

# 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

```
kali@kali: ~ - ssh: user@10.10.144.88
user@threatintel: ~
user@threatintel:~(~/threatintelligenceforsoc)
user@10.10.144.88
The authenticity of host '10.10.144.88 (10.10.144.88)' can't be established.
ED25519 key fingerprint is SHA256:LF7Hf3jRgzjPGrhGRhFIDQ2WYc+hIUIP+Sx8RWF1.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.144.88' (ED25519) to the list of known hosts.
user@10.10.144.88's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-1029-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Fri Jun 16 07:40:09 UTC 2023

System load: 1.96          Processes: 136
Usage of /: 23.5% of 19.32GB Users logged in: 0
Memory usage: 34%         IPv4 address for eth0: 10.10.144.88
Swap usage: 0%

 * Ubuntu Pro delivers the most comprehensive open source security and
  compliance features.

  https://ubuntu.com/aws/pro

128 updates can be installed immediately.
8 of these updates are security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

3 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log

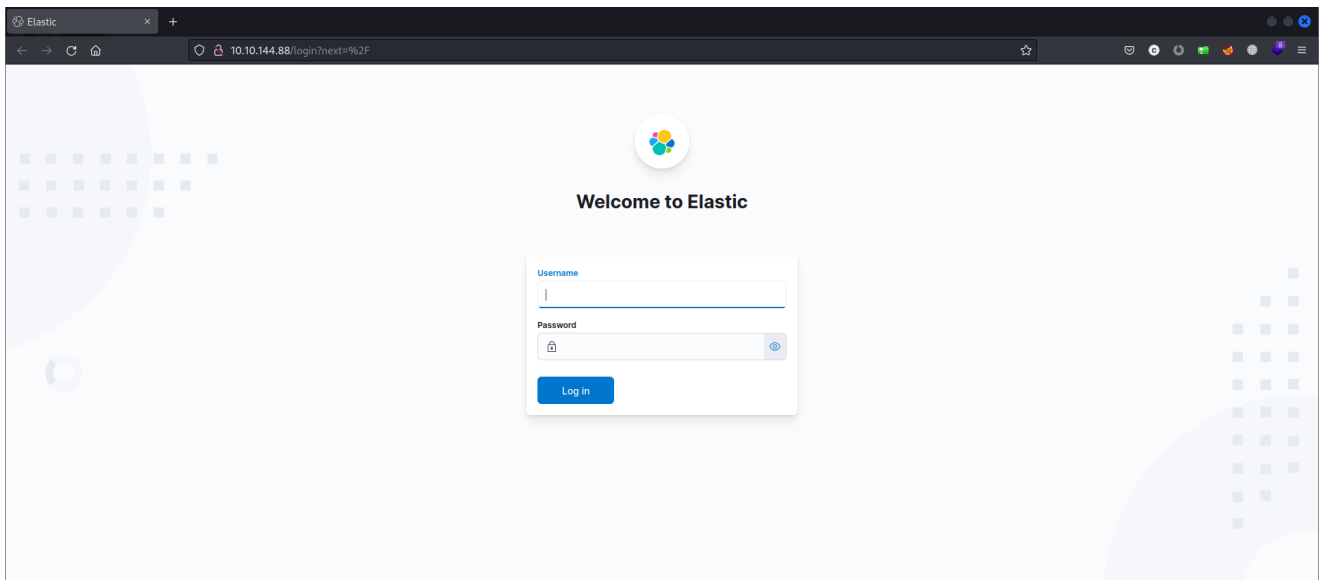
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

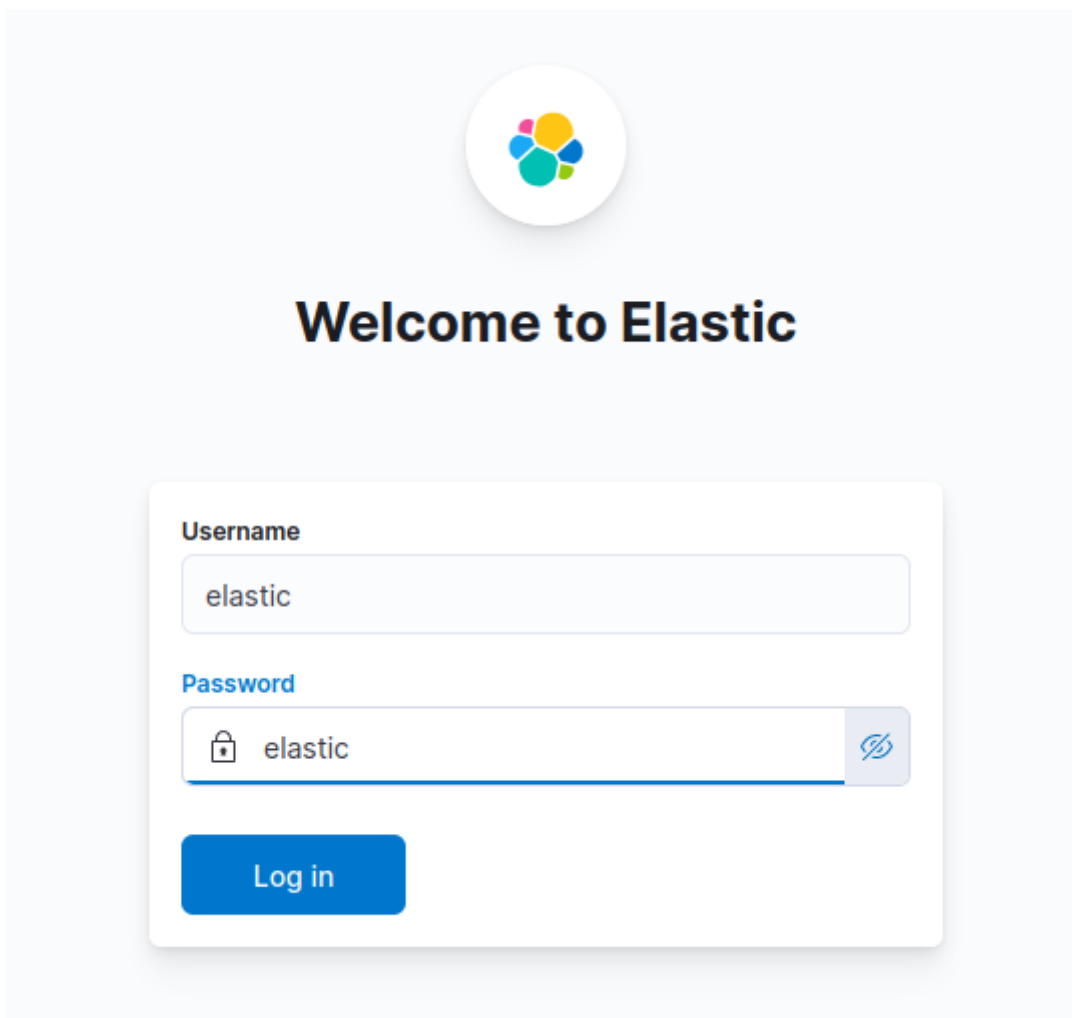
user@threatintel:~$
```

