



**RUSIEM**

Всё под контролем

# ***RuSIEM: поддерживаем организации в сложной ситуации***

***Чеботарев Дмитрий,  
Менеджер по техническому сопровождению продаж***

# Актуальные кибератаки

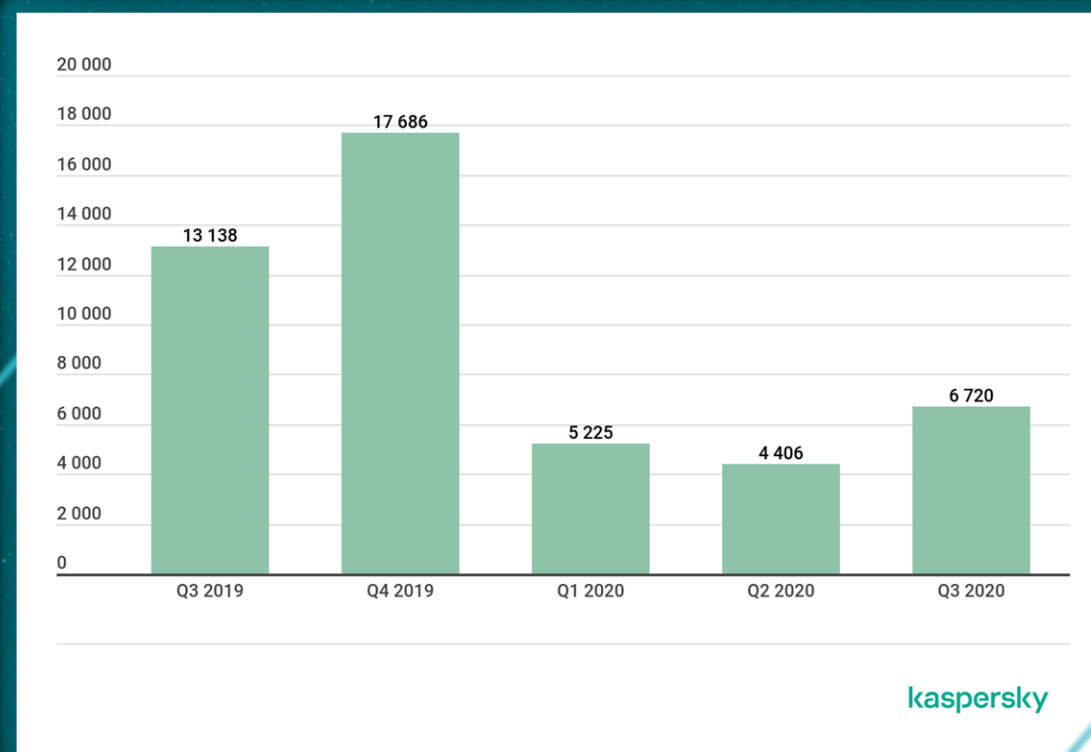
## 1,5 млрд

отраженных кибератак пришлось  
на Q3 2020 г.

