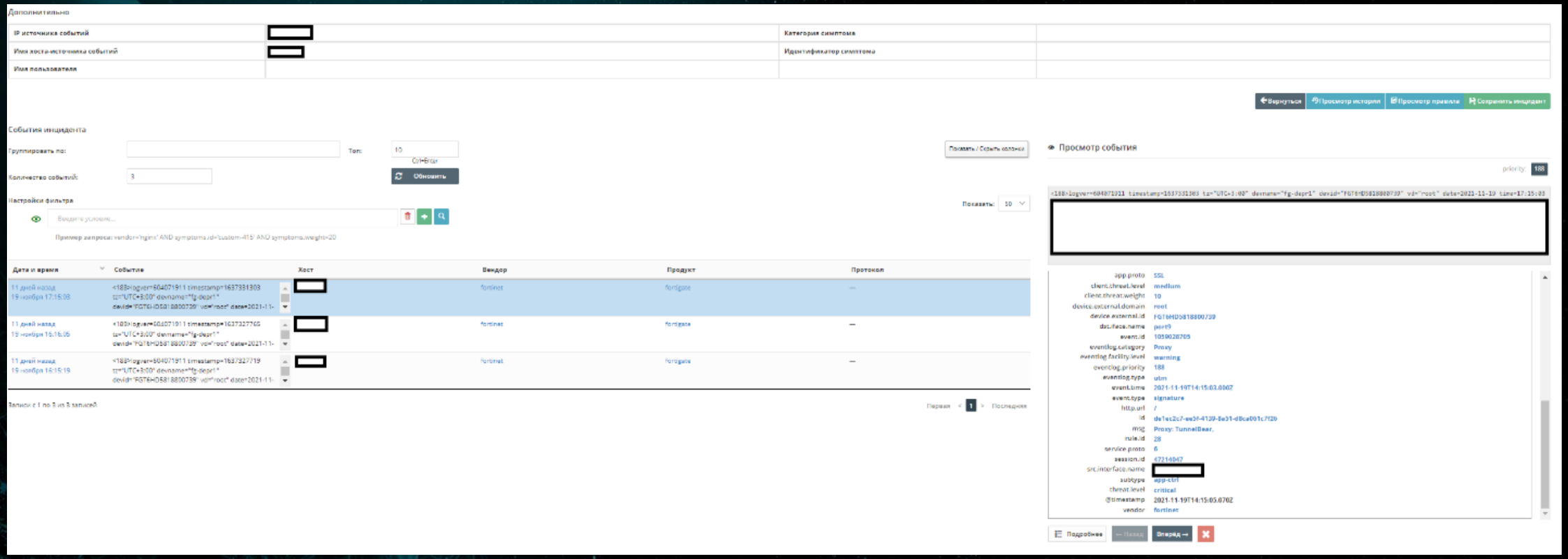
Сканеры уязвимостей



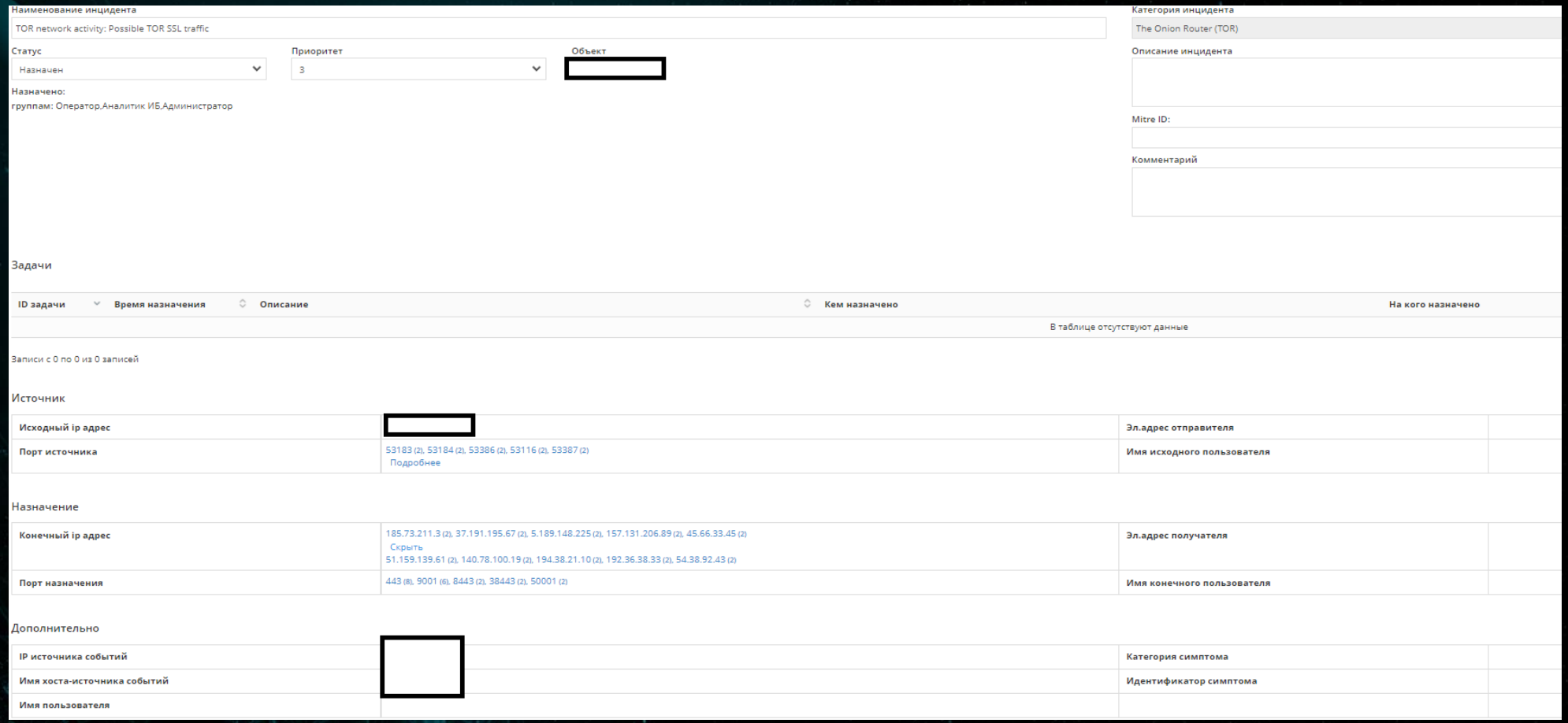
С адреса xx.xx.xx.xx выявлена активность, связанная со средствами удаленного доступа, в частности, TeamViewer



Замечено использование средств анонимизации трафика Tunnelbear VPN для подключения к серверу в Китае, что нетипично для средств VPN



Активность в сети TOR из локальной сети может свидетельствовать о заражении сети



Наименование инцидента

TOR network activity: Possible TOR SSL traffic

Категория инцидента: The Onion Router (TOR)

Статус: Назначен

Приоритет: 3

Объект: [redacted]

Описание инцидента

Назначено:
группам: Оператор,Аналитик ИБ,Администратор

Mitre ID:

Комментарий

Задачи

ID задачи	Время назначения	Описание	Кем назначено	На кого назначено
			В таблице отсутствуют данные	

Записи с 0 по 0 из 0 записей

Источник

Исходный ip адрес	[redacted]	Эл.адрес отправителя	
Порт источника	53183 (2), 53184 (2), 53386 (2), 53116 (2), 53387 (2) Подробнее	Имя исходного пользователя	

Назначение

Конечный ip адрес	185.73.211.3 (2), 37.191.195.67 (2), 5.189.148.225 (2), 157.131.206.89 (2), 45.66.33.45 (2) Скрыть 51.159.139.61 (2), 140.78.100.19 (2), 194.38.21.10 (2), 192.36.38.33 (2), 54.38.92.43 (2)	Эл.адрес получателя	
Порт назначения	443 (8), 9001 (6), 8443 (2), 38443 (2), 50001 (2)	Имя конечного пользователя	

Дополнительно

IP источника событий	[redacted]	Категория симптома	
Имя хоста-источника событий		Идентификатор симптома	
Имя пользователя			

