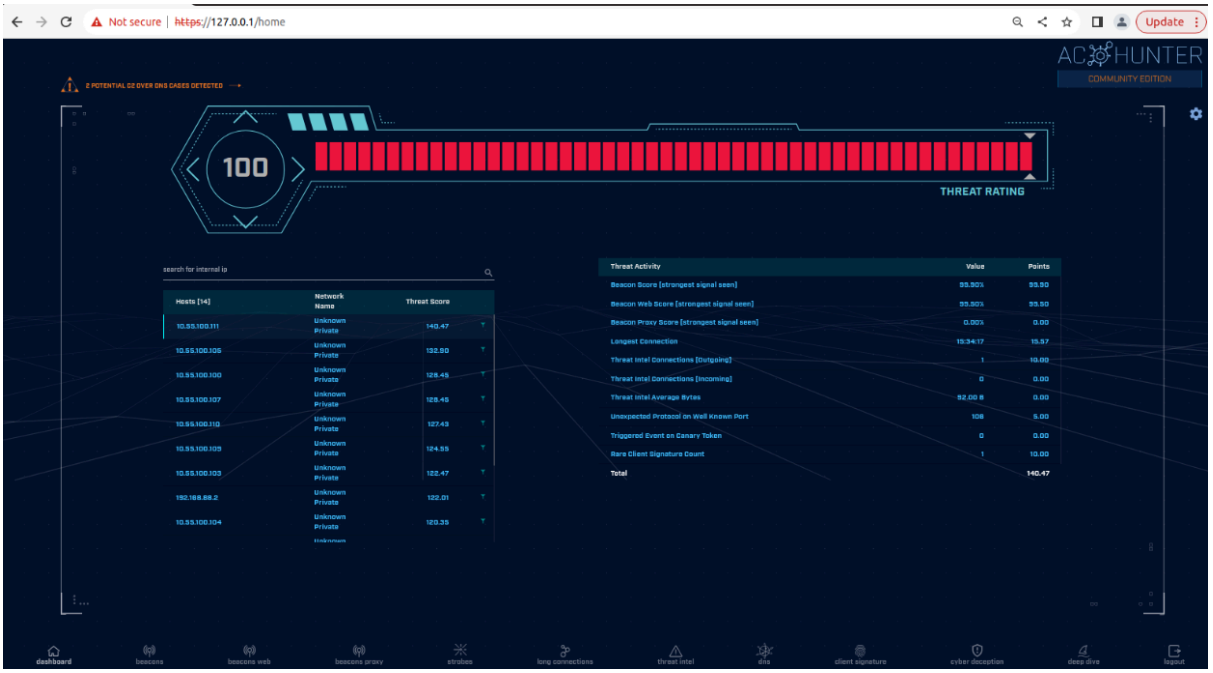
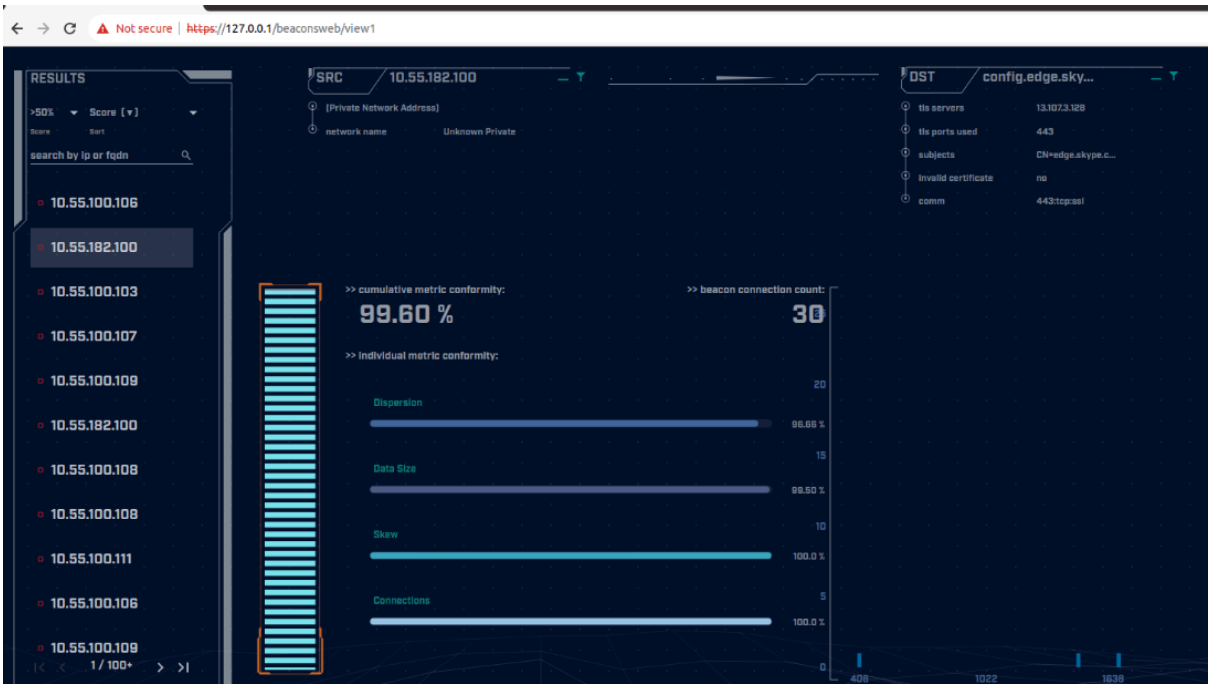
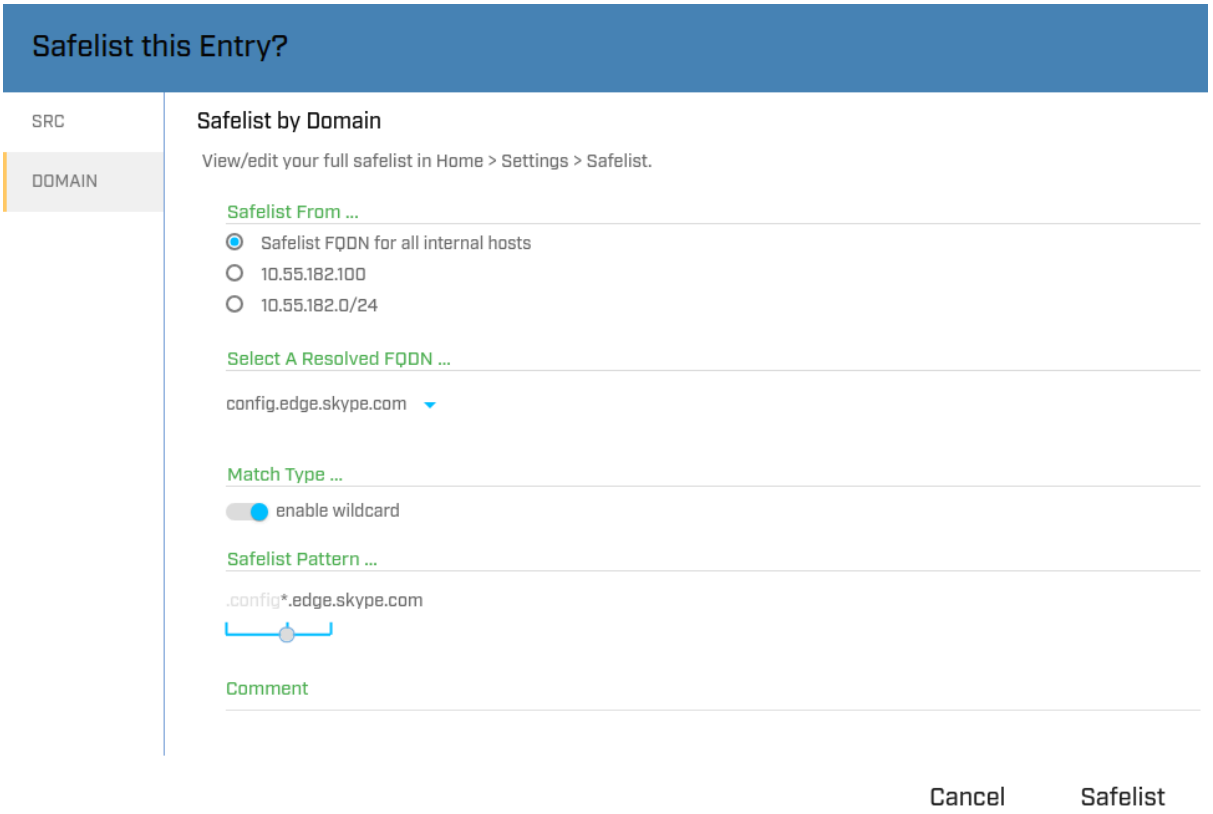
Практическая работа №4. Network Threat Hunting
Выполнил студент группы ББМО-01-23 Асатрян Д.Р.