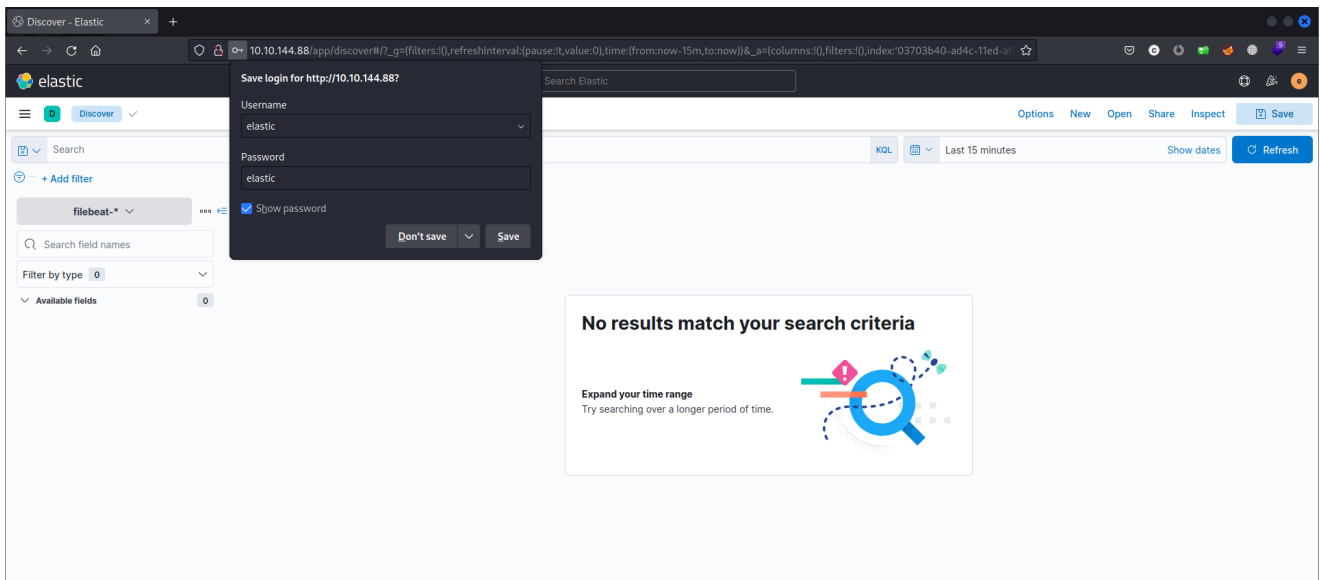
```
user@threatintel:~$ id
uid=1001(user) gid=1001(user) groups=1001(user)
user@threatintel:~$ ls -lah
total 32K
drwxr-xr-x 4 user user 4.0K Jun 16 07:40 .
drwxr-xr-x 4 root root 4.0K Feb 20 15:39 ..
-rw-r--r-- 1 user user 77 Feb 20 16:44 .bash_history
-rw-r--r-- 1 user user 220 Feb 20 15:39 .bash_logout
-rw-r--r-- 1 user user 3.7K Feb 20 15:39 .bashrc
drwxr-xr-x 2 user user 4.0K Jun 16 07:40 .cache
-rw-r--r-- 1 user user 807 Feb 20 15:39 .profile
drwxrwxr-x 3 user user 4.0K Feb 20 16:44 elastalert
user@threatintel:~$ ls -lah elastalert/
total 16K
drwxrwxr-x 3 user user 4.0K Feb 20 16:44 .
drwxr-xr-x 4 user user 4.0K Jun 16 07:40 ..
-rw-rw-r-- 1 user user 249 Feb 20 16:44 config.yaml
drwxrwxr-x 2 user user 4.0K Feb 20 16:44 rules
user@threatintel:~$ ls -lah elastalert/rules/
total 12K
drwxrwxr-x 2 user user 4.0K Feb 20 16:44 .
drwxrwxr-x 3 user user 4.0K Feb 20 16:44 ..
-rw-rw-r-- 1 user user 107 Feb 20 16:44 sinkhole.yaml
user@threatintel:~$
```

