



# aVistar/V

П Р И М Е Н Е Н И Е   и   П Р И М Е Р Ы



## Кибербезопасность

система aVistar для исследования  
киберинцидентов

В документе представлены некоторые варианты использования системы aVistar применительно к вопросам кибербезопасности.

## Оглавление

|  |    |
|--|----|
| О чем этот документ.....   | 3  |
| aVistar в экосистеме обеспечения кибербезопасности.....                              | 4  |
| Примеры использования .....  | 5  |
| #1. Контроль нарушений политики блокировки трафика по географическому признаку ..... | 5  |
| #2. Подозрительные доменные имена в запросах.....                                    | 8  |
| #3. Работа с короткими TCP сессиями .....  | 11 |
| #4. Нешифрованный трафик: HTTP сессии .....  | 13 |
| #5. Подозрение на атаки типа «отказ в обслуживании» .....                            | 18 |
| #6. Быстрый обзор серверных логических портов.....                                   | 19 |
| О системе aVistar .....  | 23 |
| Почему aVistar.....  | 23 |
| О компании-разработчике .....  | 25 |

## О чем этот документ

Система визуализации информационных потоков **aVistar/V** предлагается как прозрачный и быстрый инструмент первичного обнаружения, целеуказания или подтверждения событий в рамках анализа киберинцидентов на сетях масштаба предприятия.

---

Где применяется:

- // сети масштаба предприятия
- // сети критической инфраструктуры
- // сети IoT

---

Философия использования:

- // как часть экосистемы SIEM<sup>1</sup>

---

Кто использует:

- // подразделения, отвечающие за кибербезопасность, blue teams

Для решения задач мы используем простые и понятные визуальные подходы, мощную фильтрацию, вертикальный анализ и возможность показать информационные потоки в различных срезах в реальном времени или в ретроспективе.

---

<sup>1</sup> SIEM - Security information and event management

# aVistar в экосистеме обеспечения кибербезопасности

## Проблема 1

Поверхность кибератак на инфраструктуру и сети постоянно расширяется, что серьёзно затрудняет быстрый поиск источников атак и их вектор. Возникает потребность в инструментах, которые позволят быстро увидеть аномалии в информационных потоках, быстро оценить риски и, при необходимости, быстро принять решение о дальнейших шагах по купированию проблемы.

## Проблема 2

Существующая экосистема киберзащиты предприятия состоит из разных продуктов. Они работают по своим внутренним правилам и проприетарным алгоритмам. Это создаёт слепые зоны для инженеров, отвечающих за вопросы кибербезопасности. Приходится полагаться на «черные ящики».

## Решение

Система aVistar может стать инструментом первичного целеуказания для обнаружения и дальнейшего расследования инцидентов в области киберзащиты.

Система упрощает восприятие сложных информационных потоков в виде упорядоченного представления на основе понятных визуальных паттернов

Как правило, для первого шага противодействия кибератаке **критически важно максимально быстро сузить сектор поиска.**

Мы предлагаем использовать для этих целей простую и легко воспринимаемую графическую информацию на дашбордах aVistar.

Поиск аномалий ведется по разным направлениям и на разных уровнях. Понимается, что aVistar работает во взаимосвязи с комплексной экосистемой защиты от кибератак предприятия и является её частью.

Главная задача системы aVistar – быстро определить направления для дальнейшего поиска и анализа аномалий

## Примеры использования

### #1. Контроль нарушений политики блокировки трафика по географическому признаку

Часто возникает необходимость закрыть обмен трафиком по географическому признаку, и заблокировать трафик из/в определенных стран. В случае закрытых корпоративных сетей может быть потребность в полной блокировке внешнего трафика.

После выполнения такой блокировки возникает задача в мониторинге работы региональной политики.

Система aVistar имеет много возможностей индикации трафика по странам. Достаточно одного взгляда, чтобы убедиться работает ли политика регионального ограничения. В случае нарушения легко можно проследить, когда это случилось, из каких регионов шел трафик, каков характер этого трафика и кто был его потребителем/источником внутри периметра. Самый простой и быстрый способ увидеть распределение трафика по регионам для отдельного узла за прошедшие сутки с помощью переключателя прямо на главной странице геоинформационной системы (ГИС):

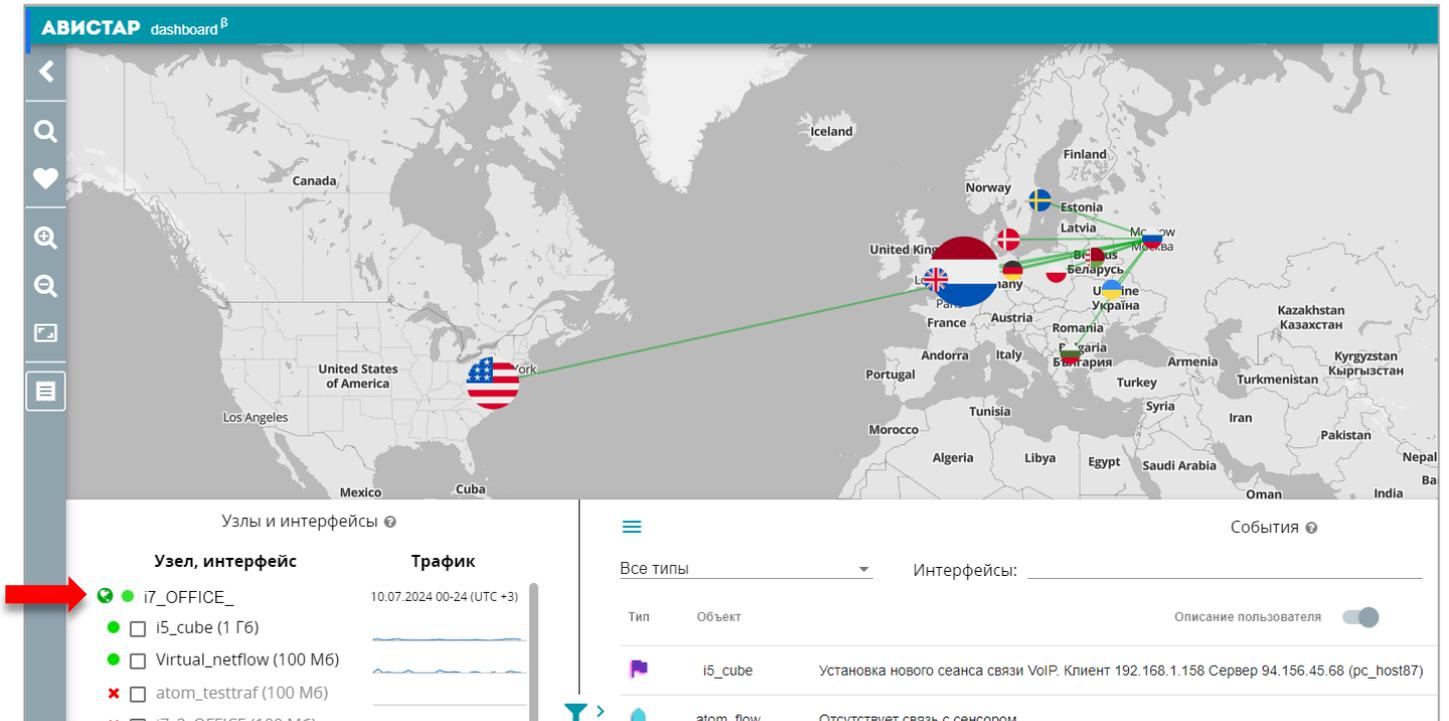
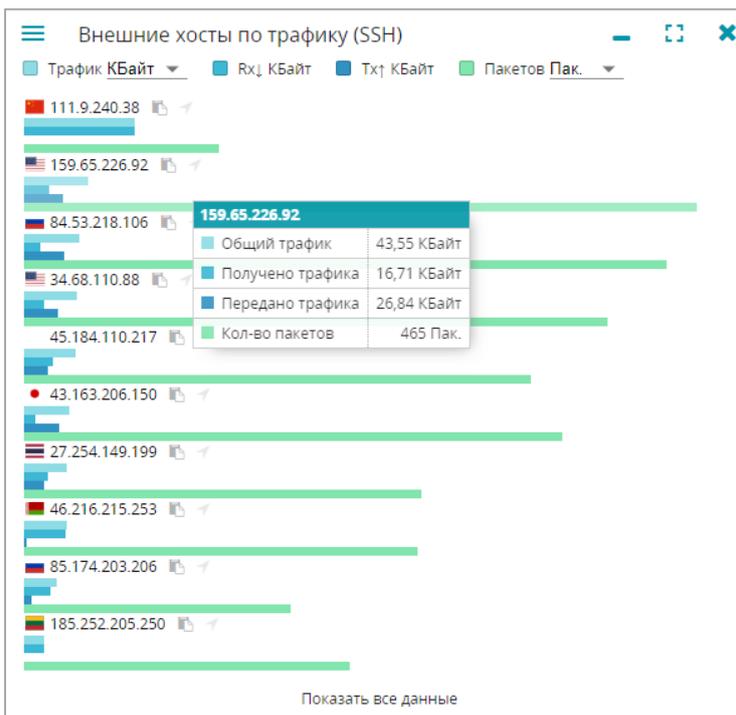


Рисунок 1 распределение трафика по географическим регионам: работают ли механизмы защиты сети от обмена трафиком с нежелательными регионами?

Предположим, в корпоративной сети есть серверы SSH, которые имеют внешние IP-адреса. Можно быстро оценить степень угрозы атак по определенному географическому вектору.

