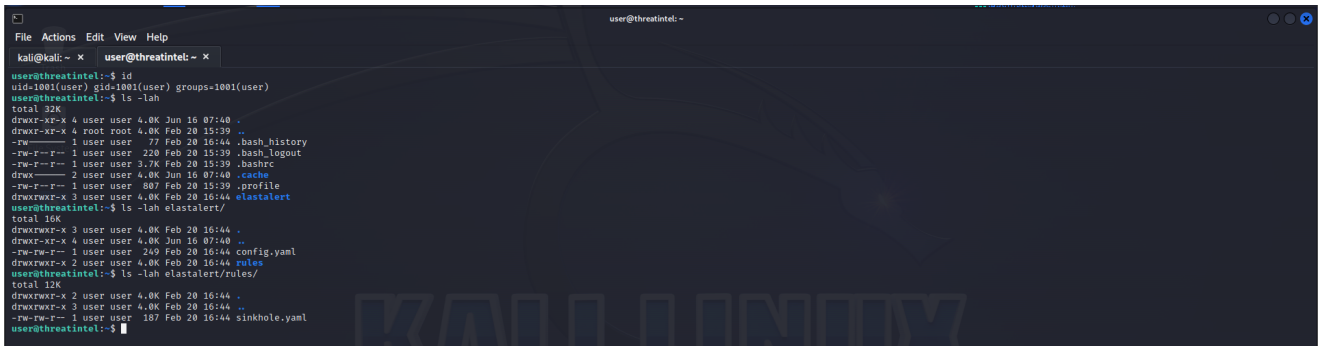
Threat Intelligence for SOC

[TryHackMe | Threat Intelligence for SOC]

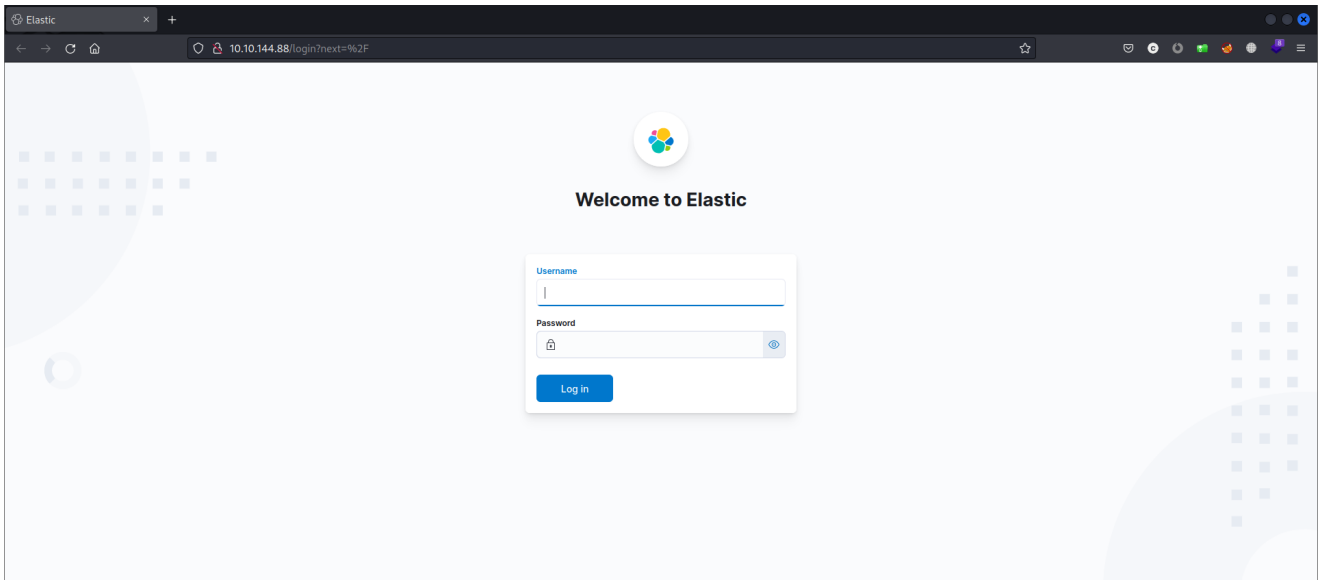
```
Learn how to utilise Threat Intelligence to improve the Security Operations pipeline.
```

```
ssh user@10.10.144.88
```