На хосте xx.xx.xx.xx было замечено использование TOR

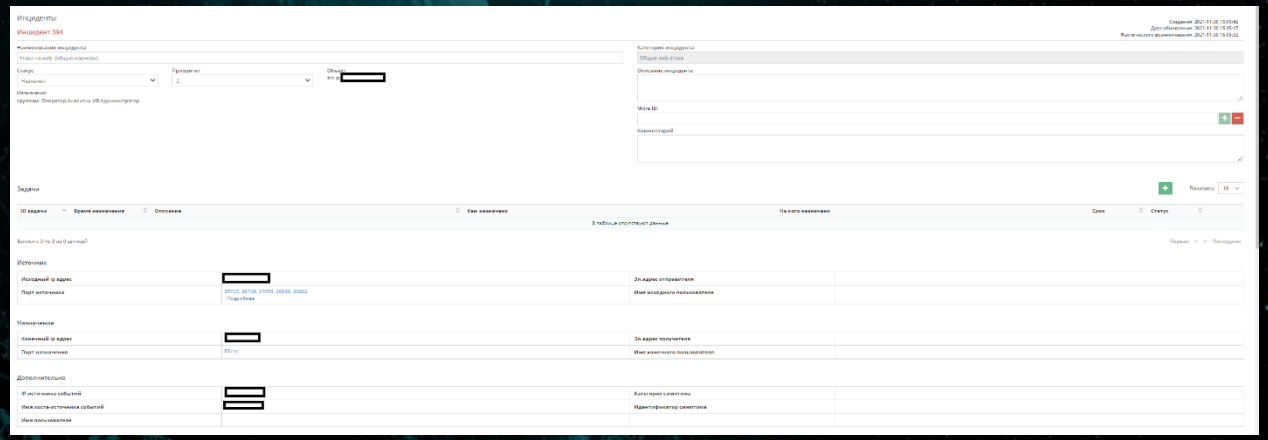
RUSIEM
Всё под контролем

Корреляция

В системе из коробки доступна корреляция, позволяющая отлавливать атаки на web-сайты

321	Атака на web (общие маркеры)	Общие web атаки	2	Назначен	Группы: Администратор, Аналитик ИБ, Оператор	Группы: Администратор, Аналитик ИБ, Оператор	src.ip: [redacted]
394	Атака на web (общие маркеры)	Общие web атаки	2	Назначен	Группы: Администратор, Аналитик ИБ, Оператор	Группы: Администратор, Аналитик ИБ, Оператор	src.ip: [redacted]

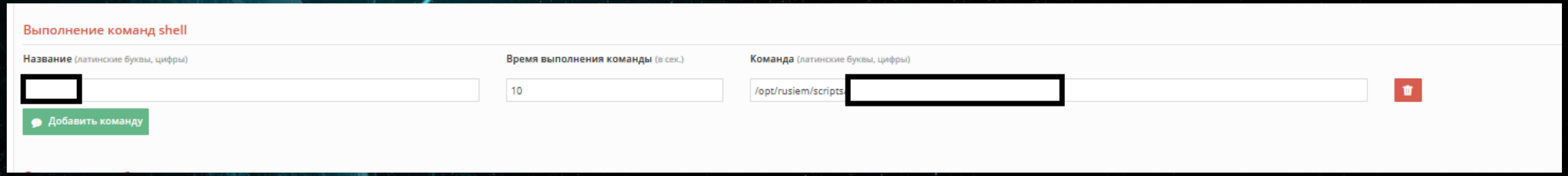
Система отработала, появился инцидент о том, что в данный момент идет атака на web-сайт предприятия



RUSIEM
Всё под контролем

Возможности RuSIEM

В SIEM-системе RuSIEM предусмотрена возможность запуска произвольного скрипта при срабатывании корреляции