Шаг 1. Для этого откроем виджет «Внешние хосты по трафику» и отфильтруем его, например, по полярному для атак протоколу SSH:



Шаг 2. Исследуем активность хоста 159.65.226.92. Система определила его принадлежность к США. Для детализации активности 159.65.226.92 одним щелчком мышки попадаем на сессии этого хоста:

Список IP сессий за выбранный период

SSH 159.65.226.92 :Порт 159.65.226.92 :Порт

Все сессии

|  | Время начала            | Время завершения        | Длительность | Сервер     | Порт сервера | Клиент        | Порт клиента | Протокол/Сервис | Трансп. протокол | Флаги TCP | VLAN | Суммарное кол-во байт | Суммарное кол-во пакетов | Суммарный payload |
|--|-------------------------|-------------------------|--------------|------------|--------------|---------------|--------------|-----------------|------------------|-----------|------|-----------------------|--------------------------|-------------------|
|  | 11.07.2024 18:31:04.843 | 11.07.2024 18:31:04.843 | 0:00:00.0    | 172.17.0.8 | 22           | 159.65.226.92 | 55036        | SSH             | TCP              | S         | -    | 1 480                 | 20                       | 0                 |
|  | 11.07.2024 18:30:13.434 | 11.07.2024 18:30:13.434 | 0:00:00.0    | 172.17.0.8 | 22           | 159.65.226.92 | 40262        | SSH             | TCP              | S         | -    | 1 480                 | 20                       | 0                 |
|  | 11.07.2024 18:29:27.708 | 11.07.2024 18:29:27.708 | 0:00:00.0    | 172.17.0.8 | 22           | 159.65.226.92 | 53728        | SSH             | TCP              | S         | -    | 1 480                 | 20                       | 0                 |
|  | 11.07.2024 18:28:45.690 | 11.07.2024 18:28:45.690 | 0:00:00.0    | 172.17.0.8 | 22           | 159.65.226.92 | 38958        | SSH             | TCP              | S         | -    | 1 480                 | 20                       | 0                 |
|  | 11.07.2024 18:28:01.988 | 11.07.2024 18:28:01.988 | 0:00:00.0    | 172.17.0.8 | 22           | 159.65.226.92 | 52424        | SSH             | TCP              | S         | -    | 1 480                 | 20                       | 0                 |
|  | 11.07.2024 18:27:18.997 | 11.07.2024 18:27:18.997 | 0:00:00.0    | 172.17.0.8 | 22           | 159.65.226.92 | 37662        | SSH             | TCP              | SYN       | -    | 1 480                 | 20                       | 0                 |
|  | 11.07.2024 18:26:36.344 | 11.07.2024 18:26:36.344 | 0:00:00.0    | 172.17.0.8 | 22           | 159.65.226.92 | 51128        | SSH             | TCP              | S         | -    | 1 480                 | 20                       | 0                 |
|  | 11.07.2024 18:25:49.330 | 11.07.2024 18:25:49.330 | 0:00:00.0    | 172.17.0.8 | 22           | 159.65.226.92 | 36358        | SSH             | TCP              | S         | -    | 1 480                 | 20                       | 0                 |
|  | 11.07.2024 18:25:03.6   | 11.07.2024 18:25:03.6   | 0:00:00.0    | 172.17.0.8 | 22           | 159.65.226.92 | 49820        | SSH             | TCP              | S         | -    | 1 480                 | 20                       | 0                 |
|  | 11.07.2024 18:24:17.341 | 11.07.2024 18:24:17.341 | 0:00:00.0    | 172.17.0.8 | 22           | 159.65.226.92 | 35054        | SSH             | TCP              | S         | -    | 1 480                 | 20                       | 0                 |
|  | 11.07.2024 18:23:32.48  | 11.07.2024 18:23:32.48  | 0:00:00.0    | 172.17.0.8 | 22           | 159.65.226.92 | 48512        | SSH             | TCP              | S         | -    | 1 480                 | 20                       | 0                 |
|  | 11.07.2024 18:22:46.619 | 11.07.2024 18:22:46.619 | 0:00:00.0    | 172.17.0.8 | 22           | 159.65.226.92 | 33744        | SSH             | TCP              | S         | -    | 1 480                 | 20                       | 0                 |
|  | 11.07.2024 18:22:03.836 | 11.07.2024 18:22:03.836 | 0:00:00.0    | 172.17.0.8 | 22           | 159.65.226.92 | 47208        | SSH             | TCP              | S         | -    | 1 480                 | 20                       | 0                 |

Записей на странице: 50 << 1 >> Всего 25 записей (1 страница)

Prod Version 0.1 Build 1

Из таблицы сессий видно, что всего было детектировано 25 сессий, но все они заканчивались на этапе попытки синхронизации (статус “S” в колонке «Флаги TCP»). Это свидетельствует о том, что сработали механизмы защиты сервера SSH, и атака не представляет серьезной угрозы. Кроме этого следует проверить легитимность существования сервера SSH на хосте с белым IP адресом.

Аналогичные действия можно легко повторить для разных протоколов, типов сервисов, IP адресов или целых подсетей.



### ВРЕМЯ.

Время, затраченное на оценку ситуации в системе, составило менее 1 минуты.

## #2. Подозрительные доменные имена в запросах

### Отправная точка

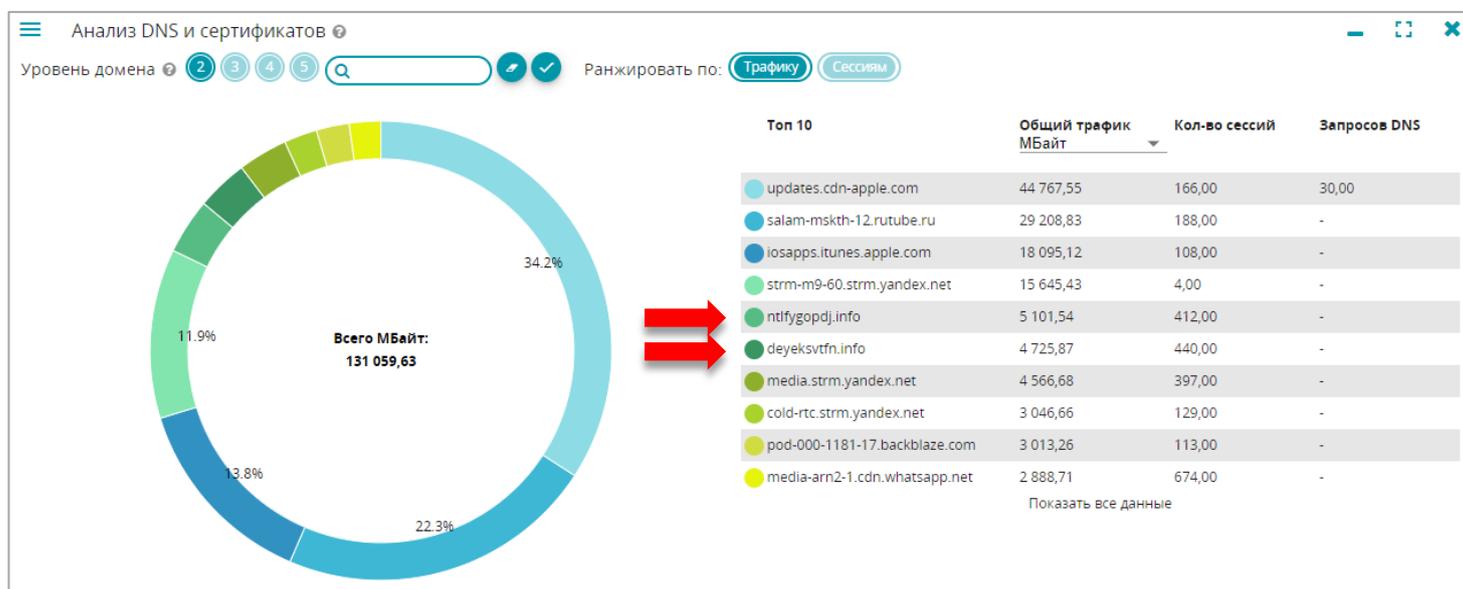


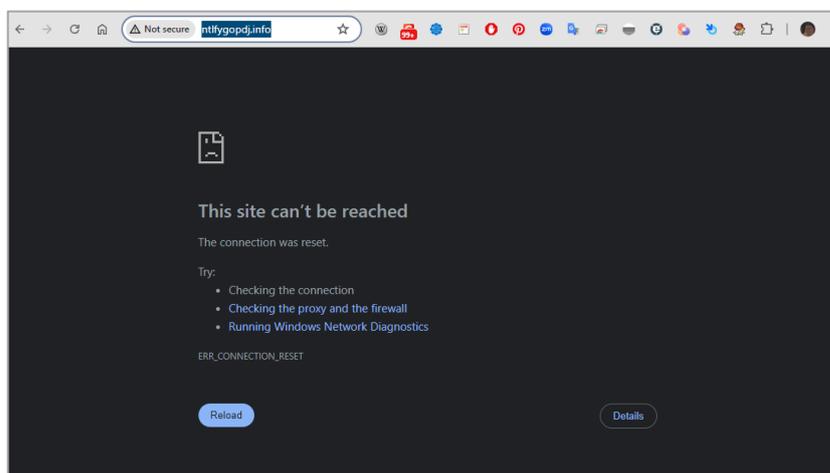
Рисунок 2 Виджет «Анализ DNS и сертификатов» со страницы Аналитика

При работе с виджетом «Анализ DNS и сертификатов» (Рисунок 2) системы aVistar обнаружилась подозрительная особенность:

- Наличие интенсивного трафика из локальной сети с нетипичными для данной сети доменными именами в запросах вида «ntlfygopdj.info».
- Одинаковая отличительная особенность: это домены второго уровня с именами из бессмысленного набора букв, принадлежащие домену «.info» первого уровня.
- Такие домены присутствуют в трафике только в течение нескольких суток.

### Дальнейшие шаги

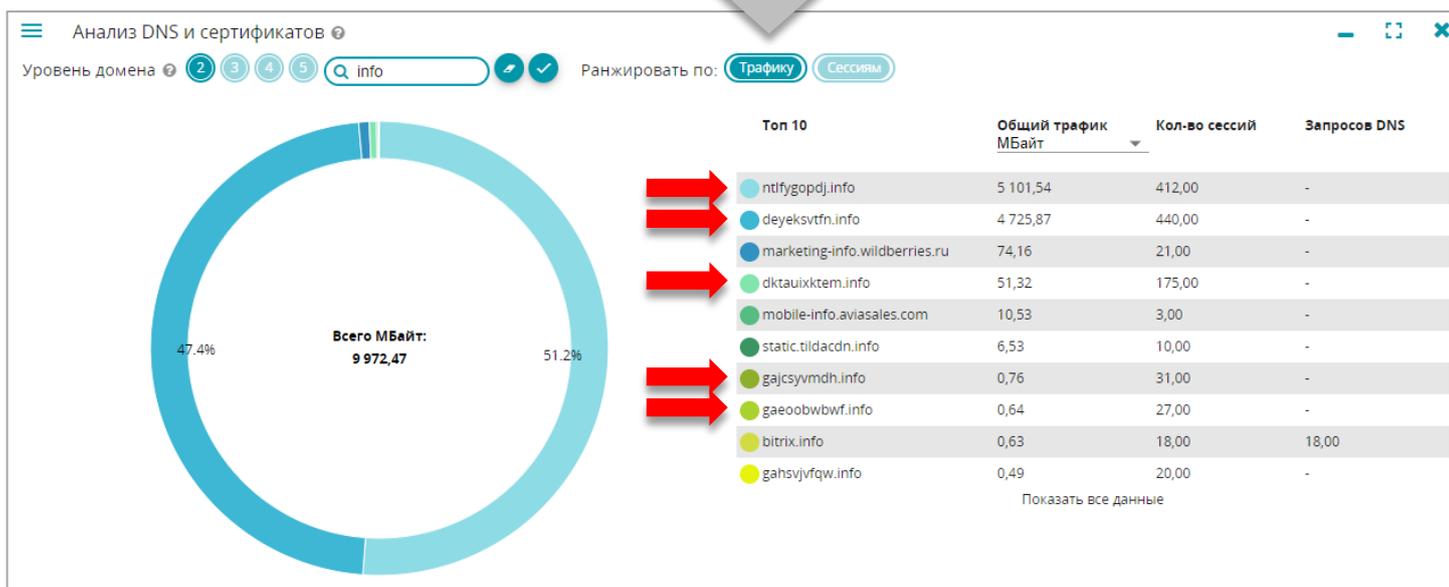
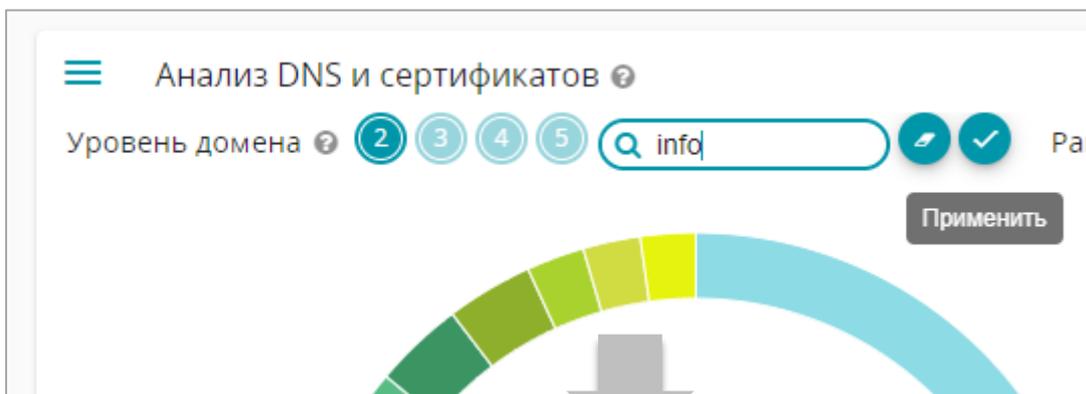
Шаг 1. Попытка зайти на один из доменов через браузер не даёт результатов:



Вместе с этим, на виджете (Рисунок 2) видно, что был интенсивный обмен трафиком между локальной сетью и доменом. Другие домены также не доступны.

Шаг 2. Выполняем поиск дополнительной информации с помощью утилиты whois и выясняем, что домен зарегистрирован анонимно из Исландии.

Шаг 3. Возвращаемся в систему, и в виджете отфильтруем все доменные имена, содержащие последовательность букв «info»:



В списке появилось ещё больше подобных доменов.

Шаг 4. Чтобы получить больше информации, нажимаем в виджете на одно из подозрительных доменных имён «deyeksvtfn.info», чтобы увидеть все сессии, которые были с этим доменом:

Информация по домену deyeksvtfn.info

| Время начала            | Время завершения        | Сервер            | Клиент               | Протокол | Кол-во байт клиент -> серв., байт | Кол-во байт серв. -> клиент, байт | Суммарное кол-во байт | Суммарное кол-во Пак. |
|-------------------------|-------------------------|-------------------|----------------------|----------|-----------------------------------|-----------------------------------|-----------------------|-----------------------|
| 19.06.2024 14:37:20.883 | 19.06.2024 14:54:38.158 | 172.67.142.33:443 | 192.168.10.180:50243 | HTTPS    | 61 102 428                        | 2 104 402 869                     | 2 165 505 297         | 2 288 949             |
| 19.06.2024 14:22:26.559 | 19.06.2024 14:37:08.401 | 172.67.142.33:443 | 192.168.10.180:50243 | HTTPS    | 58 560 380                        | 1 993 901 069                     | 2 052 461 449         | 2 197 713             |
| 19.06.2024 15:23:29.392 | 19.06.2024 15:25:56.875 | 172.67.142.33:443 | 192.168.10.180:51784 | HTTPS    | 5 488 958                         | 170 928 617                       | 176 417 575           | 180 823               |
| 19.06.2024 15:29:56.798 | 19.06.2024 15:32:02.447 | 172.67.142.33:443 | 192.168.10.180:51784 | HTTPS    | 3 559 164                         | 122 013 472                       | 125 572 636           | 125 358               |
| 19.06.2024 15:28:27.014 | 19.06.2024 15:29:41.779 | 172.67.142.33:443 | 192.168.10.180:51784 | HTTPS    | 4 144 256                         | 111 921 217                       | 116 065 473           | 126 754               |
| 19.06.2024 15:27:04.924 | 19.06.2024 15:28:11.611 | 172.67.142.33:443 | 192.168.10.180:51784 | HTTPS    | 2 657 908                         | 74 191 106                        | 76 849 014            | 86 247                |
| 19.06.2024 14:21:26.146 | 19.06.2024 14:21:57.035 | 172.67.142.33:443 | 192.168.10.180:50243 | HTTPS    | 2 841 387                         | 67 570 159                        | 70 411 546            | 77 652                |
| 19.06.2024 15:26:11.887 | 19.06.2024 15:26:49.895 | 172.67.142.33:443 | 192.168.10.180:51784 | HTTPS    | 1 453 886                         | 33 281 022                        | 34 734 908            | 38 593                |
| 19.06.2024 14:21:22.587 | 19.06.2024 14:21:41.808 | 172.67.142.33:443 | 192.168.10.180:50187 | HTTPS    | 2 466 261                         | 9 655 572                         | 12 121 833            | 20 469                |
| 19.06.2024 14:35:10.154 | 19.06.2024 14:35:57.090 | 172.67.142.33:443 | 192.168.10.180:50187 | HTTPS    | 779 998                           | 9 522 856                         | 10 302 854            | 13 020                |
| 19.06.2024 14:55:25.745 | 19.06.2024 14:55:42.943 | 172.67.142.33:443 | 192.168.10.180:51325 | HTTPS    | 428 314                           | 9 724 830                         | 10 153 144            | 10 776                |

Записей на странице: 50 << < 1 > >> **Всего 496 записей** (10 страниц)

Экспорт      Закреть

Из сводной таблицы видно, что с доменом «deyeksvtfn.info» (сервер 172.67.142.33) из локальной сети общался клиент 192.168.10.180 по протоколу HTTPS. Всего было установлено 496 сессий.

Шаг 5. Проверка IP адреса 172.67.142.33 с помощью whois показывает, что он принадлежит CDN сервису Cloudflare.

### Предварительная оценка рисков

#### Факторы:

Подозрительные доменные имена в трафике пользователей

Доменные не открываются в браузере

Регистрация доменов выполнена максимально анонимно, не ясна принадлежность этих доменов организациям

IP адреса доменов принадлежат глобальному CDN-провайдеру

Объём трафика по подозрительным направлениям – высокий

Тип трафика – зашифрованный

#### Риск:

Средний

**Высокий**

**Высокий**

Низкий

Средний

**Высокий**

Степень риска по совокупности факторов: **ВЫСОКАЯ**



**ВЫВОД.** С помощью системы aVistar мы обнаружили подозрительную активность клиента из нашей локальной сети 192.168.10.180, который использует внешние серверы по протоколу https с очень нетипичными доменными именами. Принадлежность и назначение этих внешних серверов вызывает необходимость дальнейших исследований активности хоста 192.169.10.180 дополнительными инструментами.



**ВРЕМЯ:** Время от обнаружения на дашборде до принятия решения по дальнейшим шагам составило **около 4 минут**.

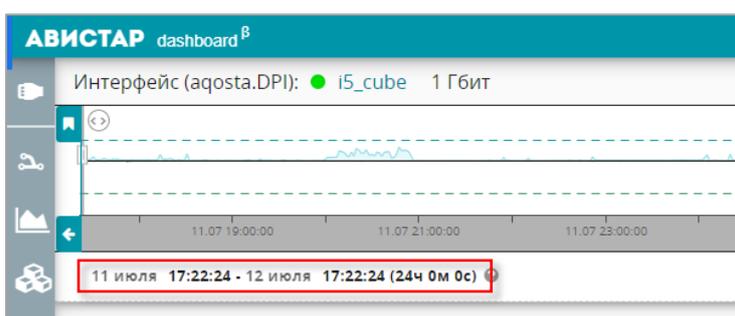
### #3. Работа с короткими TCP сессиями

В реальной сети одновременно существует большое количество сессий. Большинство из них выполняет полезную функцию.

С точки зрения кибербезопасности интерес представляют различного рода «мусорные» сессии. Как правило, это завершенная сессия, и они появляются в результате отказа промежуточных или конечных сетевых точек выполнять запрос, который содержался в такой сессии. В ряде случаев, такие сессии появляются в результате деградации качества работы сетевой инфраструктуры, или приложений.

#### Как система aVistar может помочь быстро увидеть такие сессии

Шаг 1. Выберем интервал времени на временной шкале. Например, 24 часа:



Это можно сделать как для анализа в реальном времени, так и в прошлом.

Шаг 2. Таблица на экране сессионного представления в течение нескольких секунд отобразит все 2606781 сессию за указанный интервал:

|   | Время начала            | Время завершения        | Длительность | Сервер          | Порт сервера | Клиент        | Порт клиента | Протокол/Сервис | Трансп. протокол | Флаги TCP | VLAN | Суммарное кол-во байт | Суммарное кол-во пакетов | Суммарный payload |
|---|-------------------------|-------------------------|--------------|-----------------|--------------|---------------|--------------|-----------------|------------------|-----------|------|-----------------------|--------------------------|-------------------|
| ⚠ | 12.07.2024 17:22:23.935 | 12.07.2024 17:22:23.950 | 0:00:00.15   | 35.201.107.59   | 443          | 192.168.1.147 | 57453        | SSL             | TCP              | A         | -    | 2 820                 | 45                       | 150               |
| ⚠ | 12.07.2024 17:22:23.928 | 12.07.2024 17:22:23.946 | 0:00:00.18   | 8.8.8.8         | 53           | 192.168.1.4   | 49136        | DNS             | UDP              |           | -    | 3 540                 | 36                       | 2 028             |
| ⚠ | 12.07.2024 17:22:23.919 | 12.07.2024 17:22:23.923 | 0:00:00.4    | 87.250.251.15   | 443          | 192.168.1.53  | 57792        | SSL             | TCP              | A         | -    | 2 820                 | 45                       | 150               |
| ⚠ | 12.07.2024 17:22:23.906 | 12.07.2024 17:22:23.921 | 0:00:00.15   | 108.177.14.168  | 443          | 192.168.1.61  | 54673        | SSL             | TCP              | A         | -    | 1 566                 | 26                       | 150               |
| ⚠ | 12.07.2024 17:22:23.900 | 12.07.2024 17:22:23.942 | 0:00:00.41   | 209.250.254.15  | 21116        | 192.168.1.75  | 54001        | UNKNOWN         | UDP              |           | -    | 3 000                 | 50                       | 900               |
| ⚠ | 12.07.2024 17:22:23.856 | 12.07.2024 17:22:23.939 | 0:00:00.83   | 209.250.254.15  | 21116        | 192.168.1.75  | 59311        | UNKNOWN         | TCP              | SAPFR     | -    | 12 832                | 186                      | 2 448             |
| ⚠ | 12.07.2024 17:22:23.823 | 12.07.2024 17:22:23.887 | 0:00:00.63   | 176.114.120.5   | 443          | 192.168.1.11  | 56990        | HTTPS           | UDP              | AP        | -    | 5 870                 | 59                       | 2 684             |
| ⚠ | 12.07.2024 17:22:23.609 | 12.07.2024 17:22:23.609 | 0:00:00.0    | 192.168.110.77  | 5353         | 224.0.0.251   | 5353         | MCAST           | TCP              |           | -    | 1 653                 | 19                       | 855               |
| ⚠ | 12.07.2024 17:22:23.554 | 12.07.2024 17:22:23.620 | 0:00:00.66   | 173.194.221.102 | 443          | 192.168.1.61  | 64245        | HTTPS           | TCP              | SAPR      | -    | 36 956                | 306                      | 19 952            |
| ⚠ | 12.07.2024 17:22:23.517 | 12.07.2024 17:22:23.594 | 0:00:00.76   | 173.194.221.102 | 443          | 192.168.1.61  | 64244        | HTTPS           | TCP              | SAPR      | -    | 37 084                | 306                      | 20 080            |
| ⚠ | 12.07.2024 17:22:23.470 | 12.07.2024 17:22:23.481 | 0:00:00.11   | 87.250.251.15   | 443          | 192.168.1.53  | 52319        | SSL             | TCP              | A         | -    | 2 820                 | 45                       | 150               |
| ⚠ | 12.07.2024 17:22:23.257 | 12.07.2024 17:22:23.262 | 0:00:00.4    | 77.88.44.242    | 443          | 192.168.1.147 | 55892        | SSL             | TCP              | A         | -    | 2 820                 | 45                       | 150               |
| ⚠ | 12.07.2024 17:22:23.194 | 12.07.2024 17:22:23.198 | 0:00:00.4    | 213.180.193.234 | 443          | 192.168.1.70  | 62173        | SSL             | TCP              | A         | -    | 2 820                 | 45                       | 150               |

Записей на странице: 50 << < 1 > >> Всего 2 606 781 запись (51 114 страниц)

Шаг 3. В таблице нас интересует колонка «Суммарное кол-во байт». Отсортируем данные в этой колонке по возрастанию, просто нажав на заголовок:

|   | Время начала           | Время завершения       | Длительность | Сервер          | Порт сервера | Клиент         | Порт клиента | Протокол/Сервис | Трансп. протокол | Флаги TCP | VLAN | Суммарное кол-во байт | Суммарное кол-во пакетов | Суммарный payload |
|---|------------------------|------------------------|--------------|-----------------|--------------|----------------|--------------|-----------------|------------------|-----------|------|-----------------------|--------------------------|-------------------|
| ⚠ | 12.07.2024 0:02:41.557 | 12.07.2024 0:02:41.557 | 0:00:00.0    | 173.194.221.101 | 443          | 192.168.1.147  | 58431        | SSL             | TCP              | AR        | -    | 60                    | 1                        | 6                 |
| ⚠ | 12.07.2024 0:00:20.565 | 12.07.2024 0:00:20.565 | 0:00:00.0    | 142.251.1.100   | 443          | 192.168.1.70   | 54997        | SSL             | TCP              | AR        | -    | 60                    | 1                        | 6                 |
| ⚠ | 12.07.2024 0:07:46.674 | 12.07.2024 0:07:46.674 | 0:00:00.0    | 173.194.221.101 | 443          | 192.168.1.28   | 54278        | SSL             | TCP              | AR        | -    | 60                    | 1                        | 6                 |
| ⚠ | 12.07.2024 0:06:57.635 | 12.07.2024 0:06:57.635 | 0:00:00.0    | 204.79.197.239  | 443          | 192.168.1.84   | 50759        | SSL             | TCP              | AR        | -    | 60                    | 1                        | 6                 |
| ⚠ | 12.07.2024 0:08:41.555 | 12.07.2024 0:08:41.555 | 0:00:00.0    | 173.194.222.101 | 443          | 192.168.1.147  | 58513        | SSL             | TCP              | AR        | -    | 60                    | 1                        | 6                 |
| ⚠ | 12.07.2024 0:12:46.693 | 12.07.2024 0:12:46.693 | 0:00:00.0    | 173.194.222.139 | 443          | 192.168.1.28   | 54395        | SSL             | TCP              | AR        | -    | 60                    | 1                        | 6                 |
| ⚠ | 12.07.2024 0:11:52.733 | 12.07.2024 0:11:52.733 | 0:00:00.0    | 173.194.221.138 | 443          | 192.168.1.70   | 55132        | SSL             | TCP              | AR        | -    | 60                    | 1                        | 6                 |
| ⚠ | 12.07.2024 0:13:15.324 | 12.07.2024 0:13:15.324 | 0:00:00.0    | 176.18.215.7    | 6982         | 194.180.49.119 | 43789        | UNKNOWN         | TCP              | S         | -    | 60                    | 1                        | 6                 |
| ⚠ | 12.07.2024 0:13:13.563 | 12.07.2024 0:13:13.563 | 0:00:00.0    | 173.194.222.139 | 443          | 192.168.1.70   | 55153        | TCP             | TCP              | AR        | -    | 60                    | 1                        | 6                 |
| ⚠ | 12.07.2024 0:11:51.149 | 12.07.2024 0:11:51.149 | 0:00:00.0    | 173.194.221.102 | 443          | 192.168.1.61   | 64023        | SSL             | TCP              | AR        | -    | 60                    | 1                        | 6                 |
| ⚠ | 12.07.2024 0:11:54.253 | 12.07.2024 0:11:54.253 | 0:00:00.0    | 192.168.1.177   | 445          | 192.168.1.10   | 57438        | SMBV23          | TCP              | AR        | -    | 60                    | 1                        | 6                 |
| ⚠ | 12.07.2024 0:20:44.600 | 12.07.2024 0:20:44.600 | 0:00:00.0    | 194.180.49.119  | 43789        | 178.18.215.8   | 61523        | UNKNOWN         | TCP              | S         | -    | 60                    | 1                        | 6                 |
| ⚠ | 12.07.2024 0:19:46.581 | 12.07.2024 0:19:46.581 | 0:00:00.0    | 173.194.222.138 | 443          | 192.168.1.28   | 54875        | SSL             | TCP              | AR        | -    | 60                    | 1                        | 6                 |

Записей на странице: 50 << < 1 > >> Всего 2 606 781 запись (51 114 страниц)

Мы получили список самых коротких сессий, обнаруженных системой за указанный интервал времени.

Шаг 4. Мы можем оценить характер этих сессий, используя данные таблицы:

- Флаги TCP – могут дать очень полезную информацию о состоянии этих сессий.
- Мы видим участников, логические порты и протоколы (сервисы), задействованные в этих сессиях. При необходимости можем быстро увидеть цифровой след хостов из этих сессий внутри системы.
- Продолжительность сессий.
- Детализация любой из сессий.



## ВРЕМЯ.

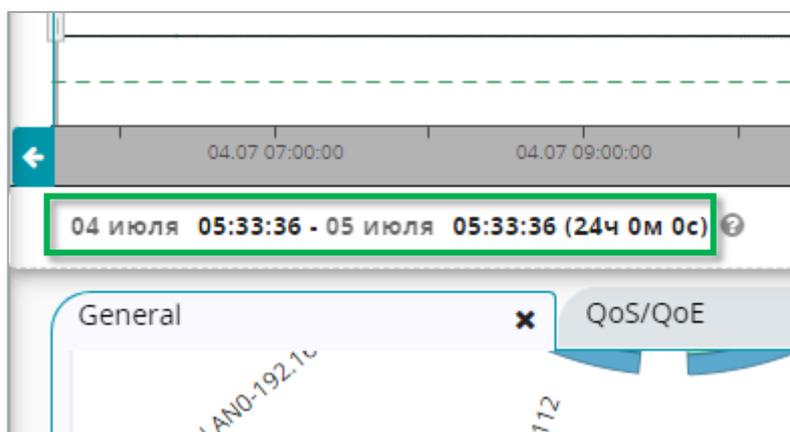
На получение исходной информации мы используем встроенный функционал. Потраченное время составляет **менее 1 минуты**.

### #4. Нешифрованный трафик: HTTP сессии

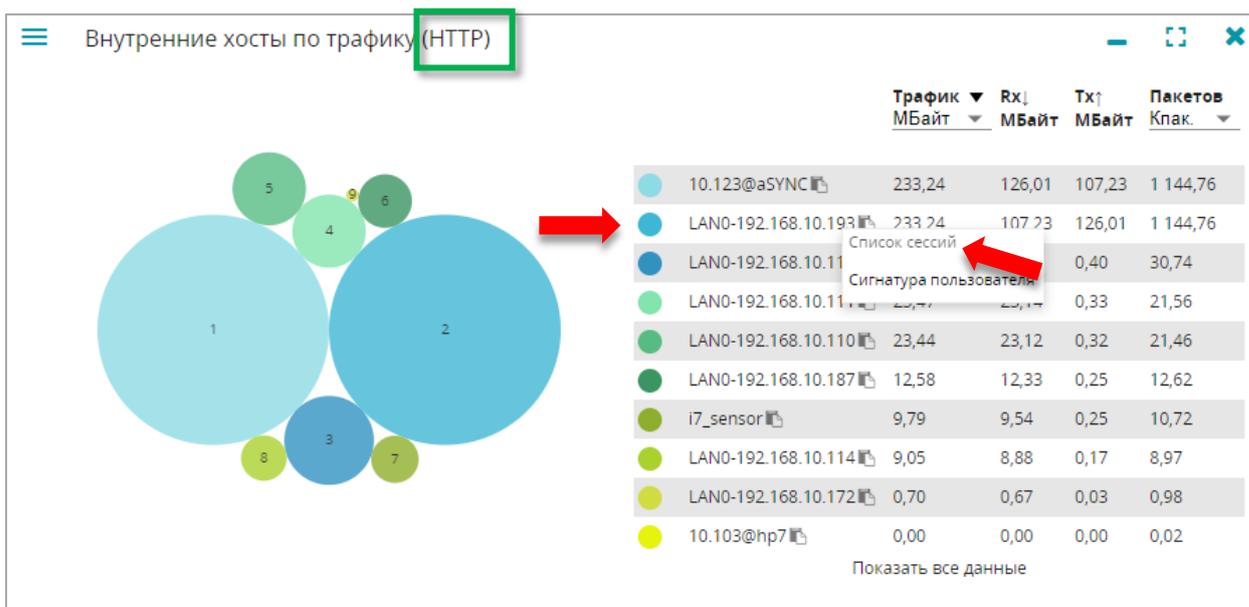
Особый интерес – соединения http. Необходимо быстро увидеть эти сессии и разобраться не несут ли они угрозы.