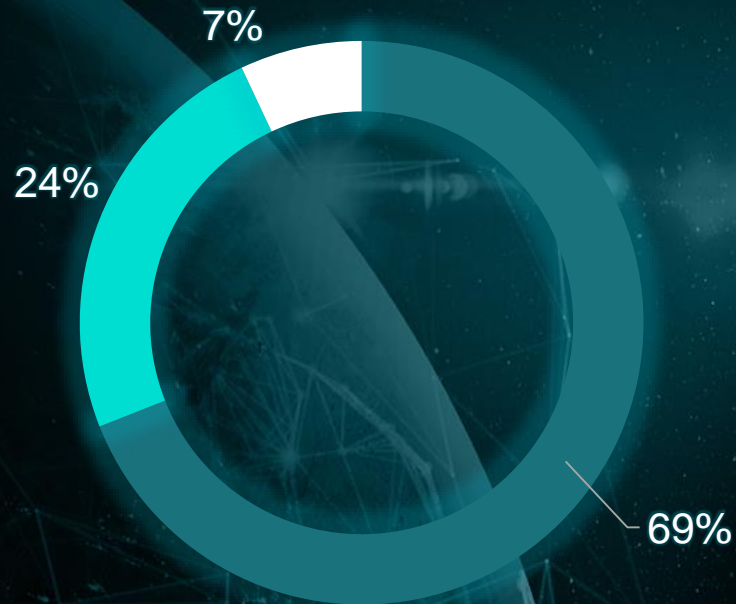
## 2 из 3

кибератак Q3 2020 г. использовали  
уязвимости Microsoft Office

Количество модификаций шифровальщиков



# 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

# 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

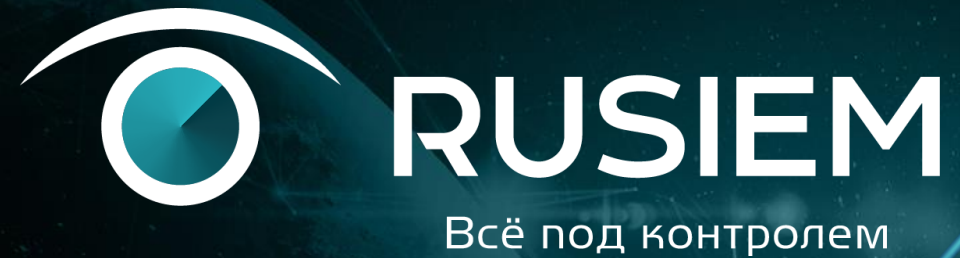


- Access Control, Authentication
- DLP-системы
- IDS/IPS-системы
- Антивирусные приложения