Создание правила корреляции

ID	Наименование	Категория	Приоритет	Статус	Назначен	Исполнитель	Объект	Mitre ID	Количество событий	Дата создания	Дата изменения	
21760	Брутофорс owa	[redacted]	1	Назначен	Группы: Оператор, Аналитик ИБ, Аналитик ИТ, Аудитор, Администратор Пользователи: admin	Группы: Оператор, Аналитик ИБ, Аналитик ИТ, Аудитор, Администратор Пользователи: admin	user.name: src.ip: [redacted]		6	2022-01-19 17:24:49	2022-01-19 17:24:49	
21759	Брутофорс owa	[redacted]	1	Назначен	Группы: Оператор, Аналитик ИБ, Аналитик ИТ, Аудитор, Администратор Пользователи: admin	Группы: Оператор, Аналитик ИБ, Аналитик ИТ, Аудитор, Администратор Пользователи: admin	user.name: [redacted] src.ip: [redacted]		14	2022-01-19 15:55:34	2022-01-19 16:12:05	
21758	Брутофорс owa	[redacted]	1	Назначен	Группы: Оператор, Аналитик ИБ, Аналитик ИТ, Аудитор, Администратор Пользователи: admin	Группы: Оператор, Аналитик ИБ, Аналитик ИТ, Аудитор, Администратор Пользователи: admin	user.name: [redacted] src.ip: [redacted]		8	2022-01-19 15:23:32	2022-01-19 15:23:32	
21757	Брутофорс owa	[redacted]	1	Назначен	Группы: Оператор, Аналитик ИБ, Аналитик ИТ, Аудитор, Администратор Пользователи: admin	Группы: Оператор, Аналитик ИБ, Аналитик ИТ, Аудитор, Администратор Пользователи: admin	user.name: [redacted] src.ip: [redacted]		43	2022-01-19 15:22:32	2022-01-19 17:23:49	
21756	Брутофорс owa	[redacted]	1	Назначен	Группы: Оператор, Аналитик ИБ, Аналитик ИТ, Аудитор, Администратор Пользователи: admin	Группы: Оператор, Аналитик ИБ, Аналитик ИТ, Аудитор, Администратор Пользователи: admin	user.name: [redacted] src.ip: [redacted]		19	2022-01-19 15:18:02	2022-01-19 15:18:02	

RUSIEM
Всё под контролем


Как мы работаем

Работа через партнёрский канал

Вендор

- Помощь в пресейле
- Помощь во внедрении
- Обучение по продукту
- Тех. поддержка

Дистрибьютор

- Документооборот по проектам
- Логистика ПО
- Логистика оборудования
- Маркетинговая поддержка
- Финансовая поддержка

Партнёр

- Подбор решения под задачи
- Пресейл проекта
- Пилотирование решения
- Продажа решения
- Внедрение решения
- 1-я линия тех. поддержки

Заказчик

- Определение целей и задач
- Выделение ресурсов
- Тестирование решения
- Обратная связь по пилоту
- Бюджетирование решения

RUSIEM
Всё под контролем

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
...

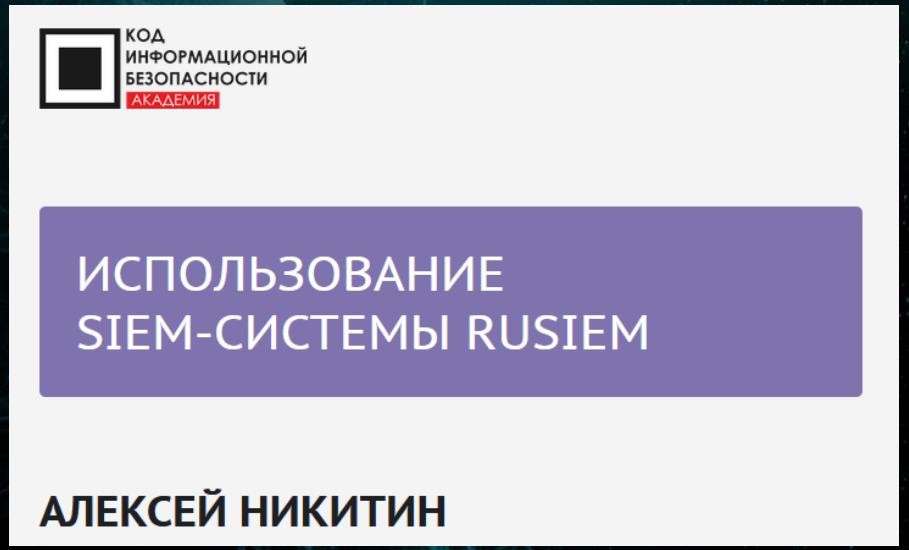
RUSIEM
Всё под контролем

Поддержка

На всех этапах проекта Партнёров и Заказчиков

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

Официальные курсы в АИС

После прохождения курсов также предоставляются свидетельства гос. образца

АИС
АКАДЕМИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

Эксплуатация системы мониторинга, сбора и анализа событий RuSIEM
1 день – 8 ак. часов

Внедрение и развертывание системы мониторинга, сбора и анализа событий RuSIEM
2 дня – 16 ак. часов

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!

Чеботарев Дмитрий
d.chebotarev@rusiem.com
+7(916) 824-65-00