Давайте посмотрим, как система aVistar может помочь.

Шаг 1. Сначала выберем интервал времени для поиска:



Шаг 2. Отфильтруем трафик внутренних хостов по протоколу HTTP, и отсортируем по объему трафика с помощью готового виджета:



Шаг 3. Перейдем на список HTTP-сессий какого-нибудь хоста из верхней части таблицы виджета выше, например, хоста с именем «LAN0-192.168.10.193»:

| Время начала           | Время завершения       | Длительность | Сервер         | Порт сервера | Клиент         | Порт клиента | Протокол/Сервис | Трансп. протокол | Флаги TCP | VLAN | Суммарное кол-во байт | Суммарное кол-во пакетов | Суммарный payload |
|------------------------|------------------------|--------------|----------------|--------------|----------------|--------------|-----------------|------------------|-----------|------|-----------------------|--------------------------|-------------------|
| 05.07.2024 5:31:56.734 | 05.07.2024 5:31:56.755 | 0:00:00.21   | 192.168.10.193 | 80           | 192.168.10.123 | 33712        | HTTP            | TCP              | SAPF      | -    | 3 388                 | 24                       | 1 772             |
| 05.07.2024 5:31:26.733 | 05.07.2024 5:31:26.760 | 0:00:00.26   | 192.168.10.193 | 80           | 192.168.10.123 | 40560        | HTTP            | TCP              | SAPF      | -    | 3 388                 | 24                       | 1 772             |
| 05.07.2024 5:30:56.734 | 05.07.2024 5:30:56.755 | 0:00:00.20   | 192.168.10.193 | 80           | 192.168.10.123 | 39834        | HTTP            | TCP              | SAPF      | -    | 3 388                 | 24                       | 1 772             |
| 05.07.2024 5:30:26.734 | 05.07.2024 5:30:26.755 | 0:00:00.21   | 192.168.10.193 | 80           | 192.168.10.123 | 47942        | HTTP            | TCP              | SAPF      | -    | 3 388                 | 24                       | 1 772             |
| 05.07.2024 5:29:56.734 | 05.07.2024 5:29:56.758 | 0:00:00.24   | 192.168.10.193 | 80           | 192.168.10.123 | 48492        | HTTP            | TCP              | SAPF      | -    | 3 388                 | 24                       | 1 772             |
| 05.07.2024 5:29:26.734 | 05.07.2024 5:29:26.754 | 0:00:00.20   | 192.168.10.193 | 80           | 192.168.10.123 | 55166        | HTTP            | TCP              | SAPF      | -    | 3 388                 | 24                       | 1 772             |
| 05.07.2024 5:28:56.733 | 05.07.2024 5:28:56.759 | 0:00:00.26   | 192.168.10.193 | 80           | 192.168.10.123 | 46928        | HTTP            | TCP              | SAPF      | -    | 3 388                 | 24                       | 1 772             |
| 05.07.2024 5:28:26.733 | 05.07.2024 5:28:26.756 | 0:00:00.22   | 192.168.10.193 | 80           | 192.168.10.123 | 45048        | HTTP            | TCP              | SAPF      | -    | 3 388                 | 24                       | 1 772             |
| 05.07.2024 5:27:56.743 | 05.07.2024 5:27:56.770 | 0:00:00.26   | 192.168.10.193 | 80           | 192.168.10.123 | 48420        | HTTP            | TCP              | SAPF      | -    | 3 388                 | 24                       | 1 772             |
| 05.07.2024 5:27:26.733 | 05.07.2024 5:27:26.759 | 0:00:00.26   | 192.168.10.193 | 80           | 192.168.10.123 | 43684        | HTTP            | TCP              | SAPF      | -    | 3 388                 | 24                       | 1 772             |
| 05.07.2024 5:26:56.733 | 05.07.2024 5:26:56.757 | 0:00:00.24   | 192.168.10.193 | 80           | 192.168.10.123 | 56852        | HTTP            | TCP              | SAPF      | -    | 3 388                 | 24                       | 1 772             |
| 05.07.2024 5:26:26.733 | 05.07.2024 5:26:26.755 | 0:00:00.22   | 192.168.10.193 | 80           | 192.168.10.123 | 56736        | HTTP            | TCP              | SAPF      | -    | 3 388                 | 24                       | 1 772             |
| 05.07.2024 5:25:56.743 | 05.07.2024 5:25:56.765 | 0:00:00.21   | 192.168.10.193 | 80           | 192.168.10.123 | 40764        | HTTP            | TCP              | SAPF      | -    | 3 388                 | 24                       | 1 772             |

Записей на странице: 50 << 1 >> Всего 41 554 записи (815 страниц)

Из рисунка выше видно, что было детектировано 41554 сессии HTTP с участием этого хоста, что свидетельствует об интенсивном трафике.

Шаг 4. Теперь зададим более детальный контекст поиска и наложим дополнительный фильтр на таблицу этих сессий. Цель – выявить сессии, в которых обнаружена полезная информация. Для этого применим дополнительное условие:

Расширенный фильтр

Название поля: Http application context

Условие: Не пустое

Отменить Применить

| Время начала           | Время завершения       | Длительность | Сервер         | Порт сервера | Клиент         | Порт клиента | Протокол/Сервис | Трансп. протокол | Флаги TCP | VLAN | Суммарное кол-во байт | Суммарное кол-во пакетов | Суммарный payload |
|------------------------|------------------------|--------------|----------------|--------------|----------------|--------------|-----------------|------------------|-----------|------|-----------------------|--------------------------|-------------------|
| 05.07.2024 5:31:56.734 | 05.07.2024 5:31:56.755 | 0:00:00.21   | 192.168.10.193 | 80           | 192.168.10.123 | 33712        | HTTP            | TCP              | SAPF      | -    | 3 388                 | 24                       | 1 772             |
| 05.07.2024 5:31:26.733 | 05.07.2024 5:31:26.760 | 0:00:00.26   | 192.168.10.193 | 80           | 192.168.10.123 | 40560        | HTTP            | TCP              | SAPF      | -    | 3 388                 | 24                       | 1 772             |
| 05.07.2024 5:30:56.734 | 05.07.2024 5:30:56.755 | 0:00:00.20   | 192.168.10.193 | 80           | 192.168.10.123 | 39834        | HTTP            | TCP              | SAPF      | -    | 3 388                 | 24                       | 1 772             |
| 05.07.2024 5:30:26.734 | 05.07.2024 5:30:26.755 | 0:00:00.21   | 192.168.10.193 | 80           | 192.168.10.123 | 47942        | HTTP            | TCP              | SAPF      | -    | 3 388                 | 24                       | 1 772             |
| 05.07.2024 5:29:56.734 | 05.07.2024 5:29:56.758 | 0:00:00.24   | 192.168.10.193 | 80           | 192.168.10.123 | 48492        | HTTP            | TCP              | SAPF      | -    | 3 388                 | 24                       | 1 772             |
| 05.07.2024 5:29:26.734 | 05.07.2024 5:29:26.754 | 0:00:00.20   | 192.168.10.193 | 80           | 192.168.10.123 | 55166        | HTTP            | TCP              | SAPF      | -    | 3 388                 | 24                       | 1 772             |
| 05.07.2024 5:28:56.733 | 05.07.2024 5:28:56.759 | 0:00:00.26   | 192.168.10.193 | 80           | 192.168.10.123 | 46928        | HTTP            | TCP              | SAPF      | -    | 3 388                 | 24                       | 1 772             |
| 05.07.2024 5:28:26.733 | 05.07.2024 5:28:26.756 | 0:00:00.22   | 192.168.10.193 | 80           | 192.168.10.123 | 45048        | HTTP            | TCP              | SAPF      | -    | 3 388                 | 24                       | 1 772             |
| 05.07.2024 5:27:56.743 | 05.07.2024 5:27:56.770 | 0:00:00.26   | 192.168.10.193 | 80           | 192.168.10.123 | 48420        | HTTP            | TCP              | SAPF      | -    | 3 388                 | 24                       | 1 772             |
| 05.07.2024 5:27:26.733 | 05.07.2024 5:27:26.759 | 0:00:00.26   | 192.168.10.193 | 80           | 192.168.10.123 | 43684        | HTTP            | TCP              | SAPF      | -    | 3 388                 | 24                       | 1 772             |

Ожидаемо, что общее количество сессий сократилось до 12101:

|   |                        |                        |           |                |
|---|------------------------|------------------------|-----------|----------------|
| ☰ | 05.07.2024 2:47:58.344 | 05.07.2024 2:47:58.351 | 0:00:00.7 | 192.168.10.193 |
| ☰ | 05.07.2024 2:47:58.131 | 05.07.2024 2:47:58.136 | 0:00:00.4 | 192.168.10.193 |
| ☰ | 05.07.2024 2:47:57.912 | 05.07.2024 2:47:57.918 | 0:00:00.6 | 192.168.10.193 |
| ☰ | 05.07.2024 2:47:57.760 | 05.07.2024 2:47:57.766 | 0:00:00.5 | 192.168.10.193 |
| ☰ | 05.07.2024 2:47:57.667 | 05.07.2024 2:47:57.674 | 0:00:00.6 | 192.168.10.193 |
| ☰ | 05.07.2024 2:47:57.655 | 05.07.2024 2:47:57.660 | 0:00:00.5 | 192.168.10.193 |
| ☰ | 05.07.2024 2:47:57.643 | 05.07.2024 2:47:57.649 | 0:00:00.5 | 192.168.10.193 |

Записей на странице: 50 << < 1 > >> Всего 12 101 запись

Шаг 5. Давайте посмотрим детализацию любой произвольной сессии из отфильтрованного списка:

Параметры сессии по интерфейсу "atom\_testtraf"

Начало: 05.07.2024 2:47:58.485  
Завершение: 05.07.2024 2:47:58.492

В текущий момент времени сессия завершена (Состояние: Завершилась по таймауту)

сервер: 192.168.10.193:80  
клиент: 192.168.10.123:53662

• VLAN -  
• ToS 0  
• CoS 0

Не показывать пустые значения

| Трафик                   | QoS / QoE  | HTTP | Нарушения трафика | Дополнительно |
|--------------------------|--|------|-------------------|---------------|
| Http application context | text/html; charset=UTF-8   |      |                   |               |
| Http url                 | http://192.168.10.193/settoppro  |      |                   |               |
| Http user agent          | Apache-HttpClient/4.5.13 (Java/11.0.16)  |      |                   |               |
| Request method           | POST   |      |                   |               |
| Http cookie              | sessionId={3d012a13-2c9e-4d8a-9056-6197ad9dacf1}; Comment=Identifies the user; Max-Age=3600; Path=/; SameSite=Lax; Version=1 |      |                   |               |