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

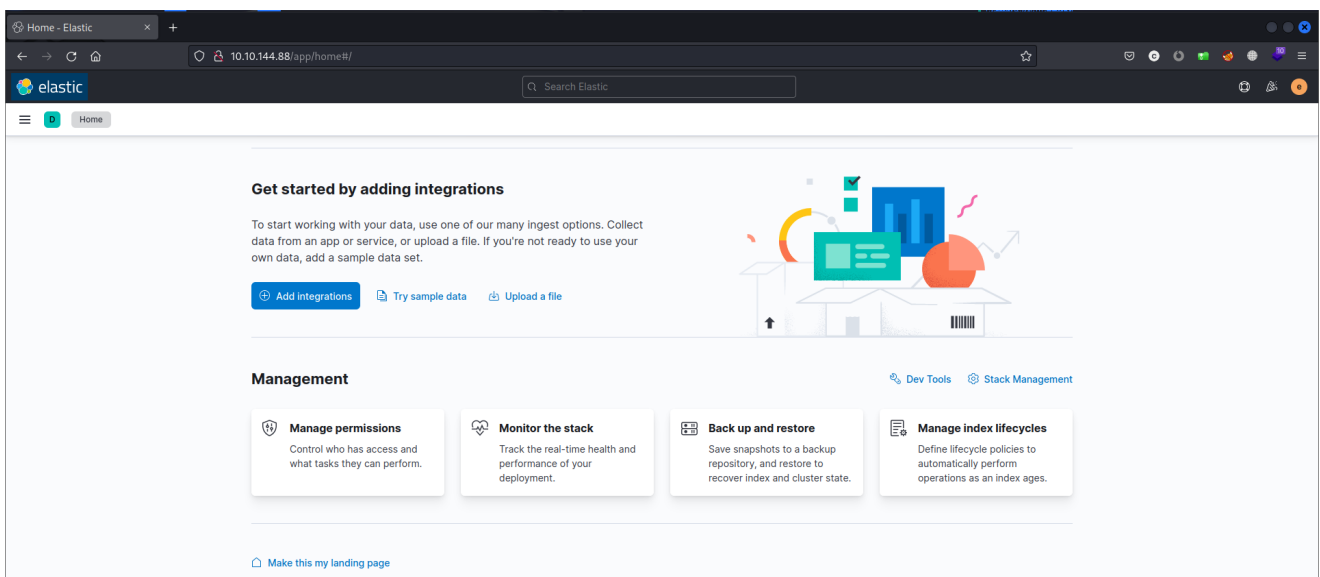
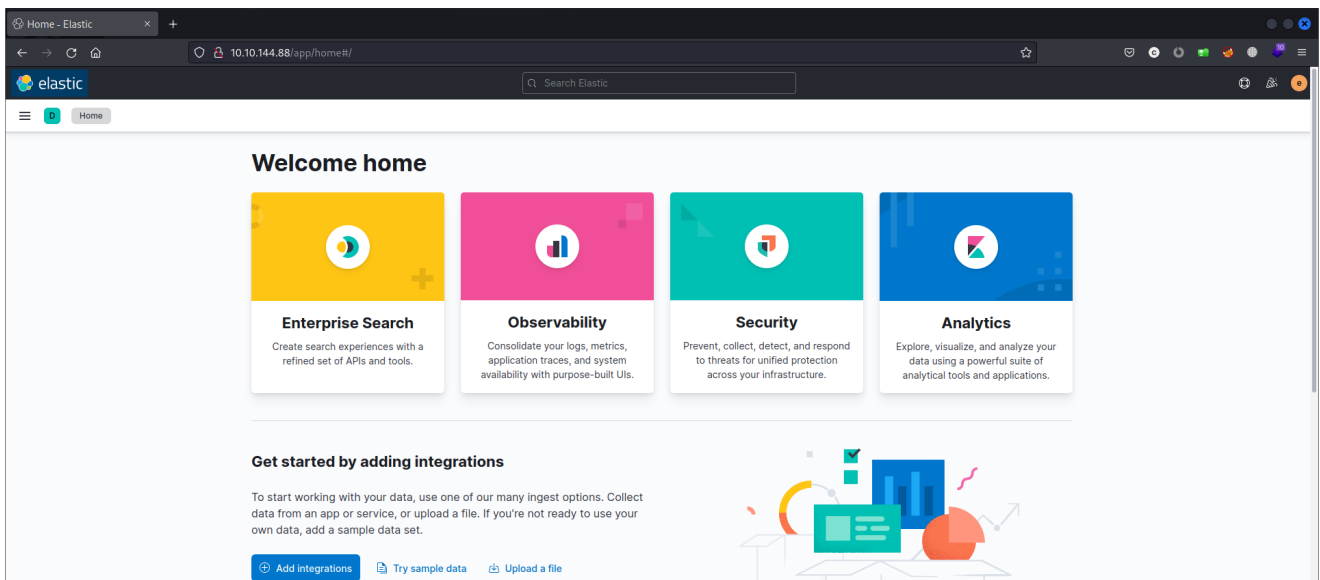