- 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



*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*

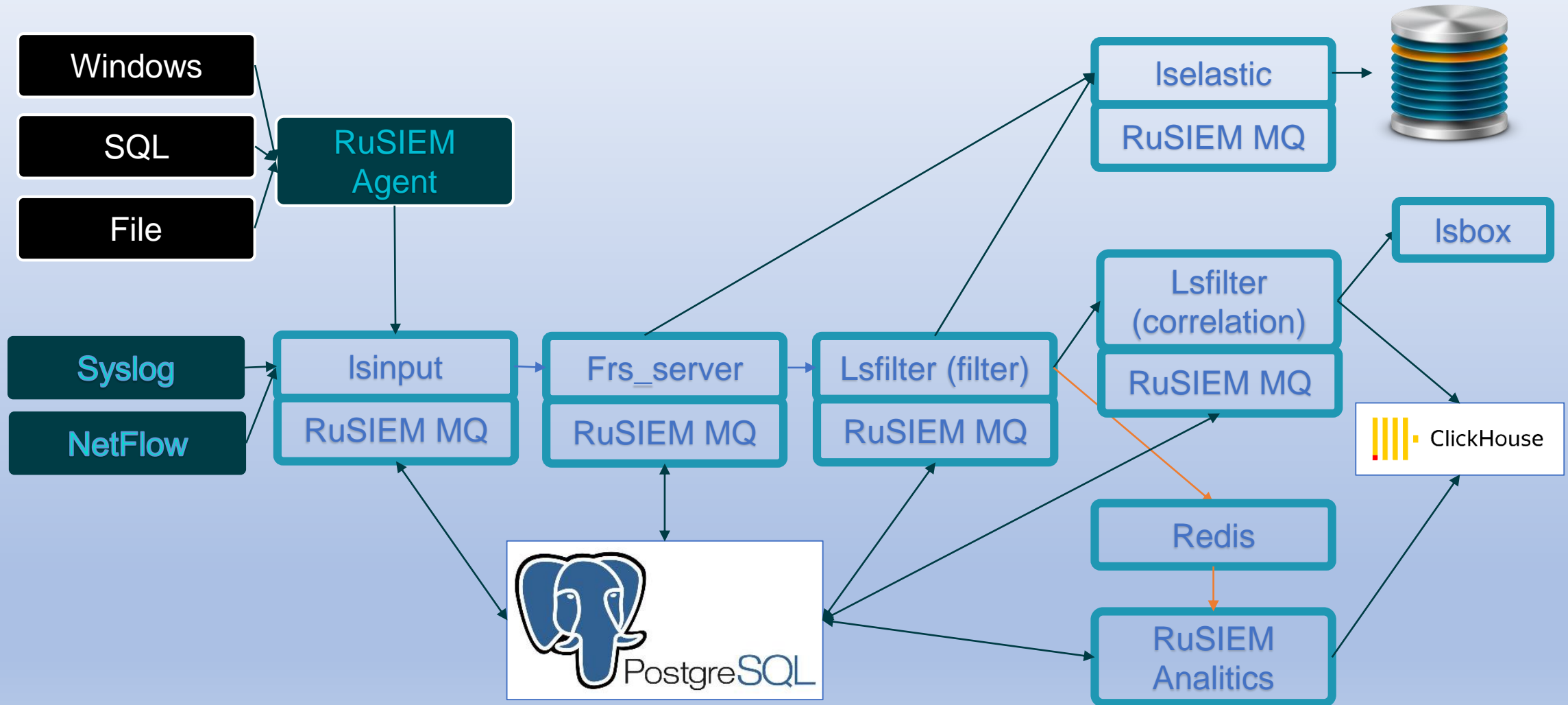


***RuSIEM***  
– коммерческая версия класса *SIEM*



***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





# Case story

История одной атаки

# 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	Брутфорс owa (aggressive)		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]		30	2022-01-19 12:19:59	2022-01-19 12:19:59		<input type="checkbox"/>
21714	Брутфорс owa (aggressive)		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]		31	2022-01-17 11:10:04	2022-01-17 11:10:04		<input type="checkbox"/>
21702	Брутфорс owa (aggressive)		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]		3517	2022-01-16 15:14:58	2022-01-19 14:23:58		<input type="checkbox"/>
21701	Брутфорс owa (aggressive)		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]		538	2022-01-16 11:28:04	2022-01-18 13:40:31		<input type="checkbox"/>
21698	Брутфорс owa (aggressive)		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]		44	2022-01-15 16:35:53	2022-01-15 16:36:23		<input type="checkbox"/>

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

The screenshot displays the Rusiem security dashboard interface. At the top, there are search filters for 'IP источника событий', 'Имя хоста-источника событий', and 'Имя пользователя'. Below this is a table with columns for 'Дата и время', 'Событие', 'Хост', 'Вендор', 'Продукт', and 'Протокол'. The table lists several events from November 29, 23, and 25, all originating from the same IP address and identified as 'Moon' malware. A detailed view of an event is shown on the right, including fields for 'Источник' (src.ip, src.port) and 'Назначение' (dst.hostname, dst.ip, dst.port). The event details also show a JSON log entry and geographical information for the source IP.

Дата и время	Событие	Хост	Вендор	Продукт	Протокол
29 ноября 21:45:27	timestamp=1638211527 tz="UTC+3:00" devname="fg-dep1"	[redacted]			
7 дней назад 23 ноября 12:08:17	<185>logver=604071911 timestamp=1637856017 tz="UTC+3:00" devname="fg-dep1"	[redacted]	fortinet	fortigate	-
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
5 дней назад 25 ноября 21:08:45	<185>logver=604071911 timestamp=1637863245 tz="UTC+3:00" devname="fg-dep1"	[redacted]	fortinet	fortigate	-
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
15 часов назад 30 ноября 07:19:04	<185>logver=604071911 timestamp=1638245944 tz="UTC+3:00" devname="fg-dep1"	[redacted]	fortinet	fortigate	-

**Просмотр события**

```
<185>logver=604071911 timestamp=1638245944 tz="UTC+3:00" devname="fg-dep1" devid="FGT0-05018090739" vid="root" data=2021-11-30 11:04 eventtime=1638245944.754876941 tz="+8:00" logid="16430016184" type="uta" subtype="ips"
```

Источник: src.ip [redacted], src.port [redacted]

Назначение: dst.hostname [redacted], dst.ip [redacted], dst.port [redacted]

Географические координаты источника: src.geolip.continent.code AS, src.geolip.country.code2 TW, src.geolip.country.code3 TWN, src.geolip.country.name Taiwan, src.geolip.latitude 23.5, src.geolip.longitude 121

# WannaCryptor



The image displays the Rusiem security management interface, showing multiple overlapping windows for incident details. The primary window in the foreground is for Incident 8149, titled "WannaCry Killswitch Domain HTTP Request".

**Incident 8149 Details:**

- Наименование инцидента:** WannaCry Killswitch Domain HTTP Request
- Статус:** Назначен
- Приоритет:** 1
- Объект:** src.ip: 192.168.50.44
- Назначено:** группам: Оператор, Аналитик ИБ, Администратор

**Источники (Sources):**

Исходный IP адрес	Эл. адрес отправителя
192.168.50.44 (ip)	
Порт источника	Имя исходного пользователя
49157 (ip), 49155 (ip), 49156	

**Назначение (Destination):**

Конечный IP адрес	Эл. адрес получателя
104.17.244.81 (ip), 104.16.173.80 (ip)	
Порт назначения	Имя конечного пользователя
80 (ip)	

**Источники событий (Event Sources):**

IP источника событий	Категория симптома
172.30.1.254 (ip)	
Имя хоста-источника событий	Идентификатор симптома
ip01-zenlog (ip)	

At the bottom of the interface, there are navigation buttons: "Вернуться", "Просмотр истории", "Просмотр правил", and "Сохранить инцидент".