Закреть

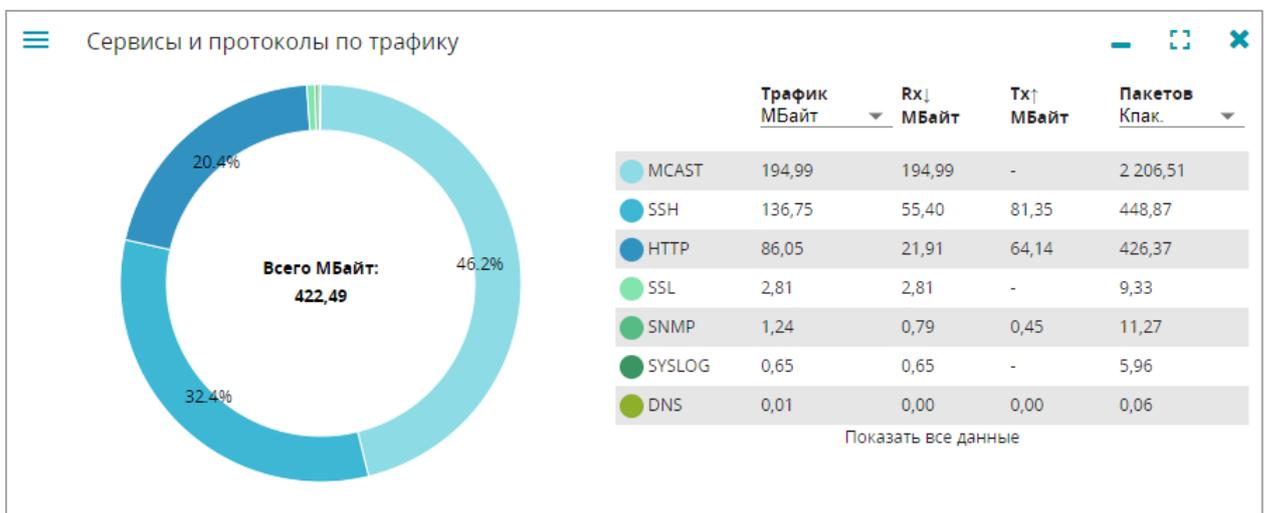
Озабоченность вызывает идентификатор сессии {3d012a13-2c9e-4d8a-9056-6197ad9dacf1}, который передаётся в cookie в открытом виде. Он может быть использован для установки несанкционированного доступа к хосту с IP адресом 192.168.10.193.

Кроме этого, клиент (192.168.10.123), который общается с названным хостом, с большой вероятностью является программой, написанной на Java v.11. Этот клиент активно воздействует на хост 10.193 с помощью процедуры POST.

Выборочная детализация по остальным сессиям показывает те же тренды.

### Дальнейшие шаги

Если информация о хосте 192.168.10.193 отсутствует, давайте попробуем быстро понять его роль в сети. Для этого воспользуемся виджетом «Сервисы и протоколы по трафику» для этого хоста. По характеру трафика видно, что это не пользовательское устройство, а, скорее всего, какой-то инфраструктурный элемент:



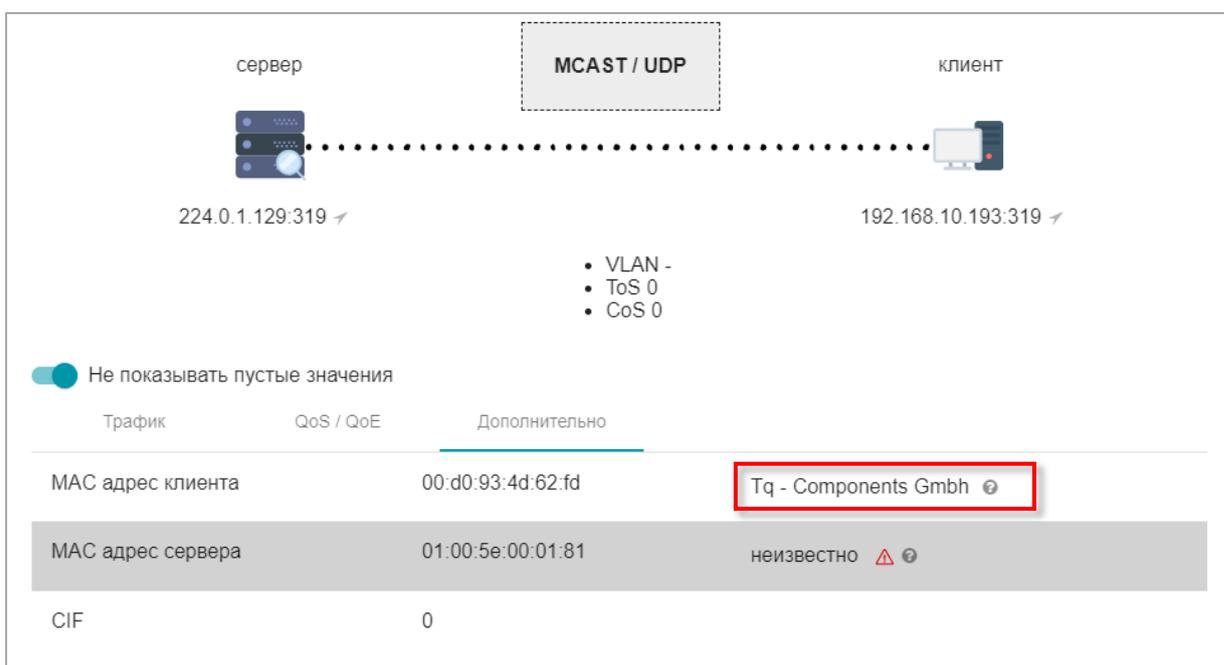
Нажатие по протоколу MCAST на виджете позволяет перейти на просмотр multicast сессий устройства 192.168.10.193:

| Время начала            | Время завершения        | Длительность | Сервер      | Порт сервера | Клиент         | Порт клиента | Протокол/Сервис | Трансп. протокол | Флаги TCP | VLAN | Суммарное кол-во байт | Суммарное кол-во пакетов | Суммарный payload |
|-------------------------|-------------------------|--------------|-------------|--------------|----------------|--------------|-----------------|------------------|-----------|------|-----------------------|--------------------------|-------------------|
| 10.07.2024 10:02:12.213 | 10.07.2024 10:02:24.214 | 0:00:12.0    | 224.0.1.129 | 320          | 192.168.10.193 | 320          | MCAST           | UDP              |           | -    | 40 414                | 419                      | 22 816            |
| 10.07.2024 10:02:08.213 | 10.07.2024 10:02:20.213 | 0:00:12.0    | 224.0.1.129 | 319          | 192.168.10.193 | 319          | MCAST           | UDP              |           | -    | 18 834                | 219                      | 9 636             |
| 10.07.2024 10:01:55.213 | 10.07.2024 10:02:07.213 | 0:00:12.0    | 224.0.1.129 | 319          | 192.168.10.193 | 319          | MCAST           | UDP              |           | -    | 20 124                | 234                      | 10 296            |
| 10.07.2024 10:01:46.213 | 10.07.2024 10:01:58.213 | 0:00:11.999  | 224.0.1.129 | 320          | 192.168.10.193 | 320          | MCAST           | UDP              |           | -    | 43 810                | 455                      | 24 700            |
| 10.07.2024 10:01:42.313 | 10.07.2024 10:01:54.213 | 0:00:11.899  | 224.0.1.129 | 319          | 192.168.10.193 | 319          | MCAST           | UDP              |           | -    | 19 006                | 221                      | 9 724             |
| 10.07.2024 10:01:33.213 | 10.07.2024 10:01:45.213 | 0:00:12.0    | 224.0.1.129 | 320          | 192.168.10.193 | 320          | MCAST           | UDP              |           | -    | 44 186                | 461                      | 24 824            |
| 10.07.2024 10:01:29.213 | 10.07.2024 10:01:41.213 | 0:00:12.0    | 224.0.1.129 | 319          | 192.168.10.193 | 319          | MCAST           | UDP              |           | -    | 20 124                | 234                      | 10 296            |
| 10.07.2024 10:01:20.213 | 10.07.2024 10:01:32.213 | 0:00:12.0    | 224.0.1.129 | 320          | 192.168.10.193 | 320          | MCAST           | UDP              |           | -    | 44 412                | 462                      | 25 008            |
| 10.07.2024 10:01:16.213 | 10.07.2024 10:01:28.213 | 0:00:12.0    | 224.0.1.129 | 319          | 192.168.10.193 | 319          | MCAST           | UDP              |           | -    | 20 124                | 234                      | 10 296            |
| 10.07.2024 10:01:07.213 | 10.07.2024 10:01:19.213 | 0:00:12.0    | 224.0.1.129 | 320          | 192.168.10.193 | 320          | MCAST           | UDP              |           | -    | 44 928                | 468                      | 25 272            |
| 10.07.2024 10:01:03.213 | 10.07.2024 10:01:15.213 | 0:00:12.0    | 224.0.1.129 | 319          | 192.168.10.193 | 319          | MCAST           | UDP              |           | -    | 20 124                | 234                      | 10 296            |
| 10.07.2024 10:00:50.213 | 10.07.2024 10:01:02.213 | 0:00:12.0    | 224.0.1.129 | 319          | 192.168.10.193 | 319          | MCAST           | UDP              |           | -    | 20 124                | 234                      | 10 296            |
| 10.07.2024 10:00:41.213 | 10.07.2024 10:00:53.213 | 0:00:12.0    | 224.0.1.129 | 320          | 192.168.10.193 | 320          | MCAST           | UDP              |           | -    | 43 982                | 457                      | 24 788            |

Записей на странице: 50 | Всего 13 174 записи (259 страниц)

Из таблицы видно, что хост вовлечен в сравнительно интенсивный multicast трафик (13174 сессии за 24 часа) с использованием портов 319 и 320. Эти порты используются для сетевой синхронизации по протоколу **PTR** (Precision Time Protocol). Это подтверждает догадку об инфраструктурной роли этого хоста и подтверждает его важность, так как протокол PTR используется, как правило, для синхронизации критической инфраструктуры.

И, наконец, из детализации (всего один клик) любой сессии хоста 10.193 мы видим производителя сетевой интерфейса этого устройства «TQ-Components GmbH»:



Такие сетевые платы являются нетипичными для данной сети и свидетельствуют о том, что 192.168.10.193 является устройством, выполняющим специализированные функции.