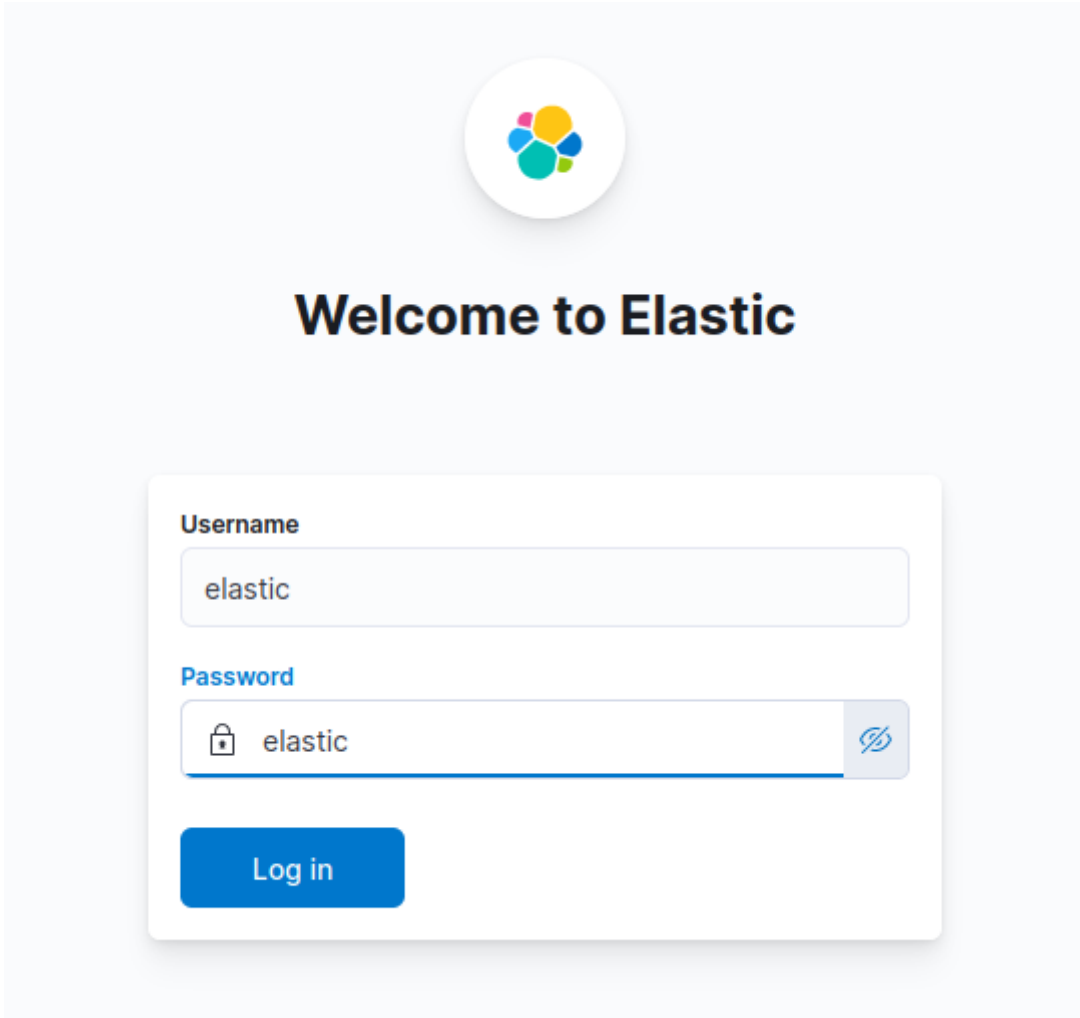
```
username: user
password: tryhackme
```