Всё под контролем

# Сканеры уязвимостей

**Русиём** | RUС | Выберите ноду

### Инциденты

#### Инцидент 7965

Наименование инцидента: Соединение более чем на 20 уникальных портов за 60 секунд

Статус: Назначен | Приоритет: 2 | Объект: src.ip: 10.100.10.2

Назначено: группам: Аналитик ИБ,Администратор

Создание: 2021-03-12 07:01:11  
Дата обновления: 2021-04-11 22:11:45  
Фактического возникновения: 2021-03-12 06:44:11

Категория инцидента: Сканеры уязвимостей

Описание инцидента

Комментарий

---

**Русиём** | RUС | Выберите ноду

### Инциденты

#### Инцидент 7963

Наименование инцидента: Соединение более чем на 20 уникальных портов за 60 секунд

Статус: Назначен | Приоритет: 2 | Объект: src.ip: 10.100.10.3

Назначено: группам: Аналитик ИБ,Администратор

Создание: 2021-03-12 01:31:02  
Дата обновления: 2021-04-12 10:32:16  
Фактического возникновения: 2021-03-12 01:13:51

Категория инцидента: Сканеры уязвимостей

Описание инцидента

Комментарий

**Задачи**

ID задачи	Время назначения	Описание
Записи с 0 по 0 из 0 записей		

**Источник**

Исходный IP адрес	10.100.10.3 (1470488) <a href="#">Подробнее</a>
Порт источника	53 (1378902), 138 (7578), 137 (902), 3389 (831), 62490 (86) <a href="#">Подробнее</a>

**Назначение**

Конечный IP адрес	10.100.10.205 (1458737), 10.100.10.255 (8480), 192.168.80.213 (832), 10.110.5.75 (174) <a href="#">Подробнее</a>
Порт назначения	3515 (83016), 138 (7578), 137 (902), 63897 (832), 45930 (226) <a href="#">Подробнее</a>
Имя конечного пользователя	

**IP источника событий**: 127.0.0.1 (1467217), 172.30.1.254 (8271)

**Имя хоста-источника событий**: rusiem (1467217), ip01-sensor (8271)

**Категория симптома**: Блокирование/фильтрованные соединения (1467217)

**Идентификатор симптома**: Блокированное соединение iptables (1467217)

← Вернуться | Просмотр истории | Просмотр правил | Сохранить инцидент

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

Дополнительно

IP источника событий	<input type="text"/>	Категория симптома	
Имя хоста-источника событий	<input type="text"/>	Идентификатор симптома	
Имя пользователя	<input type="text"/>		

← Вернуться → Просмотр истории 📄 Просмотр правил 📄 Сохранить инцидент

События инцидента

Группировать по:  Тип:

Количество событий:

Настройки фильтра

Пример запроса: vendor=fortinet AND xumptoma.id=custom:112 AND xumptoma.wgfw=20

Просмотр событий

Показаны: 50

Дата и время	События	Хост	Вендор	Продукт	Протокол
6 дней назад 24 ноября 17:59:37	<189>logver=604071911 timestamp=1637765977 ts="UTC+3:00" @hostname="fg.dnsr1" devId="FGT6HD9818800739" xid="root" date=2021-11-	<input type="text"/>	fortinet	fortigate	---
6 дней назад 24 ноября 17:59:31	<189>logver=604071911 timestamp=1637765971 ts="UTC+3:00" @hostname="fg.dnsr1" devId="FGT6HD9818800739" xid="root" date=2021-11-	<input type="text"/>	fortinet	fortigate	---
6 дней назад 24 ноября 17:59:57	<189>logver=604071911 timestamp=1637765917 ts="UTC+3:00" @hostname="fg.dnsr1" devId="FGT6HD9818800739" xid="root" date=2021-11-	<input type="text"/>	fortinet	fortigate	---
6 дней назад 24 ноября 17:55:41	<189>logver=604071911 timestamp=1637765761 ts="UTC+3:00" @hostname="fg.dnsr1" devId="FGT6HD9818800739" xid="root" date=2021-11-	<input type="text"/>	fortinet	fortigate	---
6 дней назад 24 ноября 17:59:30	<189>logver=604071911 timestamp=1637765735 ts="UTC+3:00" @hostname="fg.dnsr1" devId="FGT6HD9818800739" xid="root" date=2021-11-	<input type="text"/>	fortinet	fortigate	---
6 дней назад 24 ноября 17:53:30	<189>logver=604071911 timestamp=1637765510 ts="UTC+3:00" @hostname="fg.dnsr1" devId="FGT6HD9818800739" xid="root" date=2021-11-	<input type="text"/>	fortinet	fortigate	---