## Резюме

- С помощью системы aVistar мы быстро увидели сессии http, внутри которых может передаваться чувствительная информация.
- Обнаружили среди сессий активное сетевое хост 10.193, в трафике которого через cookie передаётся сессионный ключ в открытом виде.
- Этот хост управляется внешним устройством по протоколу http.
- Дальнейшее исследование, что хост 10.193 представляет собой инфраструктурный элемент, активно участвующий в сетевой синхронизации с использованием протокола PTR.

## ВЫВОДЫ



В сети имеется инфраструктурный элемент, предположительно задействованный в процессах синхронизации по протоколу RTP.

Этот сетевой элемент управляется по незащищённому протоколу HTTP. В трафике в открытом виде передаётся информация, которую можно использовать для несанкционированного доступа к этому инфраструктурному элементу.

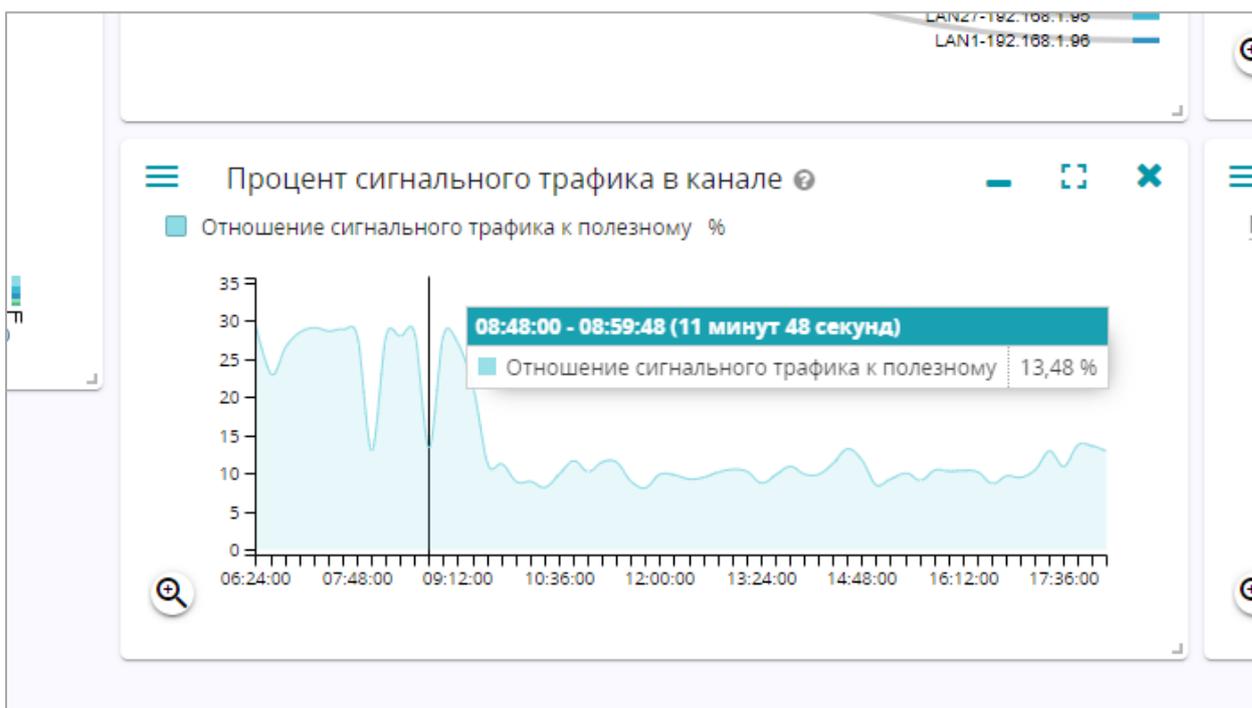
Управление этим элементом выполняется внешним Java-агентом.



**ВРЕМЯ:** Время от обнаружения на дашборде системы aVistardo принятия решения по дальнейшим шагам составило **около 2 минут**.

## #5. Подозрение на атаки типа «отказ в обслуживании»

Большой трафик без полезной нагрузки (payload), или с минимальной нагрузкой



Проседание доли сигнального трафика на этом виджете совпадает с началом рабочего дня и не является признаком DOS-атак.

## #6. Быстрый обзор серверных логических портов

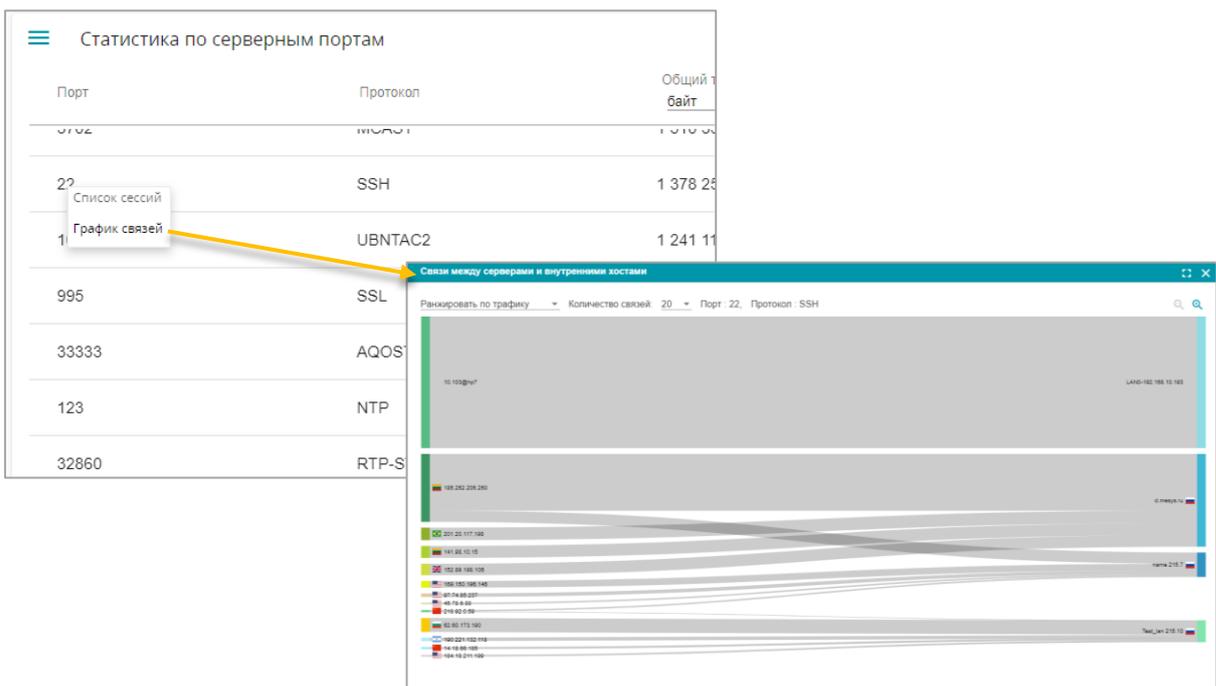
Информация о задействованных логических портах на внешних и внутренних серверах может дать дополнительное представление о возможных инцидентах. Система aVistar показывает эту информацию на специальном виджете «Статистика по серверным портам»:

| Порт  | Протокол | Общий трафик<br>байт | Сессий |
|-------|----------|----------------------|--------|
| 319   | MCAST    | 2 477 746            | 138    |
| 50360 | UNKNOWN  | 2 336 176            | 93     |
| 3702  | MCAST    | 2 236 432            | 41     |
| 137   | NETBIOS  | 1 711 405            | 200    |
| 3389  | RDP      | 1 369 092            | 68     |
| 10001 | UBNTAC2  | 1 181 061            | 355    |
| 5358  | UNKNOWN  | 1 141 847            | 17     |

Записей на странице: 100 << < 1 >

Виджет связывает логические порты и сервисы, которые детектированы на них с объемом трафика.

С помощью вертикального (drill-down) анализа, реализованного на этом виджете, легко увидеть ещё и связи этих серверных логических портов, с клиентами:

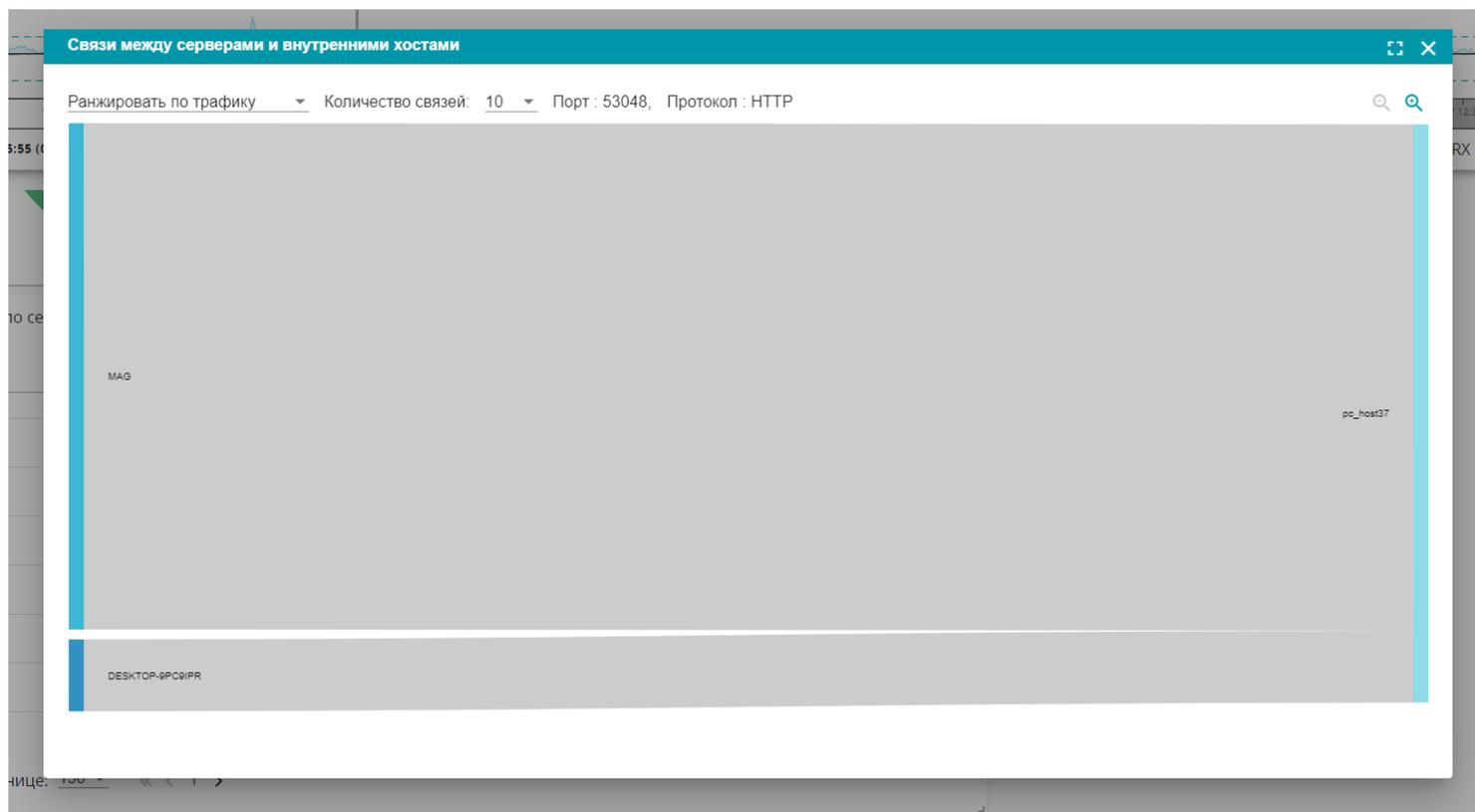


**Пример.** На таком виджете удобно заметить и проанализировать трафик, где протоколы используют нестандартные порты, или нераспознанный системой трафик.

| Порт ↑ | Протокол | Общий трафик<br>байт | Сессий |
|--------|----------|----------------------|--------|
| 53048  | UNKNOWN  | 392 803              | 9      |
| 53048  | HTTP     | 64 963               | 11     |
| 52841  | FTP_DATA | 1 320                | 1      |

Шаг 1. Отсортируем трафик на виджете по убыванию портов. На примере выше, мы заметили, что протокол HTTP использует нестандартный порт 53048.