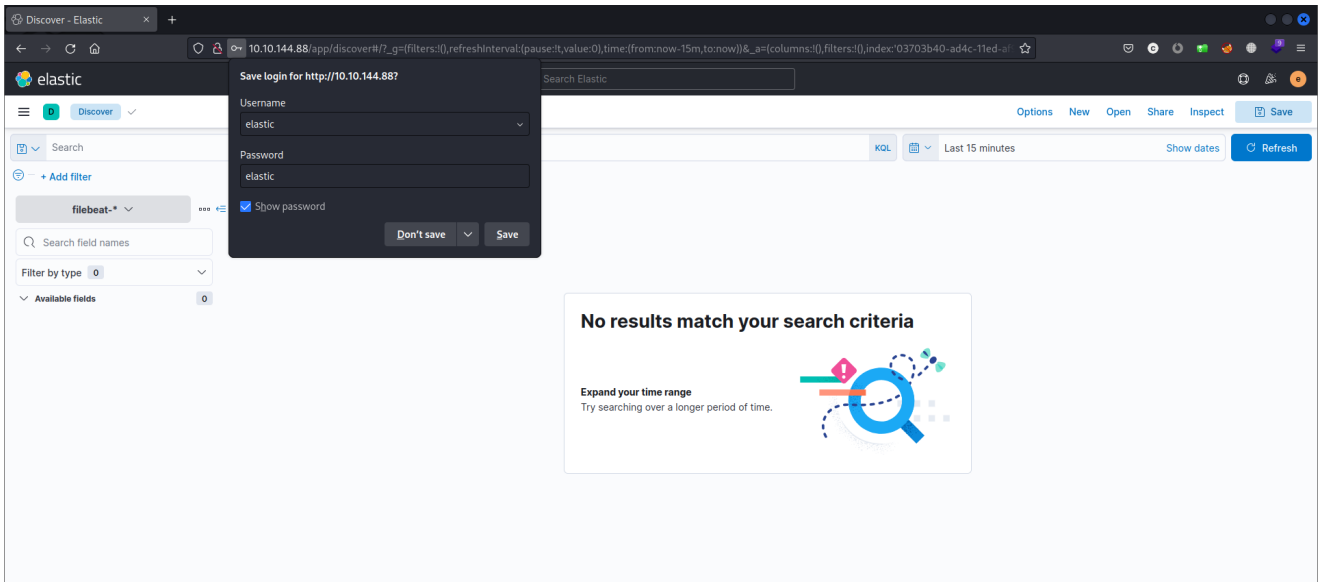



```
http://10.10.144.88/
```

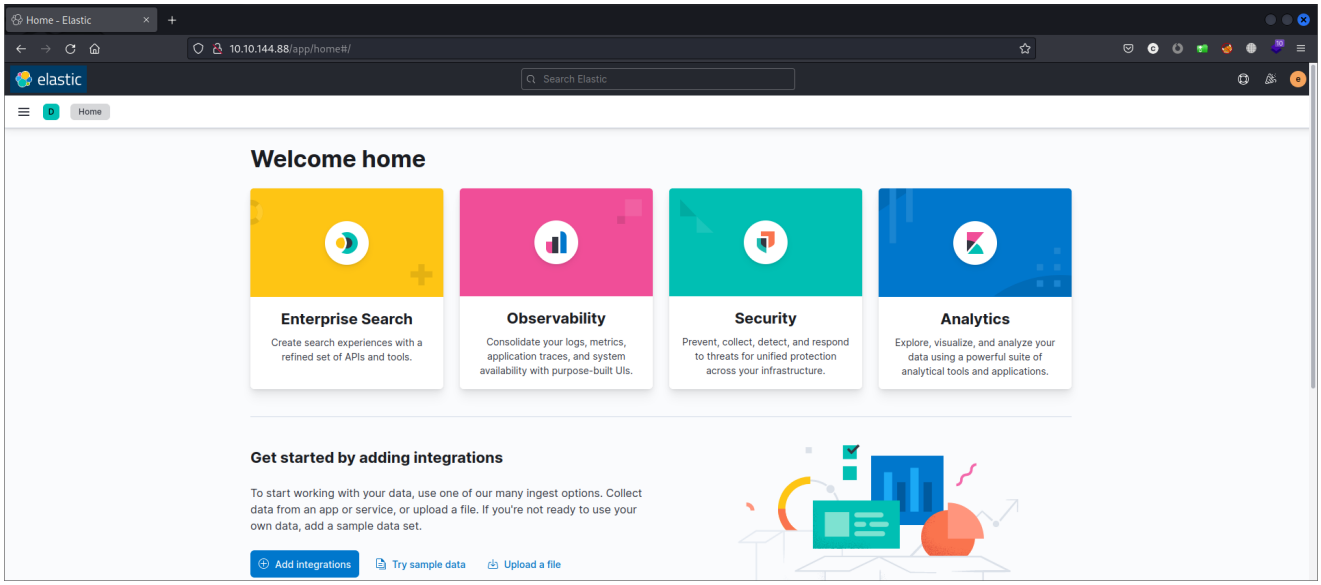


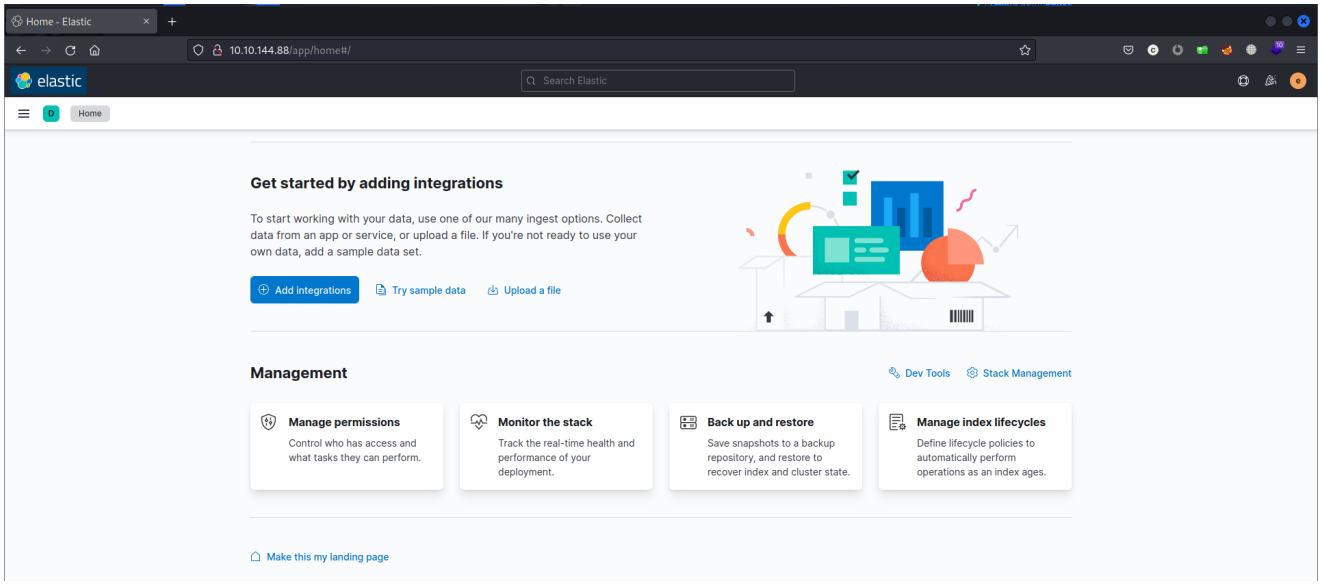
`elastic:elastic`






```
http://10.10.144.88/app/discover#/?_g=(filters:!(),refreshInterval:
(pause:!t,value:0),time:(from:now-15m,to:now))&_a=(columns:!(),filters:!
(),index:'03703b40-ad4c-11ed-af96-59e340b1e912',interval:auto,query:
(language:kuery,query:''),sort:!(!('@timestamp',desc)))
```