Выбранная БД

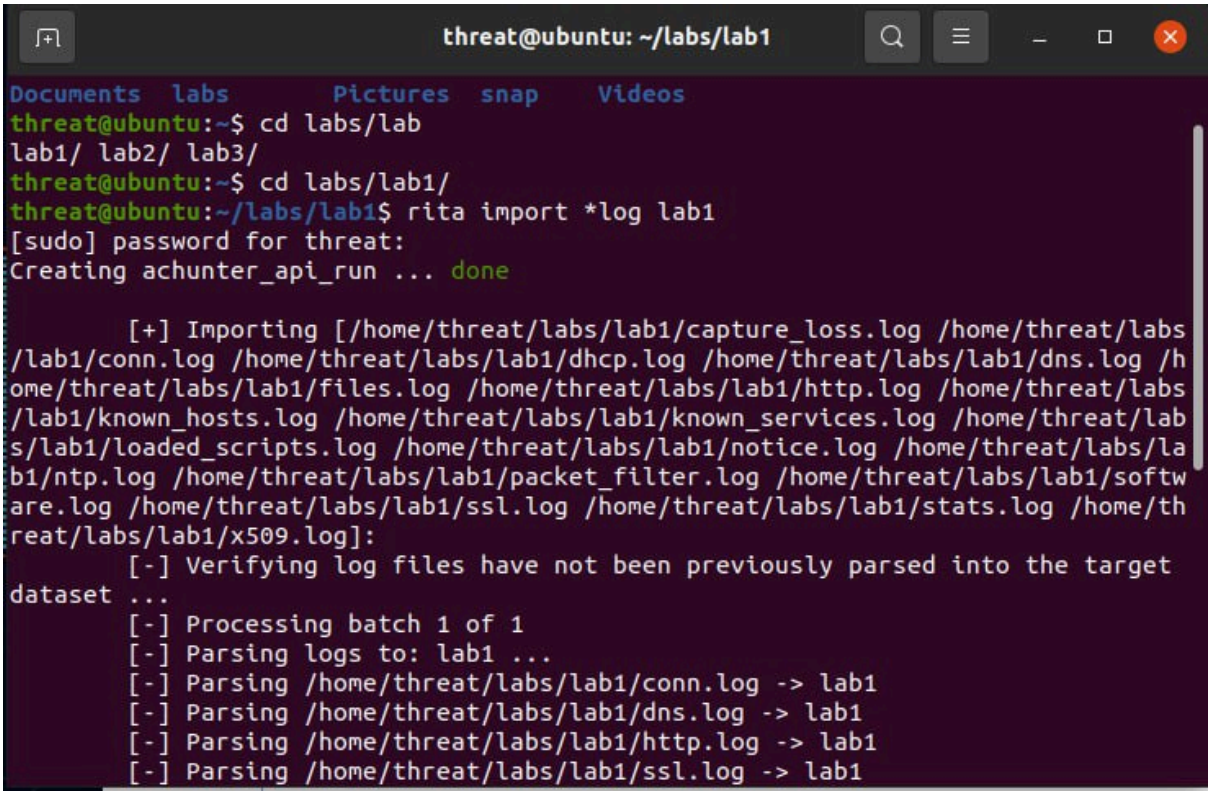


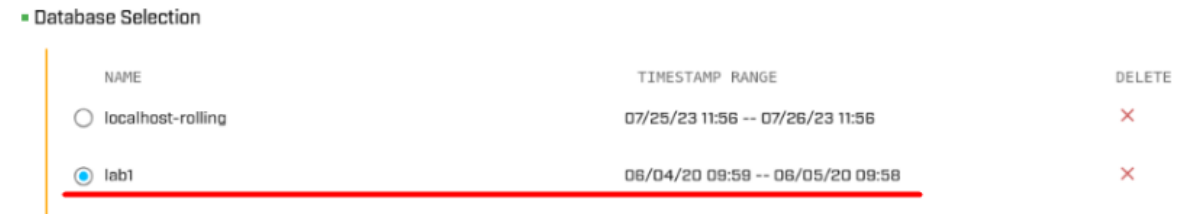
Добавление в safelist адреса скайп



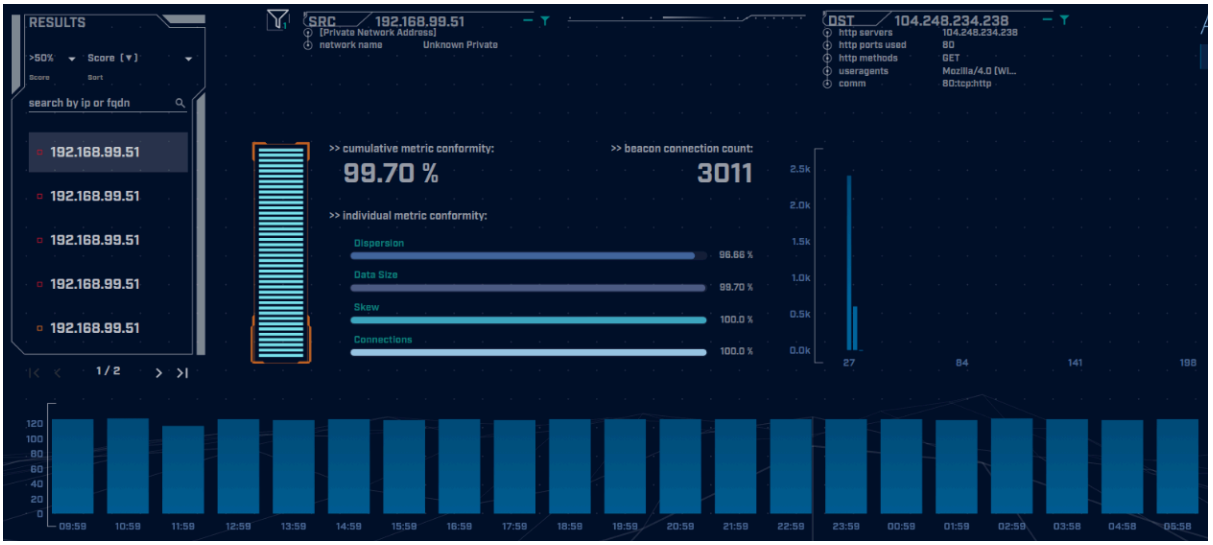


Импорт логов 1