elastic:elastic





```
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)))
```

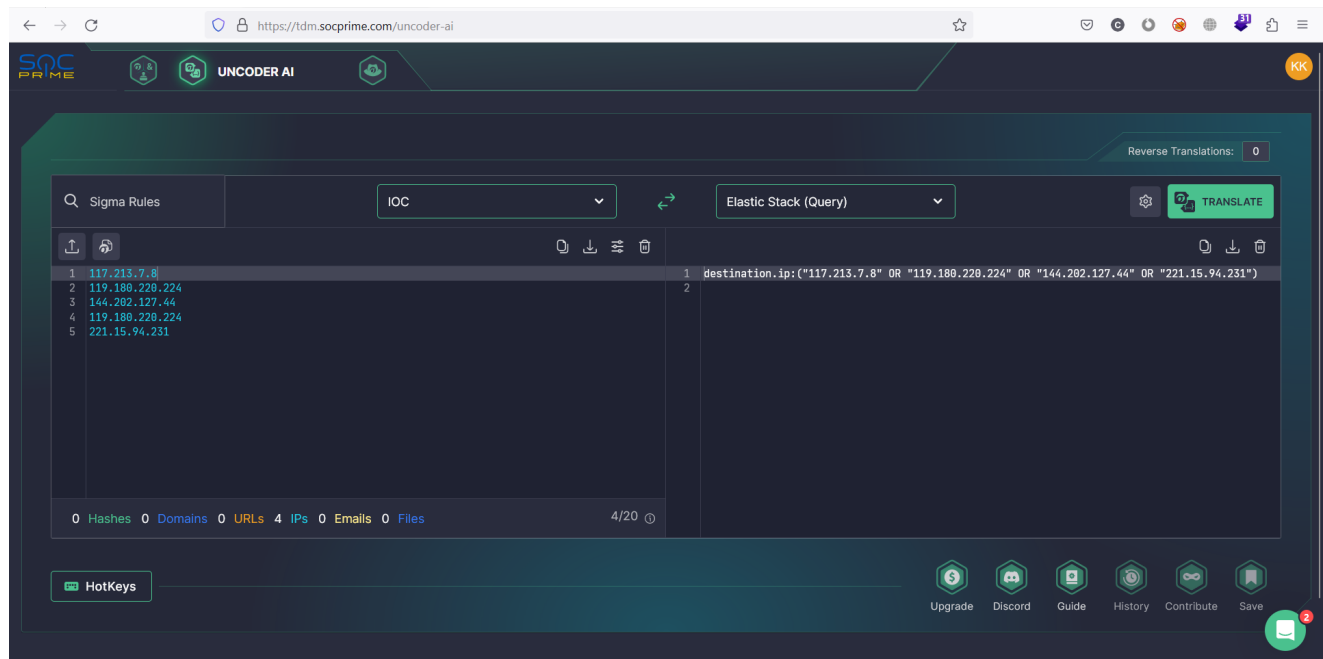


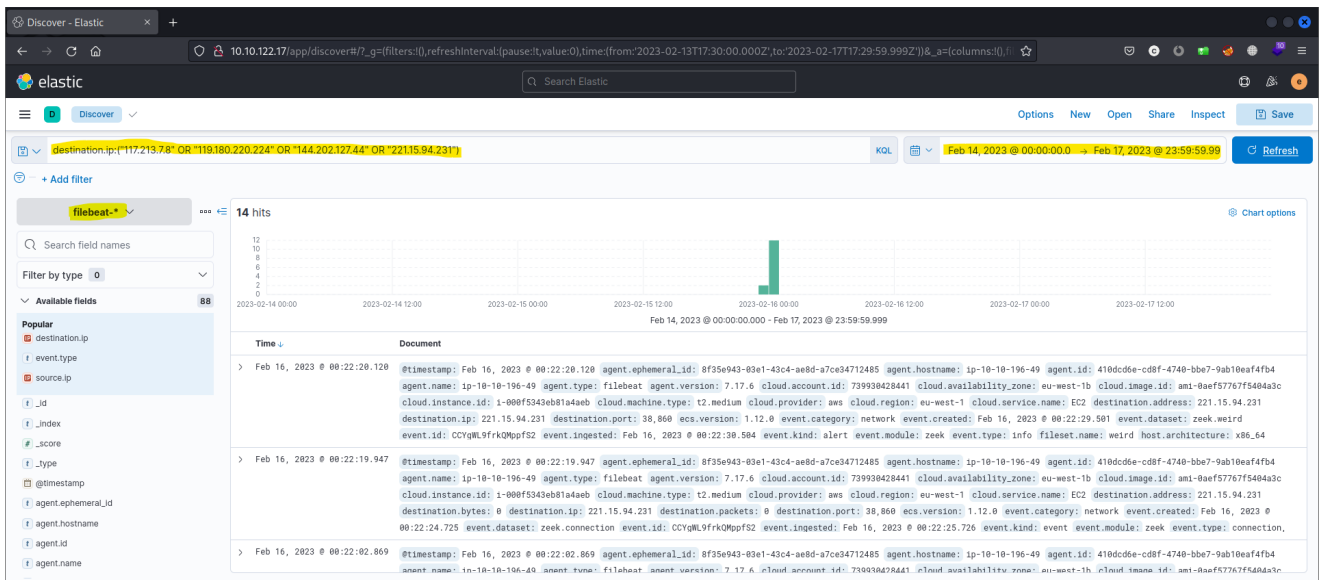
ioc\_list.txt

```
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")
```

UNCODER AI

Reverse Translations: 0

Search: Sigma Rules

IOC

Elastic Stack (Query)