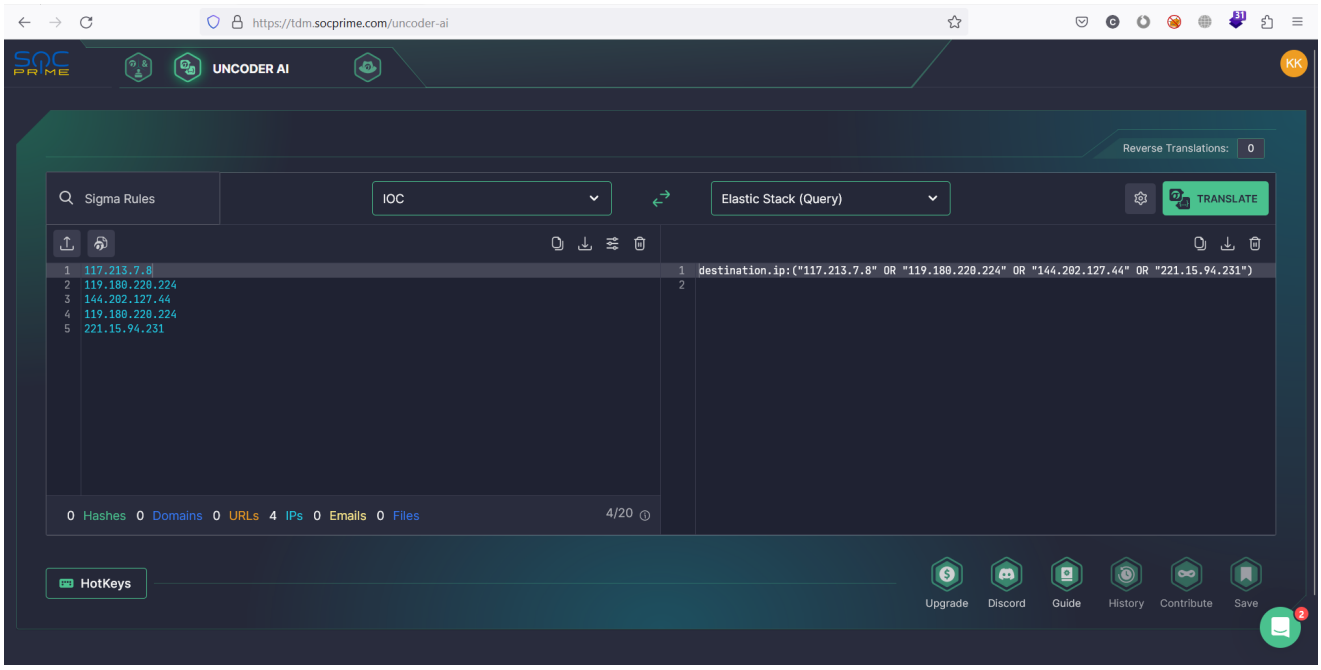
[Uncoder.IO | Universal Sigma Rule Converter for SIEM, EDR, and NTDR]

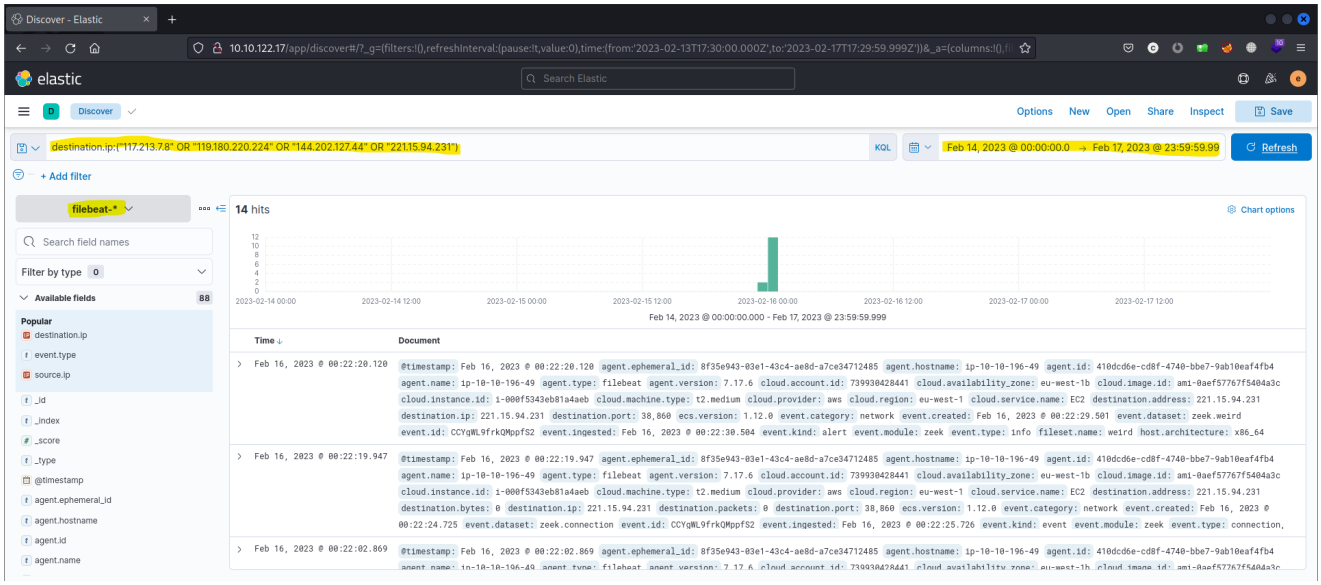
`ioc_list.txt`

```
117[.]213[.]7[.]8
119[.]180[.]220[.]224
144[.]202[.]127[.]44
119[.]180[.]220[.]224
221[.]15[.]94[.]231
```

