



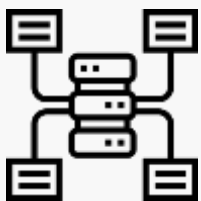
ПАНГЕО
РАДАР

Платформа Радар

Ключевое звено эффективного SOC

ПЛАТФОРМА РАДАР

НОВЫЙ ПРОГРАММНЫЙ ПРОДУКТ ДЛЯ АВТОМАТИЗАЦИИ РАБОТЫ SOC



Интеллектуальная группировка инцидентов

Схожие инциденты группируются в одну сущность, аналитик не тратит время на ненужную работу.



Масштабирование производительности

Платформа является модульной, горизонтально масштабируется под требуемый поток событий и размер инфраструктуры



Гибкий язык написания правил корреляции

Удобный интерфейс для разработки правил;
Язык базируется на Python, сохраняя его гибкость и возможности

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

1

**В ЕДИНОМ РЕЕСТРЕ
РОССИЙСКИХ ПРОГРАММ
ДЛЯ ЭВМ (№ 4791)**

3

**СООТВЕТСТВИЕ
ПРИКАЗУ ФСБ №196**

2

**ИСКЛЮЧИТЕЛЬНЫЕ ПРАВА
ПРИНАДЛЕЖАТ
РОССИЙСКОЙ КОМПАНИИ
– ЛИЦЕНЗИАТУ ФСТЭК**

4

**СЕРТИФИКАТ
ФСТЭК ***

Финальная стадия получения.
Решение ФСТЭК о проведении сертификации
от 26.03.2019

ИНТЕГРАЦИИ С РОССИЙСКИМИ СИСТЕМАМИ



ВЗАИМОДЕЙСТВИЕ С ГОССОПКА

Обеспечение непрерывного взаимодействия и передача инцидентов



ИНТЕГРАЦИЯ СО СРЕДСТВАМИ ЗАЩИТЫ ИНФОРМАЦИИ

Получение событий безопасности, корреляция данных, выявление инцидентов, предоставление рекомендаций по минимизации риска



ИНТЕГРАЦИЯ СО СКАННЕРАМИ УЯЗВИМОСТЕЙ

Запуск задач, обработка результатов, приоритизация уязвимостей, предоставление рекомендаций по устранению