TRANSLATE

1 135.181.103.89

2 185.224.126.215

3 185.224.128.215

4 171.24.136.15

5 171.22.136.15

6 195.133.40.108

7 103.190.37.169

8 103.170.37.169

9 103.190.37.169

10 185.224.128.215

11 107.175.202.151

12 107.175.202.158

13 195.133.40.108

14 107.175.202.158

15 109.206.240.194

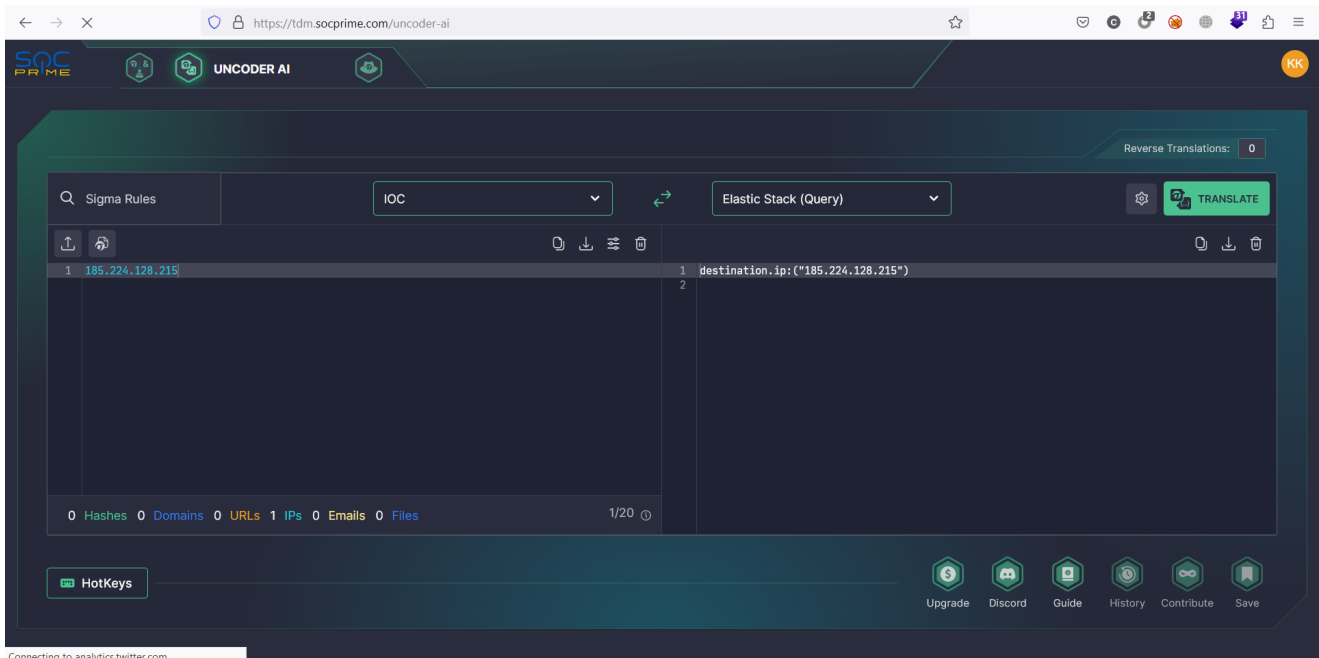
0 Hashes 0 Domains 0 URLs 11 IPs 0 Emails 0 Files

11/20

HotKeys

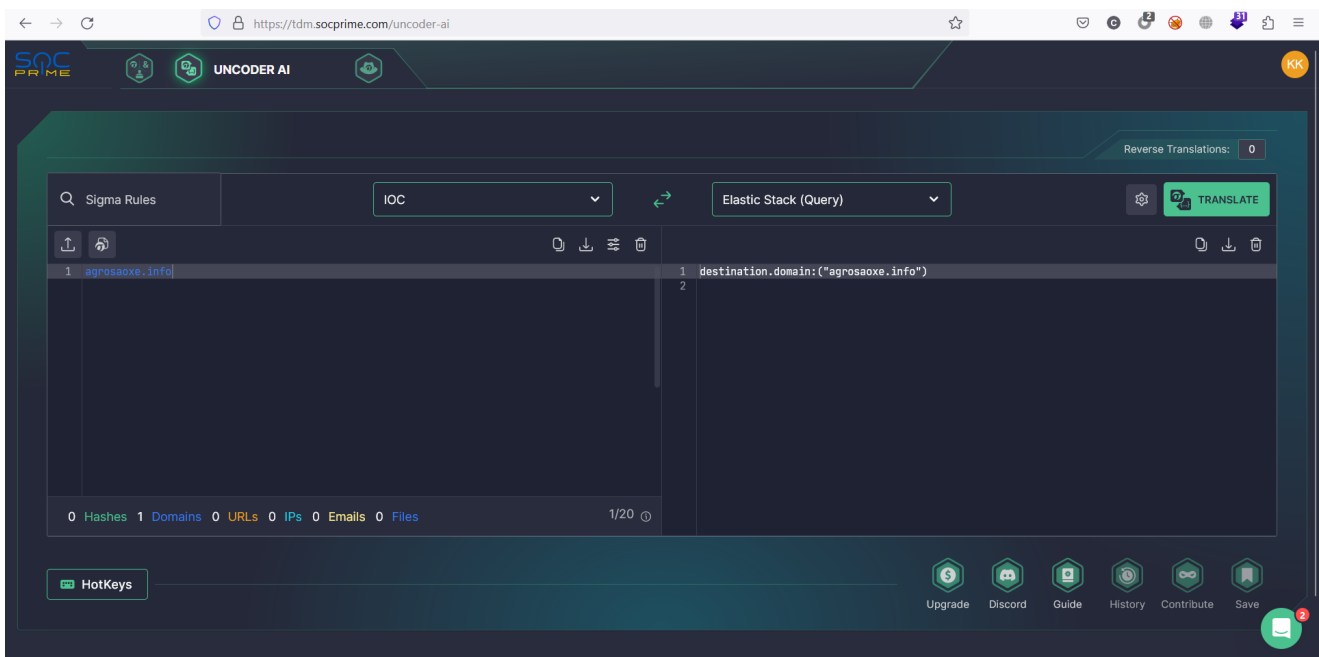
Upgrade Discord Guide History Contribute Save