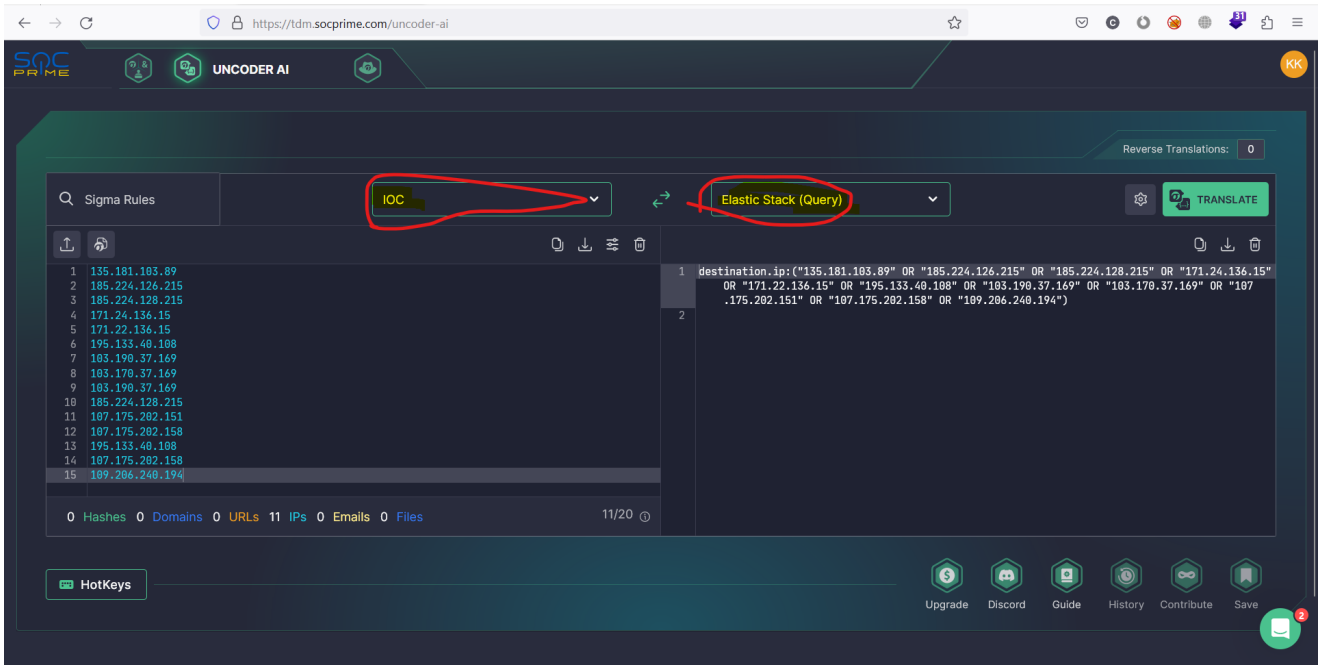
```
117.213.7.8
119.180.220.224
144.202.127.44
119.180.220.224
221.15.94.231
```

```
destination.ip:("117.213.7.8" OR "119.180.220.224" OR "144.202.127.44" OR
"221.15.94.231")
```

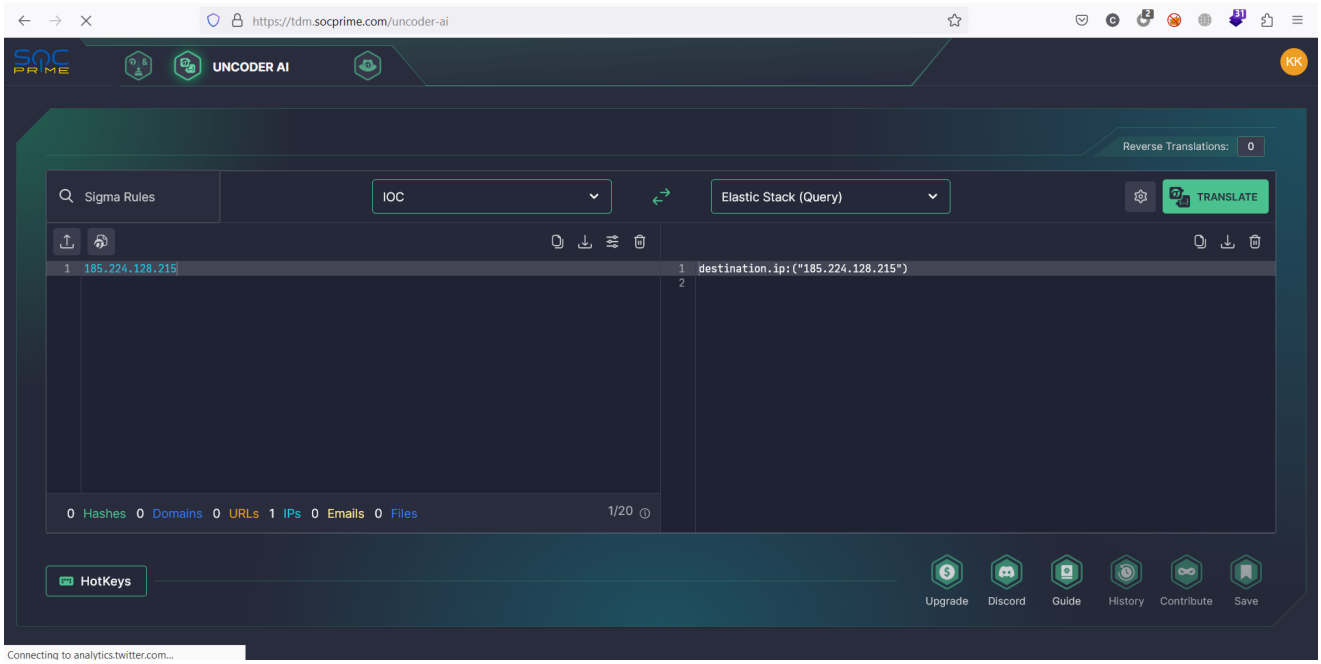





```
destination.ip:("135.181.103.89" OR "185.224.126.215" OR "185.224.128.215" OR "171.24.136.15" OR "171.22.136.15" OR "195.133.40.108" OR "103.190.37.169" OR "103.170.37.169" OR "107.175.202.151" OR "107.175.202.158" OR "109.206.240.194")
```