БАЗА ЗНАНИЙ



УЯЗВИМОСТИ



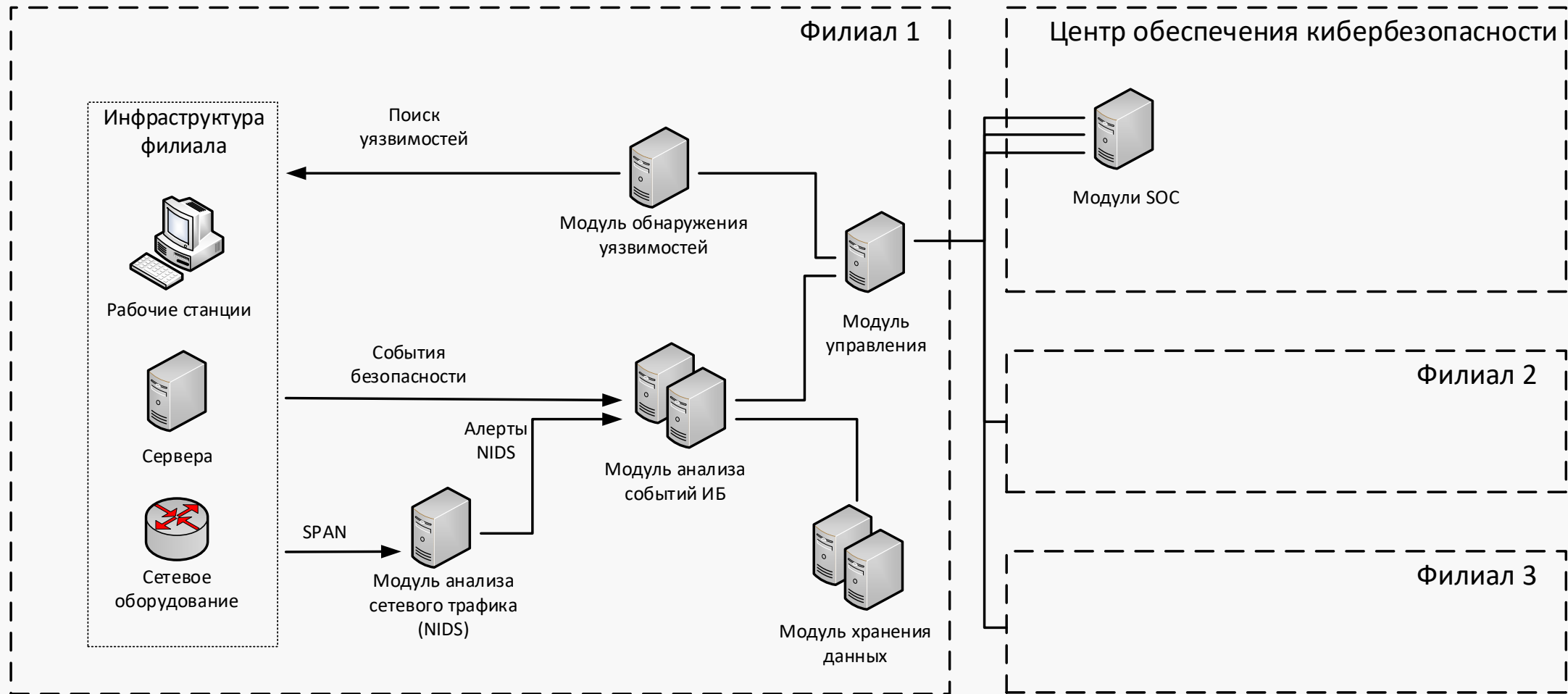
**НАРУШЕНИЯ
ПОЛИТИК**



**СЕТЕВЫЕ
АНОМАЛИИ**

Более 9 000 записей, база регулярно обновляется

АРХИТЕКТУРА РЕШЕНИЯ





**ПАНГЕО
РАДАР**

Спасибо за внимание!

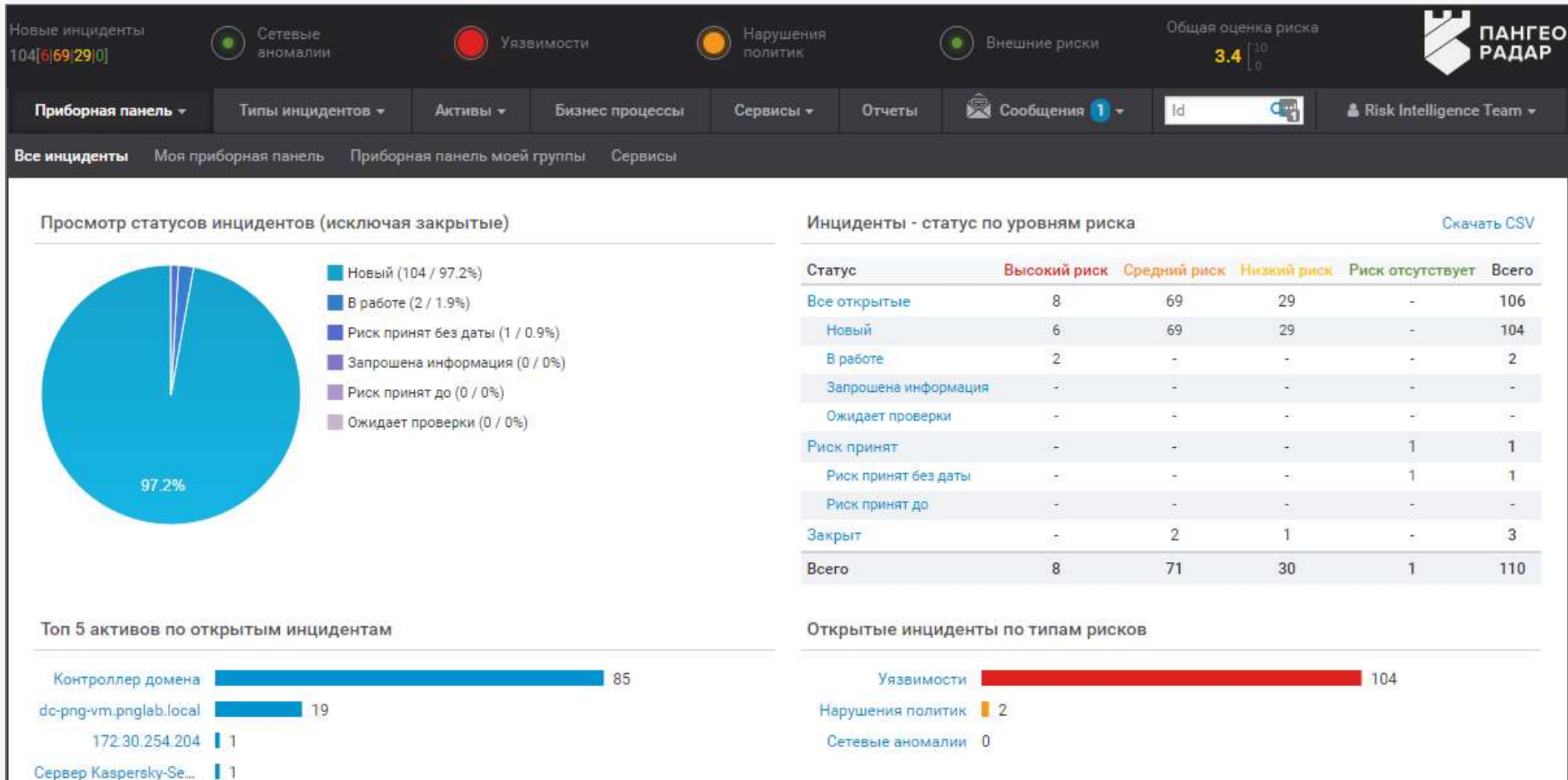
+7 (495) 252 03 00 | info@rangeoradar.ru | г. Москва. Краснопресненская наб.. 12