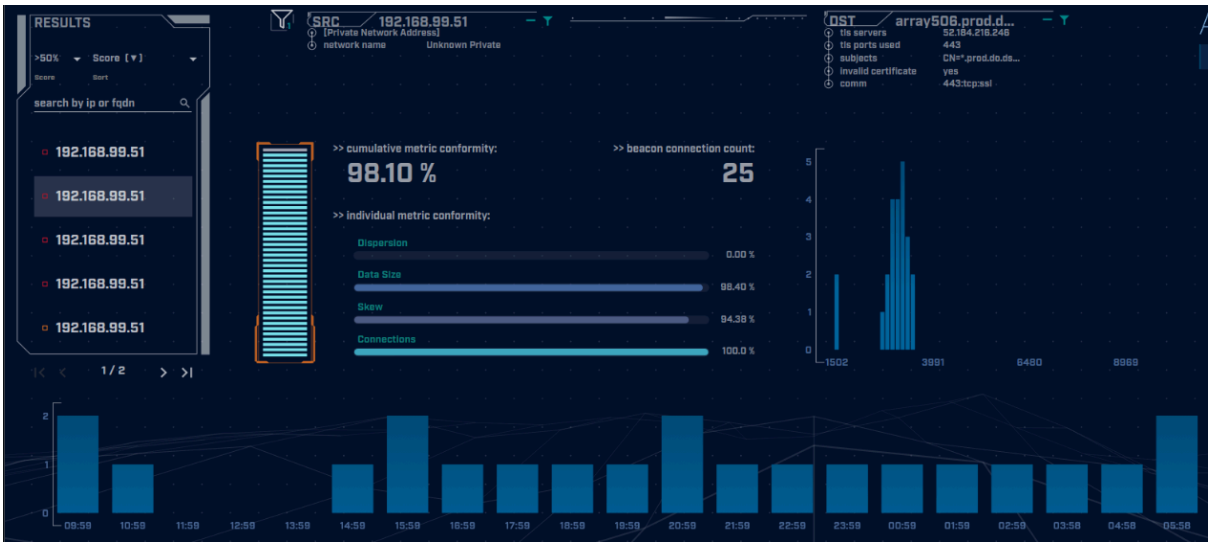


Первая запись



- Большое количество подключений за последние 24 часа (3 011)
- Ровная гистограмма
- Отсутствует строка хостинга. Необходимо указать полное доменное имя