Записи с 1 по 7 из 7 записей

Первая 1 Последняя

Источники

```
<189>logver=604071911 timestamp=1637765977 ts="UTC+3:00" @hostname="fg.dnsr1" devId="FGT6HD9818800739" xid="root" date=2021-11-24
```

vendor: fortinet  
@timestamp: 2021-11-24T14:59:43.999Z  
event.type: 2021-11-24T14:59:37.009Z  
type: normalized\_date\_ssk  
hostname:

Источники

src.hostname:   
src.ip:   
src.mac:   
src.port:

Назначение

dst.ip: 37.252.246.104  
dst.port: 9938

Данные хоста

host: 10.35.4.223  
hostname:   
product: fortigate  
program: fortigate

Службы

host.port: 916  
host.proto: tcp  
tags: normalized\_date\_ssk  
type: syslog

🔍 Подробнее ⏪ Назад ⏩ Перед 🗑

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

Детали инцидента

ID источника событий	[REDACTED]	Категория симптома	
Имя хоста-источника событий	[REDACTED]	Идентификатор симптома	
Имя пользователя			

События инцидента

Группировать по:  Тип:

Количество событий:

Настройки фильтра

Введите условия...

Пример запроса: vendor="h3mit" AND symptoms.id="custom-415" AND symptoms.weight>20

Показать / Скрыть детали

Просмотр события

priority: 188

```
<188>logver=60407211 timestamp=1637331308 src="UTC+8:00" devname="fg-degr1" devid="FG1610581800739" vsh="root" date=2021-11-19 17:15:08
```

Дата и время	Событие	Хост	Вендор	Продукт	Протокол
11 дней назад 19 ноября 17:15:08	<188>logver=604071911 timestamp=1637331308 src="UTC+8:00" devname="fg-degr1" devid="FG1610581800739" vsh="root" date=2021-11-19 17:15:08	[REDACTED]	fortinet	fortigate	—
11 дней назад 19 ноября 15:16:06	<100>logver=604071911 timestamp=1637327765 src="UTC+8:00" devname="fg-degr1" devid="FG1610581800739" vsh="root" date=2021-11-19 15:16:06	[REDACTED]	fortinet	fortigate	—
11 дней назад 19 ноября 16:15:19	<188>logver=604071911 timestamp=1637327719 src="UTC+8:00" devname="fg-degr1" devid="FG1610581800739" vsh="root" date=2021-11-19 16:15:19	[REDACTED]	fortinet	fortigate	—

Всего: 1 из 3 из 3 записей

Первый    Последний

app.proto: SSL  
client.threat.level: medium  
client.threat.weight: 10  
device.external.domain: root  
device.external.id: FG1610581800739  
dev.name: pwr9  
event.id: 1059628705  
eventlog.category: Proxy  
eventlog.facility.level: warning  
eventlog.priority: 188  
eventlog.type: utm  
event.time: 2021-11-19T14:15:03.000Z  
event.type: signature  
http.url: /  
id: de1ec2c7-ee3f-4139-8e31-d8ca091c7f2b  
msg: Proxy: TunnelBear.  
rule.id: 28  
service.proto: 8  
session.id: 47314867  
src.interface.name: [REDACTED]  
subtype: app-ssl  
threat.level: critical  
@timestamp: 2021-11-19T14:15:03.070Z  
vendor: fortinet