ПАНГЕО
РАДАР

ПРИЛОЖЕНИЯ | Интерфейсы системы

СВОДНАЯ ПРИБОРНАЯ ПАНЕЛЬ



УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

Типы инцидентов **Все инциденты** Мои инциденты Риск принят до Для переоценки + Новый инцидент

110 Все **Все открытые** 106 Новый 104 В работе 2 Запрошена информация 0 Ожидает проверки 0 Риск принят 1 3 Закрыт

Все типы Все уровни риска -- -- Время обработки

Все группы пользователей Все пользователи Все группы активов Все активы Расположение ак... Все

Открыт: От До Статус изменен: От До Последнее происшествие: От До

Поиск по: Id IP/Актив Примечание Поисковый запрос 20 Применить Сбросить

Тип	Id	Инциденты	Статус	Актив	Ответственный	Группа	Открыто	Статус изменен	Последнее происшествие
9.3	FIN9543-270	Debian DSA-4371-1 : apt - security update	Новый	Контролле...	Не задан	Группа Ана...	09.09.2019 0	09.09.2019 12:52	04.09.2019 13:47
9.3	FIN9581-286	Debian DSA-4497-1 : linux - security update	В работе	Контролле...	Risk Intelligenc...	Группа Ана...	09.09.2019 0	20.09.2019 15:32	04.09.2019 13:47
9.3	FIN9588-293	Debian DSA-4431-1 : libssh2 - security update	В работе	Контролле...	Risk Intelligenc...	Не задана	09.09.2019 0	20.09.2019 15:33	04.09.2019 13:47
9.3	FIN9594-300	Kibana ESA-2019-01, ESA-2019-02, ESA-2019-03	Новый	Контролле...	Не задан	Не задана	09.09.2019 0	09.09.2019 12:53	04.09.2019 13:47
9.0	FIN9546-269	Debian DSA-4368-1 : zeromq3 - security update	Новый	Контролле...	Не задан	Не задана	09.09.2019 0	09.09.2019 12:52	04.09.2019 13:47
9.0	FIN9574-279	Debian DSA-4350-1 : policykit-1 - security update	Новый	Контролле...	Не задан	Не задана	09.09.2019 0	09.09.2019 12:53	04.09.2019 13:47
8.7	FIN7779-252	KB4022715: Windows 10 Version 1607 and Wind...	Новый	dc-png-vm...	Не задан	Не задана	09.09.2019 0	09.09.2019 12:52	04.09.2019 13:40
8.1	FIN718-261	KB4343887: Windows 10 Version 1607 and Wind...	Новый	dc-png-vm...	Не задан	Не задана	09.09.2019 0	09.09.2019 12:52	04.09.2019 13:40
7.8	FIN7356-253	KB4025339: Windows 10 Version 1607 and Wind...	Новый	dc-png-vm...	Не задан	Не задана	09.09.2019 0	09.09.2019 12:52	04.09.2019 13:40
7.8	FIN8118-262	Debian DSA-4272-1 : linux - security update	Новый	Контролле...	Не задан	Не задана	09.09.2019 0	09.09.2019 12:52	04.09.2019 13:47