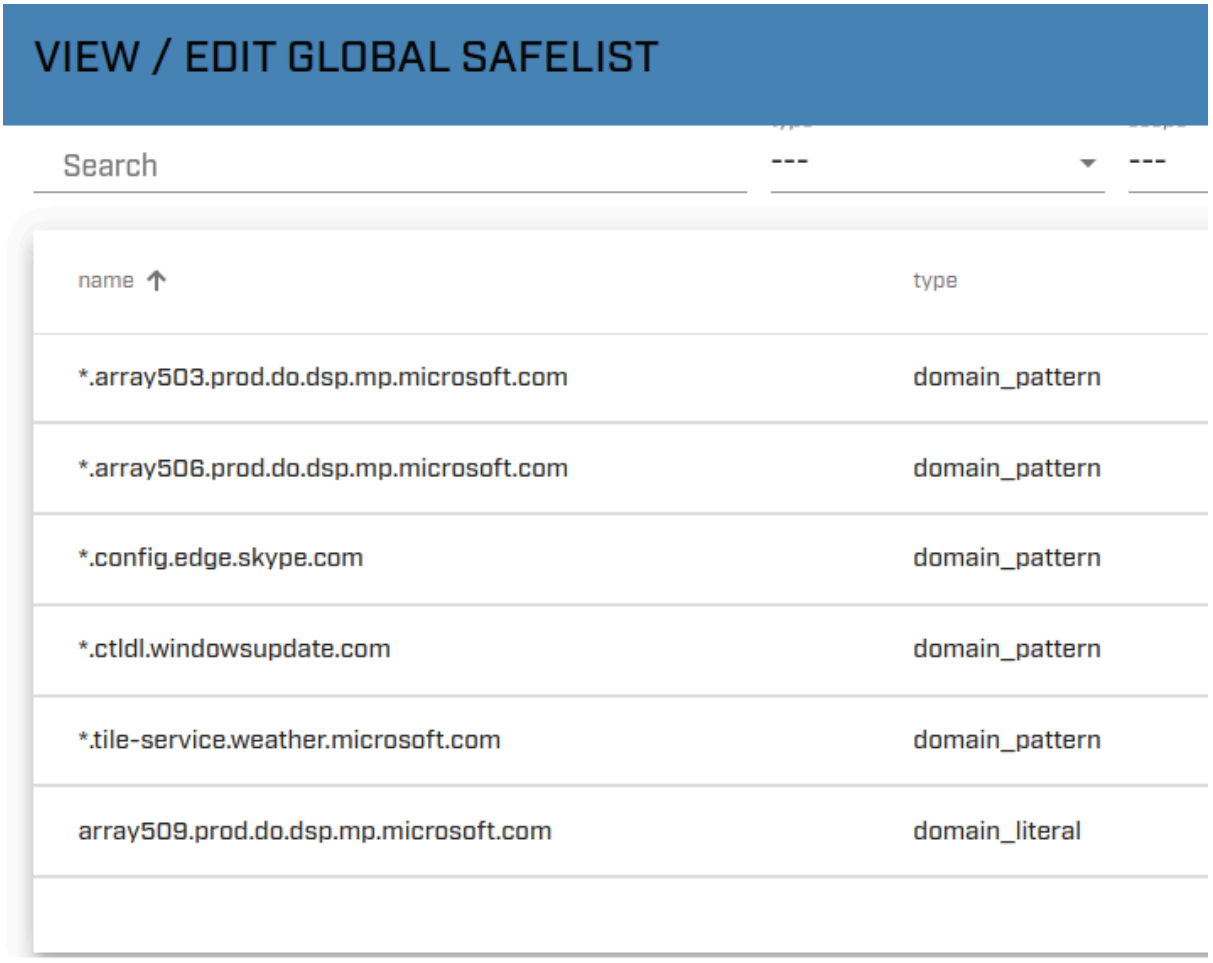
Вторая запись



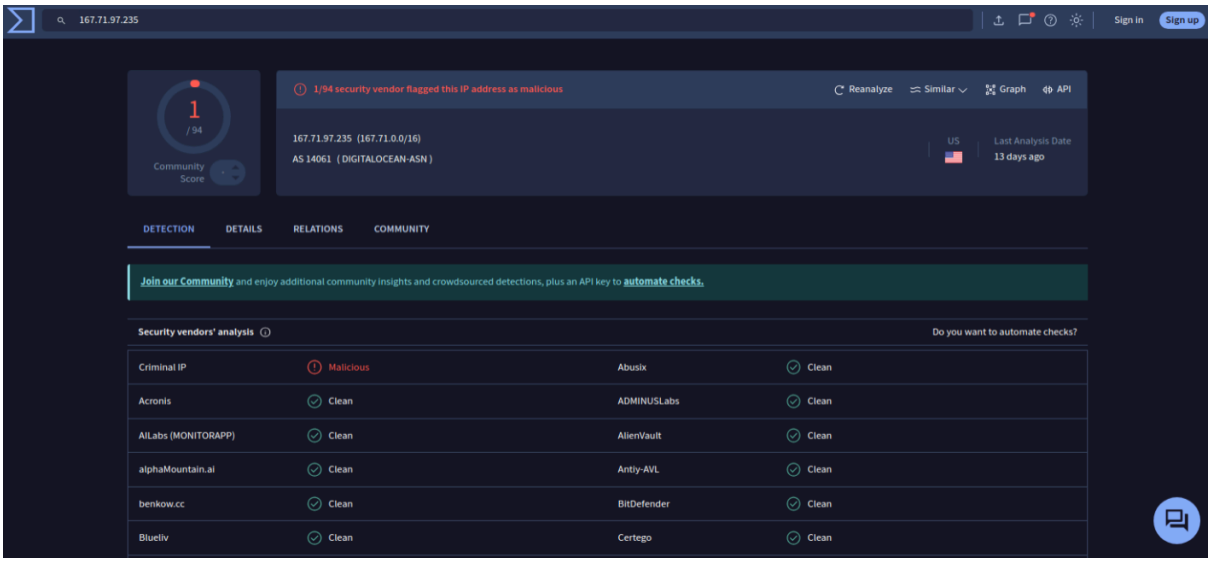
- Является узлом оптимизации доставки MS, который используется для установки исправлений.
- Цифровой сертификат вполне легитимный, следовательно, можно внести данную запись в safelist.