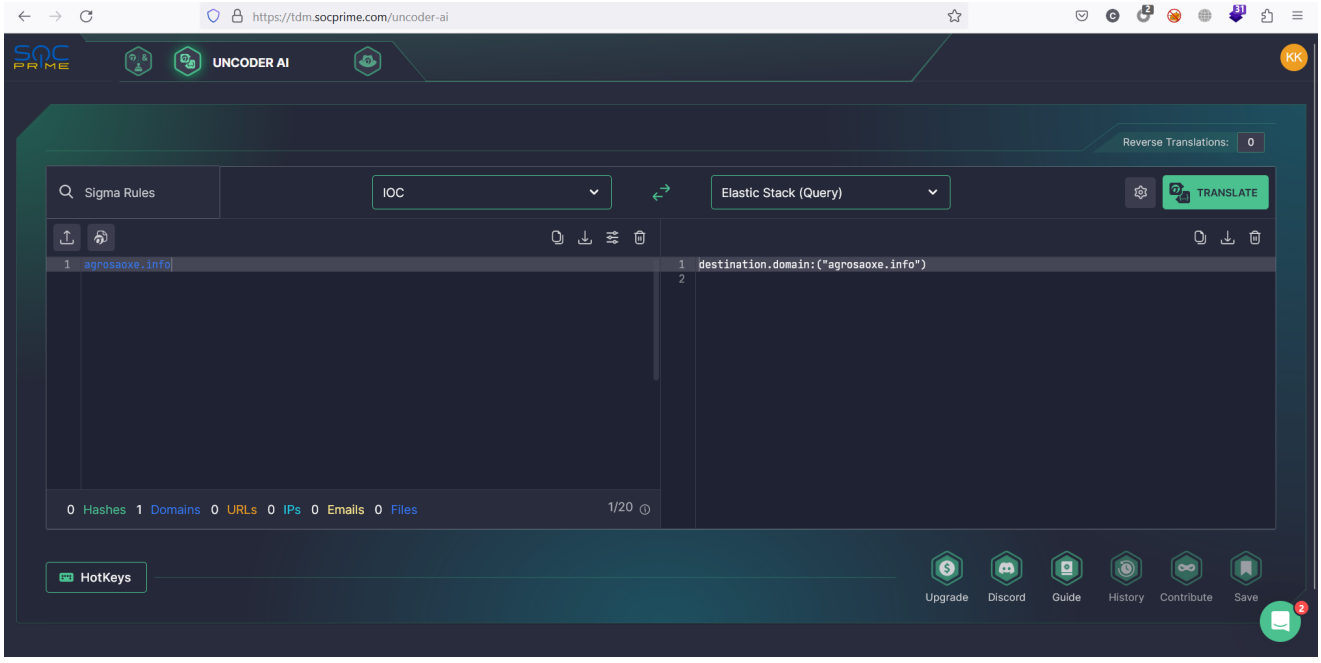



```
destination.ip:("185.224.128.215")
```




```
destination.ip:("107.175.202.151")
```

```
dns.question.name:"agrosaoxe.info"
```



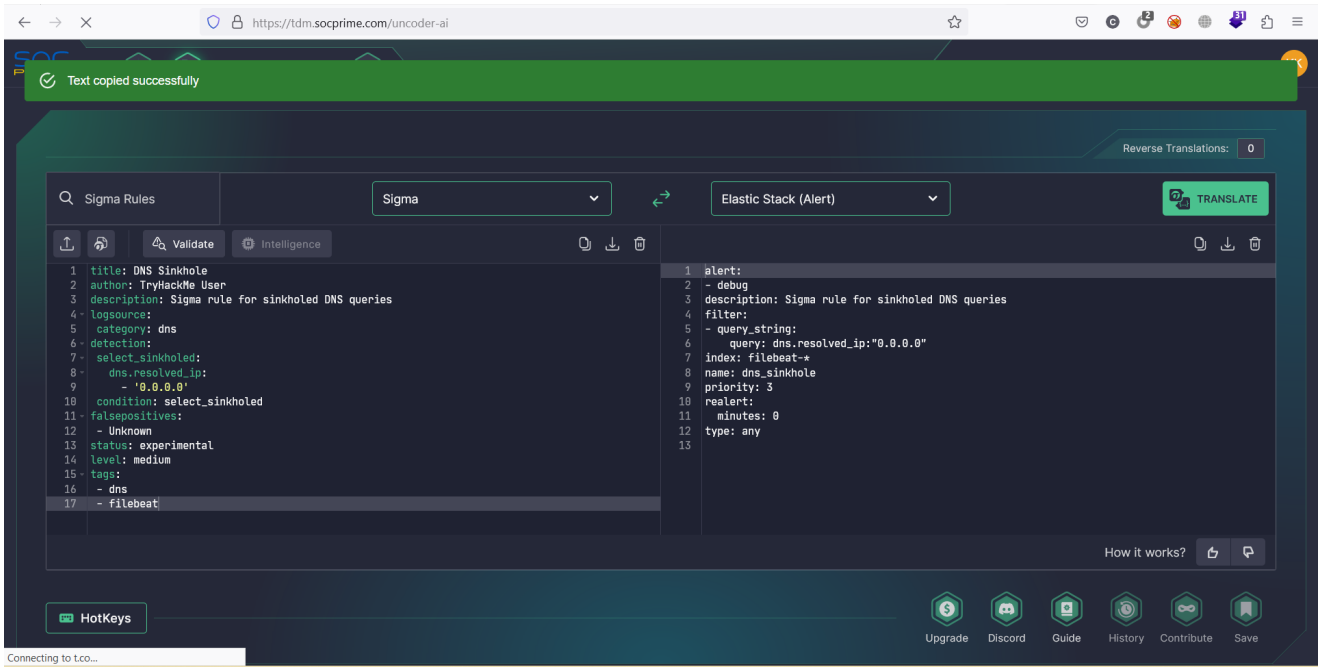

```
dns.answers.data: "0.0.0.0"
```

```
elastalert --start 2023-02-16T00:00:00 --verbose 2>&1 | tee output.txt
```