Подробности

# 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 <input type="text"/>
Назначено: группам: Оператор, Аналитик ИБ, Администратор		Описание инцидента <input type="text"/>
		Mitre ID: <input type="text"/>
		Комментарий <input type="text"/>
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	<input type="text"/>	Эл. адрес отправителя
Порт источника	53183 (2), 53184 (2), 53386 (2), 53116 (2), 53387 (2) <a href="#">Подробнее</a>	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) <a href="#">Скрыть</a> 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	<input type="text"/>	Категория симптома
Имя хоста-источника событий	<input type="text"/>	Идентификатор симптома
Имя пользователя		

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



# 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

The screenshot displays the RUSIEM incident management system interface. At the top, it shows the incident ID '394' and its status as 'Активен' (Active). The incident is categorized as 'Атака на web (общие маркеры)' (Web attack (general markers)). The interface includes a search bar, a list of tasks, and a detailed view of the incident. The detailed view shows the source IP address as '[REDACTED]' and the target as '192.168.1.100'. The incident is assigned to the 'Администратор, Аналитик ИБ, Оператор' groups. The interface also shows a list of related incidents and a detailed view of the incident's history.


# Возможности RuSIEM

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

**Выполнение команд shell**

Название (латинские буквы, цифры)	Время выполнения команды (в сек.)	Команда (латинские буквы, цифры)	
<input type="text"/>	<input type="text" value="10"/>	<input type="text" value="/opt/rusiem/scripts/"/> <input type="text"/>	<input type="button" value="🗑"/>

# Создание правила корреляции

ID	Наименование	Категория	Приоритет	Статус	Назначен	Исполнитель	Объект	Mitre ID	Количество событий	Дата создания	Дата изменения		
21760	Брутофорс owa	<input type="checkbox"/>	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]		6	2022-01-19 17:24:49	2022-01-19 17:24:49	   	<input type="checkbox"/>
21759	Брутофорс owa	<input type="checkbox"/>	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	   	<input type="checkbox"/>
21758	Брутофорс owa	<input type="checkbox"/>	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	   	<input type="checkbox"/>
21757	Брутофорс owa	<input type="checkbox"/>	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	   	<input type="checkbox"/>
21756	Брутофорс owa	<input type="checkbox"/>	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	   	<input type="checkbox"/>

# 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



# 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

...

# Поддержка

*На всех этапах проекта  
Партнёров и Заказчиков*

КАМ под  
проект

Pre-Sale под  
проект



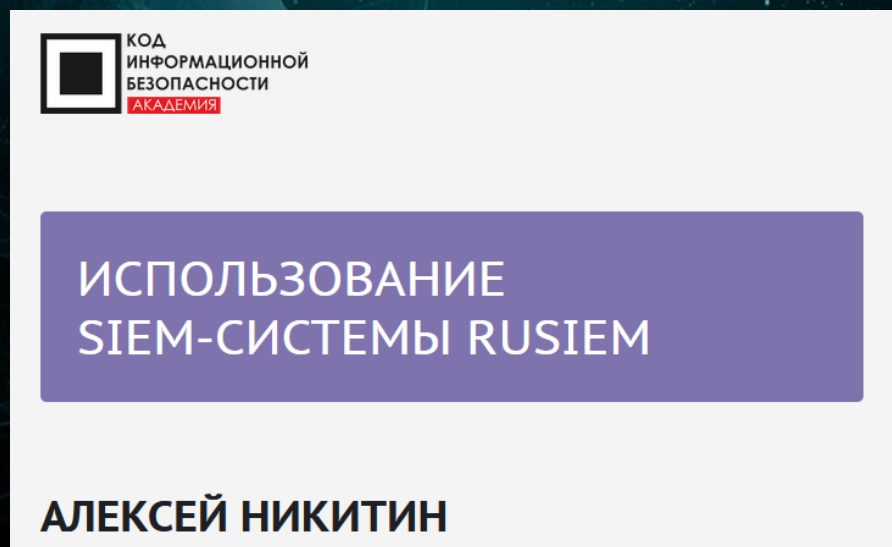
RUSIEM

Поддержка с  
внедрением

Совместные  
активности

# 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





# Официальные курсы в АИС

*После прохождения курсов  
также предоставляются  
свидетельства гос. образца*



**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**



# Telegram-каналы RuSIEM

<https://t.me/rusiem> -

последние новости, важные события

<https://t.me/rusiemsupport> -

возможность быстро связаться с  
технической поддержкой

**Спасибо за внимание!**

 **Чеботарев Дмитрий**  
 **[d.chebotarev@rusiem.com](mailto:d.chebotarev@rusiem.com)**  
 **+7(916) 824-65-00**