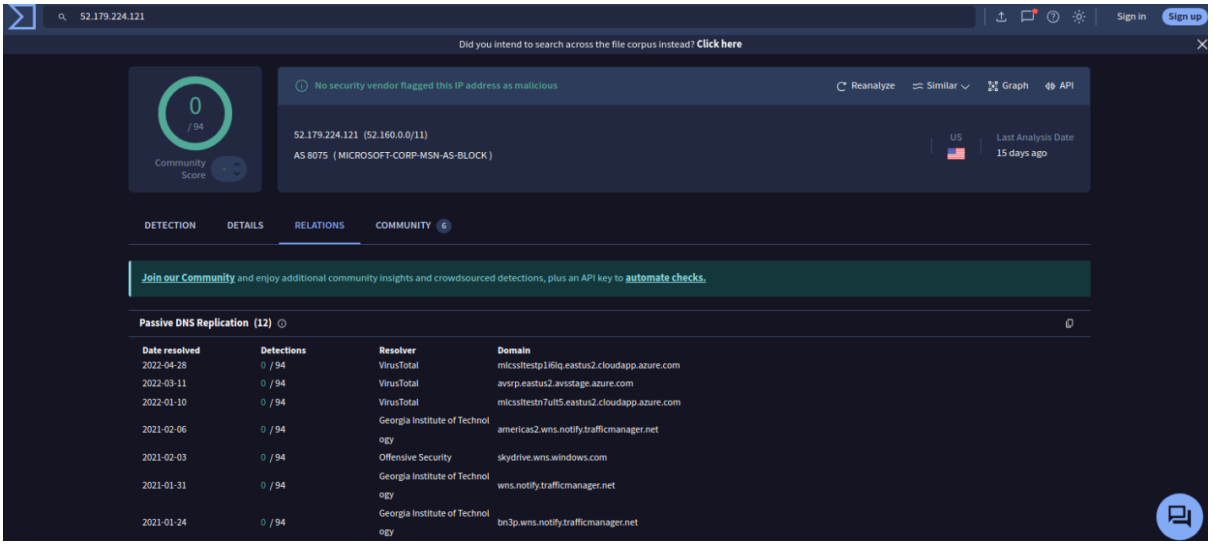
Третья запись

Итог safelist

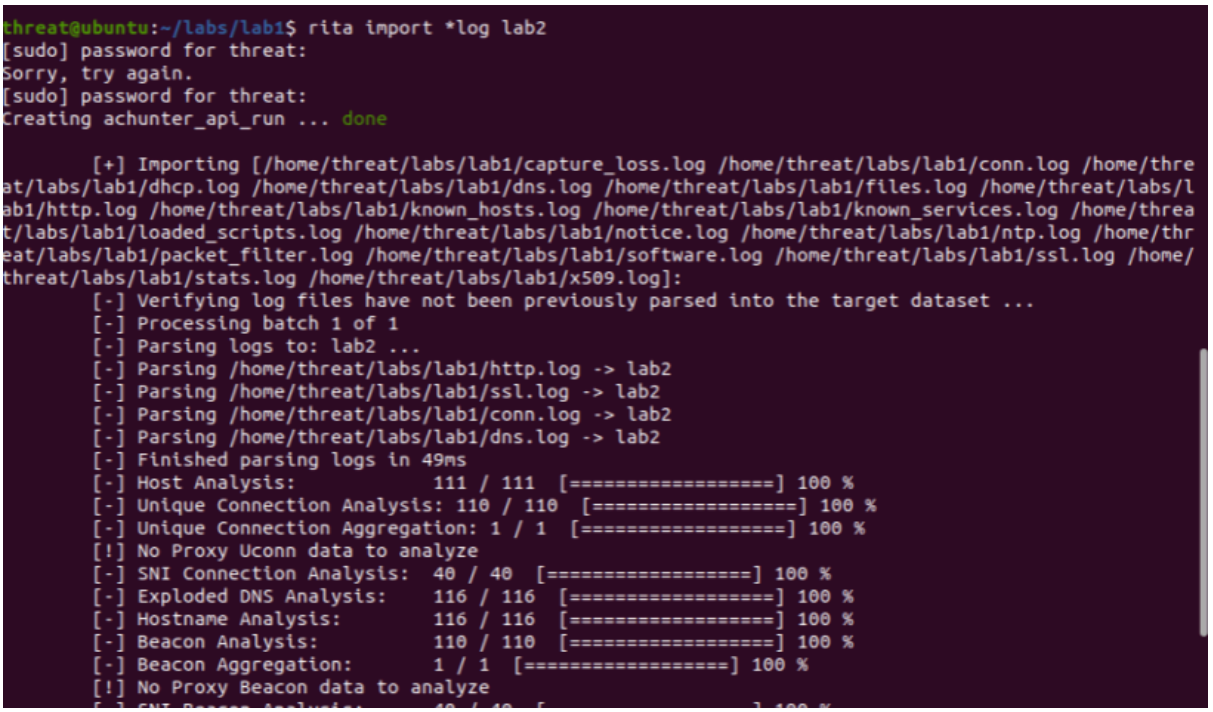


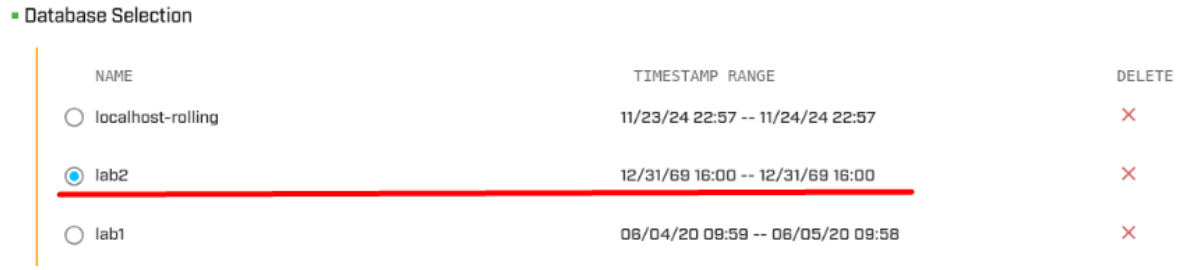
Просмотр записей с помощью VirusTotal





Импорт логов 2



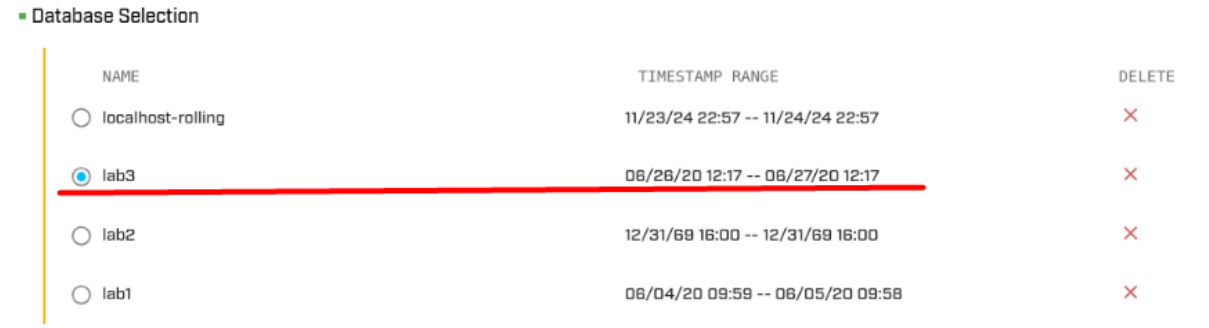


Можно заметить большое количество обращений на различные поддомены honestimnotevil.com. Это может указывать на потенциальный C2 через DNS.

Импорт логов 3

```
threat@ubuntu:~/labs/lab1$ rita import *log lab3
Creating achunter_api_run ... done

       [+] Importing [/home/threat/labs/lab1/capture_loss.log /home/threat/labs/lab1/conn.log /home/threat/labs/lab1/dhcp.log
 /home/threat/labs/lab1/dns.log /home/threat/labs/lab1/files.log /home/threat/labs/lab1/http.log /home/threat/labs/lab1/known_
hosts.log /home/threat/labs/lab1/known_services.log /home/threat/labs/lab1/loaded_scripts.log /home/threat/labs/lab1/notice.lo
g /home/threat/labs/lab1/ntp.log /home/threat/labs/lab1/packet_filter.log /home/threat/labs/lab1/software.log /home/threat/lab
s/lab1/ssl.log /home/threat/labs/lab1/stats.log /home/threat/labs/lab1/x509.log]:
       [-] Verifying log files have not been previously parsed into the target dataset ...
       [-] Processing batch 1 of 1
       [-] Parsing logs to: lab3 ...
       [-] Parsing /home/threat/labs/lab1/conn.log -> lab3
       [-] Parsing /home/threat/labs/lab1/dns.log -> lab3