Шаг 2. Посмотрим, где проявился такой нестандартный трафик на диаграмме связей:



Из диаграммы выше видно, что в сессиях участвовали три хоста из внутренней LAN предприятия.

Шаг 4. Посмотрим детализацию сессий (один клик) с участием этого нестандартного трафика:

Список IP сессий за выбранный период

Все сессии

HTTP Сервер :53048 Клиент :Порт

|   | Время начала            | Время завершения        | Длительность | Сервер       | Порт сервера | Клиент       | Порт клиента | Протокол/Сервис | Трансп. протокол | Флаги TCP | VLAN | Суммарное кол-во байт | Суммарное кол-во пакетов | Суммарный payload |
|---|-------------------------|-------------------------|--------------|--------------|--------------|--------------|--------------|-----------------|------------------|-----------|------|-----------------------|--------------------------|-------------------|
| ⚠ | 12.07.2024 12:32:39.111 | 12.07.2024 12:32:39.362 | 0:00:00.250  | 192.168.1.86 | 53048        | 192.168.1.43 | 55068        | HTTP            | TCP              | SAPF      | 100  | 1 736                 | 6                        | 1 376             |
| ⚠ | 12.07.2024 12:32:38.639 | 12.07.2024 12:32:38.890 | 0:00:00.250  | 192.168.1.86 | 53048        | 192.168.1.43 | 55063        | HTTP            | TCP              | SAPF      | 100  | 1 736                 | 6                        | 1 376             |
| ⚠ | 12.07.2024 12:32:38.541 | 12.07.2024 12:32:38.793 | 0:00:00.251  | 192.168.1.86 | 53048        | 192.168.1.43 | 55062        | HTTP            | TCP              | SAPF      | 100  | 1 736                 | 6                        | 1 376             |
| ⚠ | 12.07.2024 12:32:38.342 | 12.07.2024 12:32:38.594 | 0:00:00.251  | 192.168.1.86 | 53048        | 192.168.1.43 | 55061        | HTTP            | TCP              | SAPF      | 100  | 1 736                 | 6                        | 1 376             |
| ⚠ | 12.07.2024 12:32:38.250 | 12.07.2024 12:32:38.500 | 0:00:00.250  | 192.168.1.86 | 53048        | 192.168.1.43 | 55060        | HTTP            | TCP              | SAPF      | 100  | 1 736                 | 6                        | 1 376             |
| ⚠ | 12.07.2024 12:28:59.324 | 12.07.2024 12:28:59.881 | 0:00:00.557  | 192.168.1.86 | 53048        | 192.168.1.50 | 54537        | HTTP            | TCP              | SAPF      | 100  | 1 736                 | 6                        | 1 376             |
| ⚠ | 12.07.2024 12:28:58.968 | 12.07.2024 12:28:59.527 | 0:00:00.559  | 192.168.1.86 | 53048        | 192.168.1.50 | 54536        | HTTP            | TCP              | SAPF      | 100  | 1 736                 | 6                        | 1 376             |
| ⚠ | 12.07.2024 12:28:58.874 | 12.07.2024 12:28:59.125 | 0:00:00.250  | 192.168.1.86 | 53048        | 192.168.1.50 | 54535        | HTTP            | TCP              | SAPF      | 100  | 1 736                 | 6                        | 1 376             |
| ⚠ | 12.07.2024 12:28:58.9   | 12.07.2024 12:28:58.560 | 0:00:00.551  | 192.168.1.86 | 53048        | 192.168.1.50 | 54533        | HTTP            | TCP              | SAPF      | -    | 47 603                | 225                      | 35 309            |
| ⚠ | 12.07.2024 12:28:57.978 | 12.07.2024 12:28:58.530 | 0:00:00.551  | 192.168.1.86 | 53048        | 192.168.1.50 | 54532        | HTTP            | TCP              | SAPF      | 100  | 1 736                 | 6                        | 1 376             |

Записей на странице: 50 << < 1 > >> Всего 11 записей (1 страница)

Шаг 5. Всего детектировано 11 сессий. Посмотрим, что было передано в сессии с наибольшим количеством переданных данных (47603 байт). Из таблицы выше видно, что данные в этой сессии передавались в другом VLAN'е, чем в других аналогичных сессиях:

Параметры сессии по интерфейсу "i5\_cube"

Начало: 12.07.2024 12:28:58.9  
Завершение: 12.07.2024 12:28:58.560

В текущий момент времени сессия завершена (Состояние: Завершилась успешно)

сервер 192.168.1.86:53048 HTTP / TCP клиент 192.168.1.50:54533  
MAG

- VLAN -
- ToS 0
- CoS 0

Не показывать пустые значения

Трафик QoS / QoE HTTP Нарушения трафика Дополнительно

Http application context application/soap+xml

Http url http://192.168.1.86:53048/

Http user agent WSDAPI

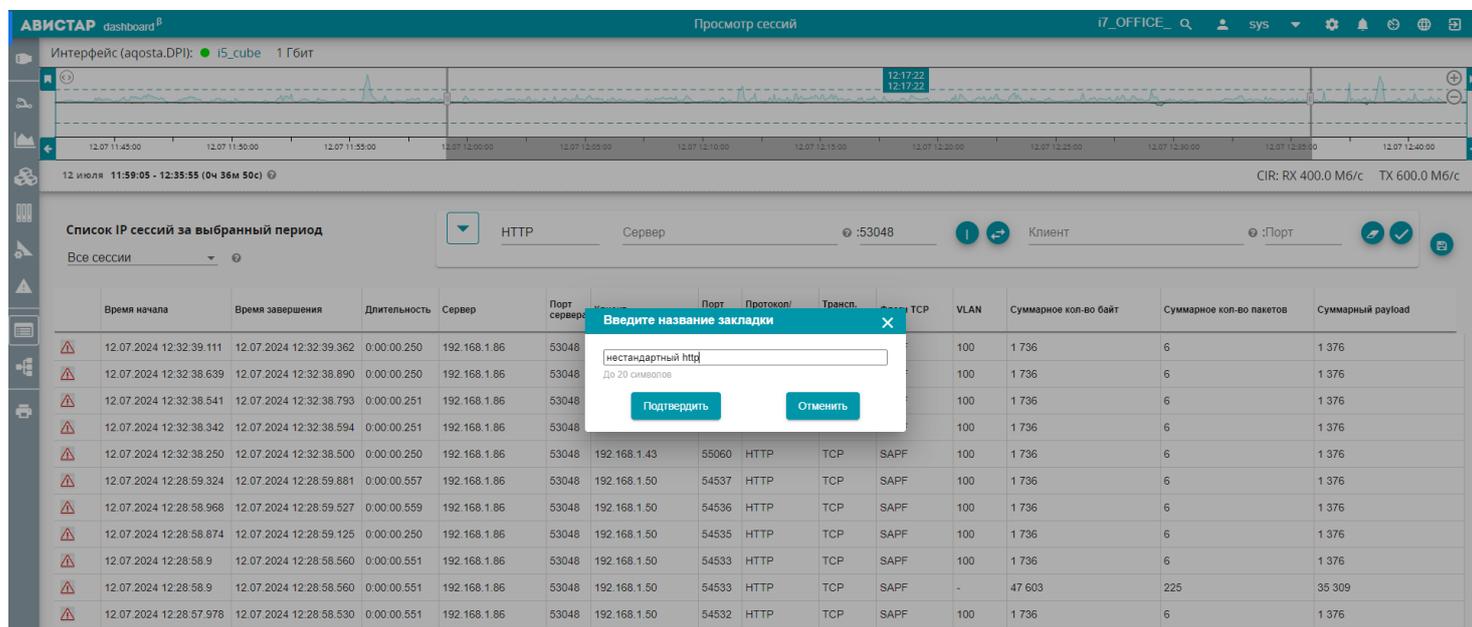
Request method POST

Закрыть

Из детализации становится понятным, что это трафик WSDAPI поверх HTTP. Однако по умолчанию WSDAPI использует TCP-порт 5357.

Шаг 6. Этот случай требует дополнительной проверки всех хостов, где используется нестандартная реализация WSDAPI/HTTP/TCP.

Пока мы ставим на таймлайне закладку (верхний виджет на экране), чтобы потом быстро вернуться к этому событию в любое другое время:



**ВЫВОД.** Встроенные средства анализ помогают быстро визуально увидеть аномалии с задействованными логическими портами. Мы можем легко убедиться, что аномалия не является подозрительной, либо эскалировать дальнейшие действия по расследованию и купированию проблемы.



**ВРЕМЯ:** Время от обнаружения на дашборде системы aVistar до принятия решения по дальнейшим шагам составило **около 3 минут.**



## **aVistar/V**

это мгновенный взгляд на  
сложные информационные  
потоки с помощью DPI-сенсо-  
ров и гибкой системы  
дашбордов

## О компании-разработчике

Компания «Метрологические системы» является технологическим стартапом и участником Сколково.

Мы сфокусированы на решении актуальных проблем в области измерения качества на сетях передачи данных. В настоящее время мы занимаемся разработкой программно-аппаратных средств мониторинга трафика и синхронизации для операторов связи и предприятий.

### Контакты:



сайт с формой обратной связи:

[www.mesys.ru](http://www.mesys.ru)

электронная почта:

[getmail@mesys.ru](mailto:getmail@mesys.ru)

перейти на страницу  
продукта по QR-коду