УПРАВЛЕНИЕ АКТИВАМИ

Приборная панель ▾ Типы инцидентов ▾ **Активы** ▾ Бизнес процессы Сервисы ▾ Отчеты Сообщения 1 ▾ Id C-1 Risk Intelligence Team ▾

Активы Сканирования на уязвимости История запросов на остановку сканирования

Все группы активов ▾ Все ▾ Все ▾ Расположение ▾ -- ▾

ОС IP/MAC/Актив Примечание актива Поисковый запрос 20 ▾ Поиск Сбросить

Актив	Тип	Расположение	Все открытые	Риск принят	Закрит	Операционная система	IP (MAC)	Последнее скан.
9.3 Контроллер домена	Host		85	-	2	Linux Kernel 4.9....	172.30.254.30 (52:54:00:f0:15:1a), 17...	04.09.2019 13:29
8.7 dc-png-vm.pnglab.local	Host		19	-	1	Microsoft Windows...	172.30.254.211 (52:54:00:fc:0b:b1)	04.09.2019 13:30
5.0 Сервер Kaspersky-Security C...			1	-	-	Microsoft Windows...	172.30.254.209 (52:54:00:7a:2f:ac)	-
5.0 172.30.254.204	Host		1	-	-		172.30.254.204 (н.д.)	-
0.0 10.10.10.10	Host		-	1	-		10.10.10.10 (н.д.)	-
172.30.254.254	Host		-	-	-	Cisco	172.30.254.254 (00:24:f7:91:c4:42)	21.01.2019 13:31
172.30.254.210	Host		-	-	-	Linux Kernel 4.8	172.30.254.210 (52:54:00:9d:3f:7d)	14.02.2019 12:57
pgrserver	Host	Москва	-	-	-			11.03.2019 13:22
Это Хост	Host	Москва	-	-	-	Linux Kernel 4.9....	172.30.254.208 (52:54:00:e5:c6:fa)	14.02.2019 12:57
dc02.pnglab.local	Server	Москва	-	-	-	Linux Kernel 4.9....	172.30.254.207 (52:54:00:52:c8:79)	11.03.2019 08:21
172.30.254.206	Host		-	-	-	Linux Kernel 4.9....	172.30.254.206 (52:54:00:9f:ed:99)	14.02.2019 12:57
172.30.254.205	Host		-	-	-	Linux Kernel 4.9....	172.30.254.205 (52:18:00:e7:18:c2)	11.03.2019 08:20
172.30.254.138	Host		-	-	-	FreeBSD 6.0, Free...	172.30.254.138 (54:26:96:dd:8e:e9)	14.02.2019 12:56
172.30.254.104	Host		-	-	-	FreeBSD 6.0, Free...	172.30.254.104 (dc:a9:04:99:f3:87)	11.03.2019 08:21

ИНТЕРФЕЙС АНАЛИТИКА

ПАНГЕО РАДАР ver. 2.0.3 Тактические Анализ **Наблюдатель** Панели Rulex

Analyze assets and loglines.

Активы & События

Выбранные активы

193.221.113.53

- microsoft
 - dns
 - dns_recursive_answer
 - 11 A DNS query was answered
 - dns_recursive_query
 - 11 A DNS query was raised
- 172.30.254.211 (DC-PNG-VM.pnglab.local)
- microsoft
 - dns
 - dns_answer
 - 9958 A DNS query was answered
 - dns_query
 - 10247 A DNS query was raised
 - dns_recursive_answer
 - 2243 A DNS query was answered
 - dns_recursive_query
 - 2247 A DNS query was raised