       [-] Parsing /home/threat/labs/lab1/http.log -> lab3
       [-] Parsing /home/threat/labs/lab1/ssl.log -> lab3
       [-] Finished parsing logs in 89ms
       [-] Host Analysis:              111 / 111  [==================] 100 %
       [-] Unique Connection Analysis: 110 / 110  [==================] 100 %
       [-] Unique Connection Aggregation: 1 / 1  [==================] 100 %
       [!] No Proxy Uconn data to analyze
       [-] SNI Connection Analysis:  40 / 40  [==================] 100 %
       [-] Exploded DNS Analysis:    116 / 116  [==================] 100 %
       [-] Hostname Analysis:        116 / 116  [==================] 100 %
       [-] Beacon Analysis:          110 / 110  [==================] 100 %
       [-] Beacon Aggregation:       1 / 1  [==================] 100 %
       [!] No Proxy Beacon data to analyze
       [-] SNI Beacon Analysis:      40 / 40  [==================] 100 %
       [-] SNI Beacon Aggregation:   1 / 1  [==================] 100 %
       [-] UserAgent Analysis:       8 / 8  [==================] 100 %
       [-] UserAgent Aggregation:    8 / 8  [==================] 100 %
       [-] Invalid Cert Analysis:    24 / 24  [==================] 100 %
       [-] Indexing log entries ...
       [-] Updating metadatabase ...
       [-] Done!
```



Данная запись нестандартна для домен “Skype”

Просмотр записи через VirusTotal