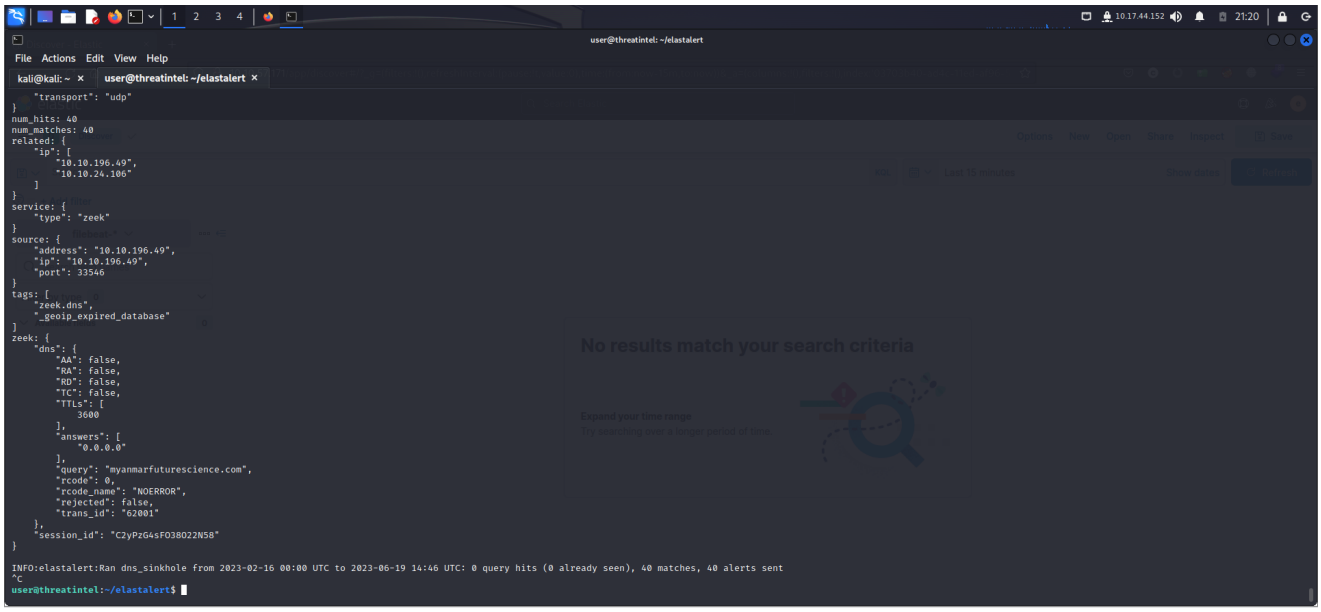
```
title: DNS Sinkhole
author: TryHackMe User
description: Sigma rule for sinkholed DNS queries
logsource:
```

```
 category: dns
detection:
 select_sinkholed:
   dns.resolved_ip:
     - '0.0.0.0'
 condition: select_sinkholed
falsepositives:
 - Unknown
status: experimental
level: medium
tags:
 - dns
 - filebeat
```

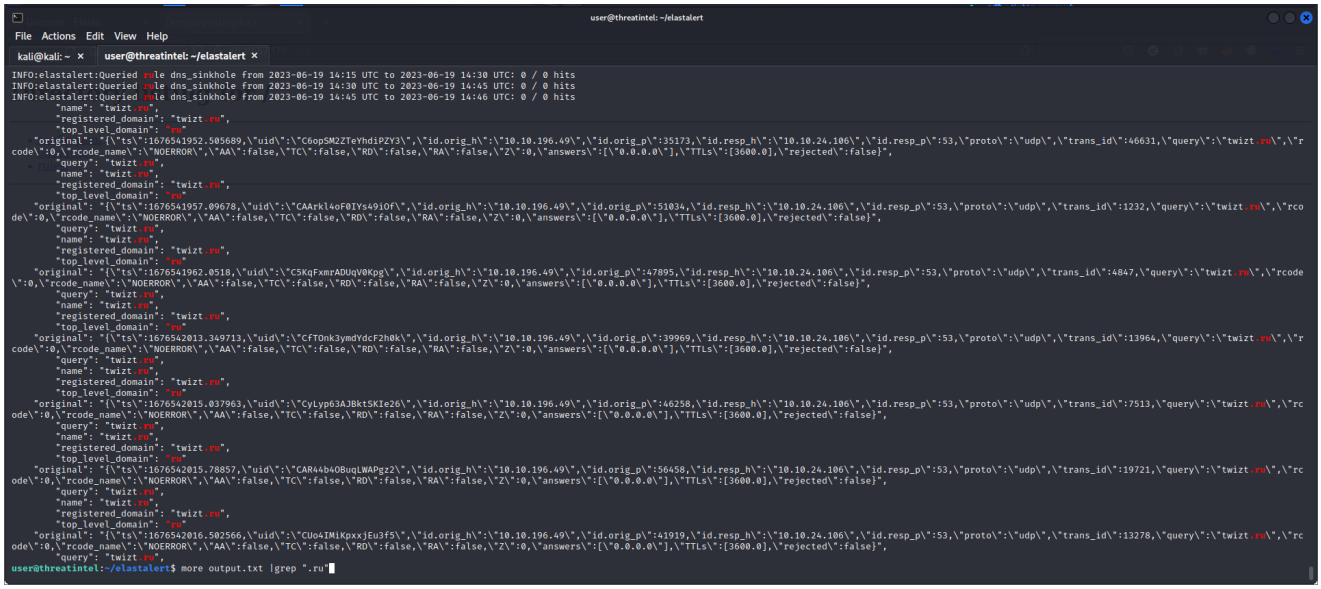
```
alert:
- debug
description: Sigma rule for sinkholed DNS queries
filter:
- query_string:
        query: dns.resolved_ip:"0.0.0.0"
index: filebeat-*
name: dns_sinkhole
priority: 3
realert:
        minutes: 0
type: any
```