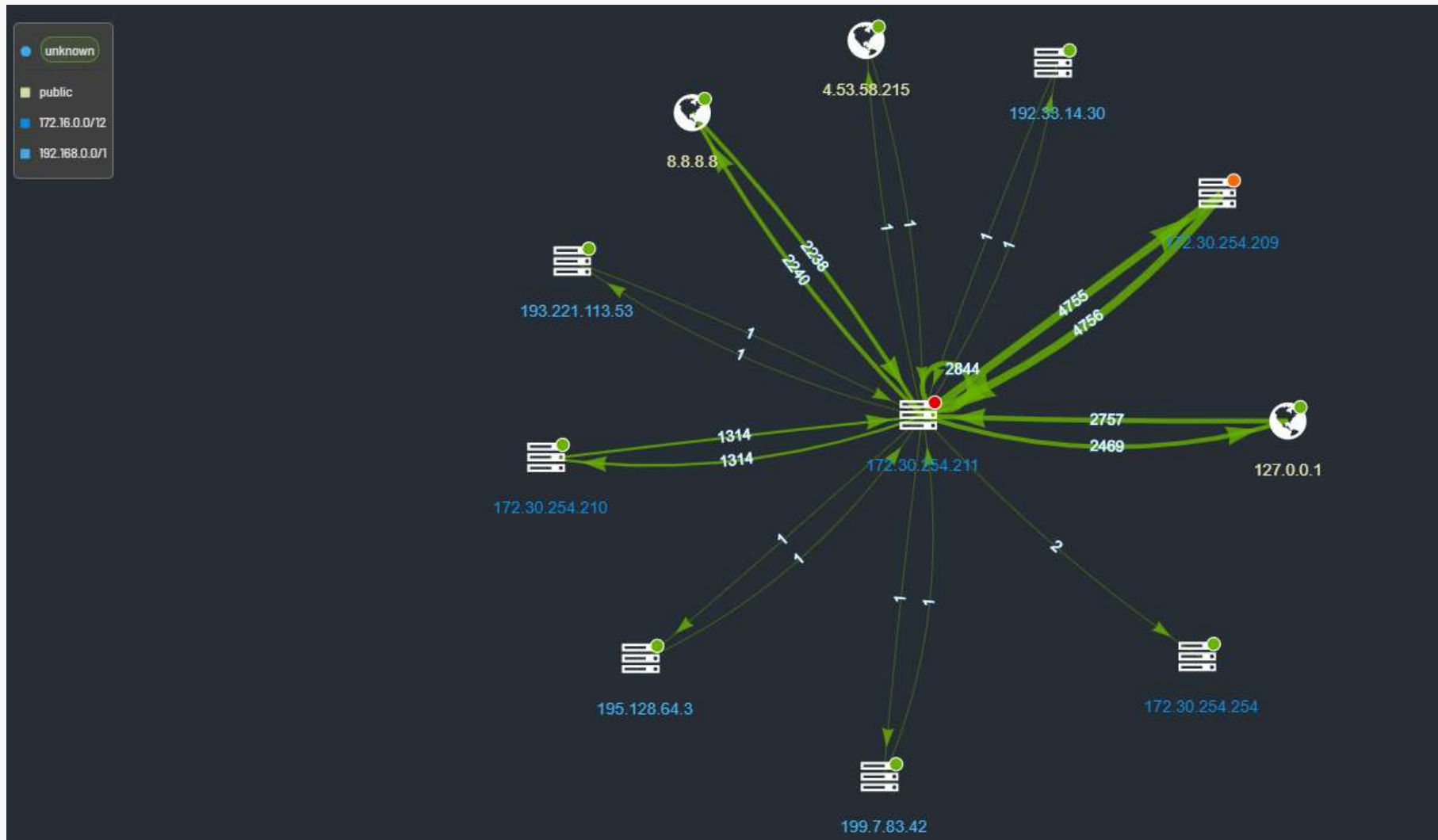
Добавить метку

Выбранные события

172.30.254.211 / microsoft / dns / dns_answer / A DNS query was answered

Обр	Дата	Отправитель (→)	Получатель (←)	Черный список	initiator.servi
<input type="checkbox"/>	24.09.2019, 12:18:42:000 (+0300)	172.30.254.211	172.30.254.210	н/д	
<input type="checkbox"/>	24.09.2019, 12:18:24:000 (+0300)	172.30.254.211	127.0.0.1	н/д	
<input type="checkbox"/>	24.09.2019, 12:17:37:000 (+0300)	172.30.254.211	172.30.254.210	н/д	
<input type="checkbox"/>	24.09.2019, 12:16:32:000 (+0300)	172.30.254.211	172.30.254.210	н/д	
<input type="checkbox"/>	24.09.2019, 12:15:27:000 (+0300)	172.30.254.211	172.30.254.210	н/д	

ИНТЕРФЕЙС АНАЛИТИКА



Карта взаимодействия хостов