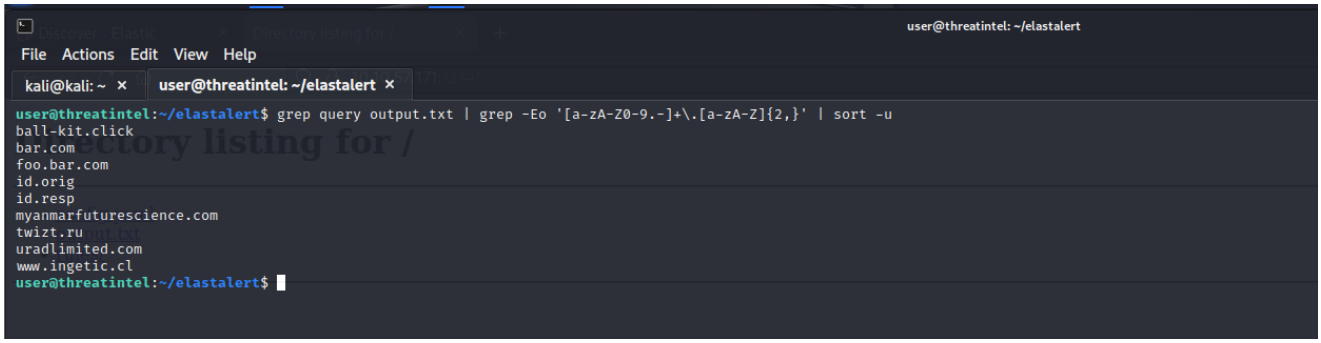
```
elastalert --start 2023-02-16T00:00:00 --verbose 2>&1 | tee output.txt
```

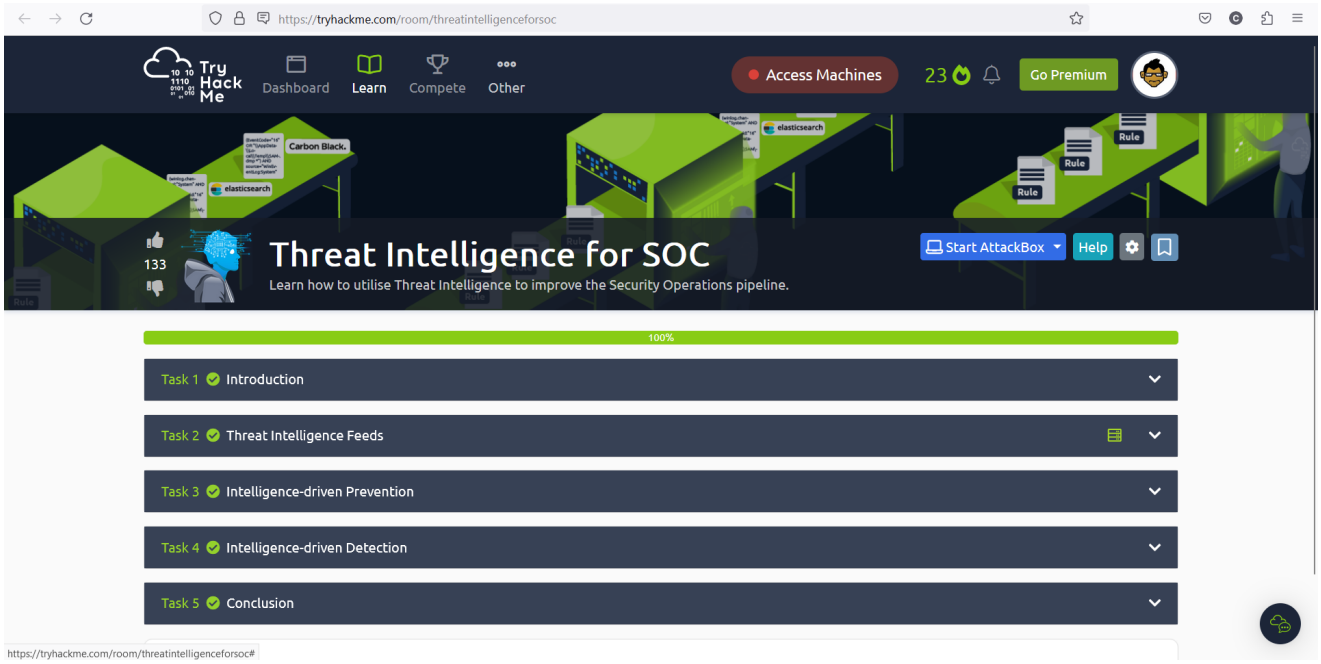



```
more output.txt |grep ".ru"
```




```
grep query output.txt | grep -Eo '[a-zA-Z0-9.-]+\.[a-zA-Z]{2,}' | sort -u
```




https://tryhackme.com/room/threatintelligenceforsoc
Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
23
Go Premium
Carbon Black.
elasticsearch
Rule
133
Threat Intelligence for SOC
Learn how to utilise Threat Intelligence to improve the Security Operations pipeline.
Start AttackBox
Help
100%
Task 1 Introduction
Task 2 Threat Intelligence Feeds
Task 3 Intelligence-driven Prevention
Task 4 Intelligence-driven Detection
Task 5 Conclusion
https://tryhackme.com/room/threatintelligenceforsoc#