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



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

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



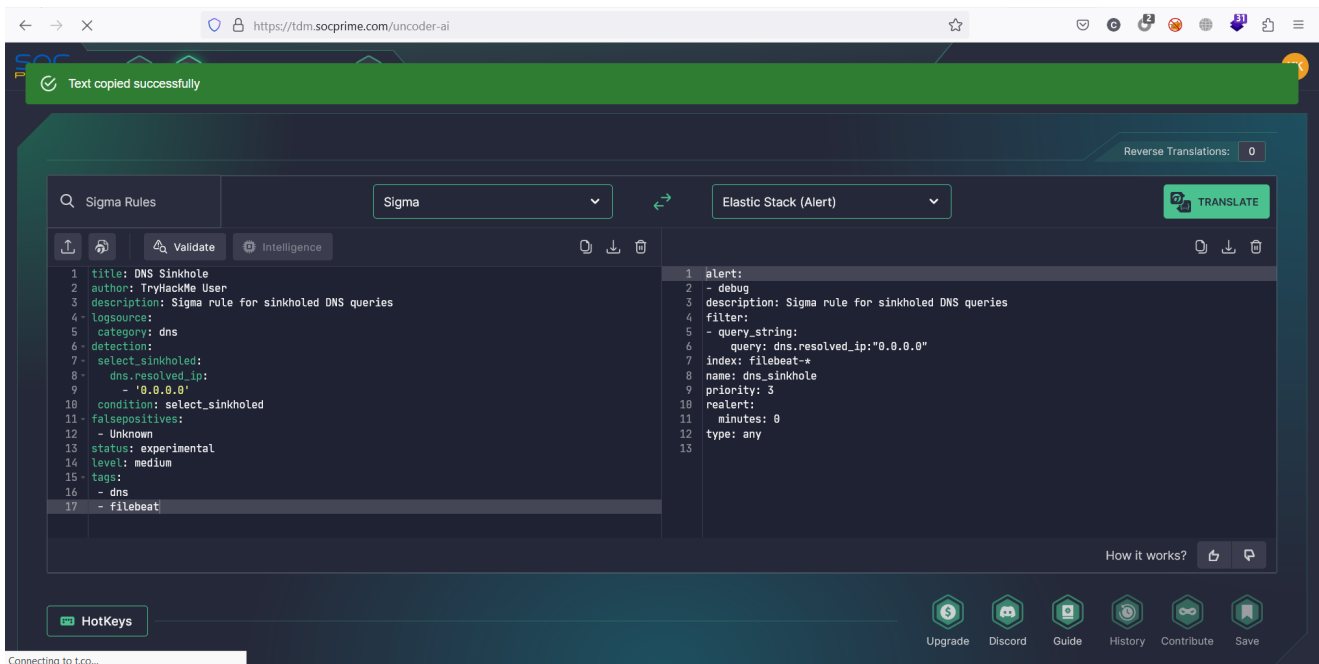
```
dns.answers.data: "0.0.0.0"
```

```
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
```

```
File Actions Edit View Help
kali@kali: ~ x user@threatintel: ~/elastalert x
}
transport: "udp"
}
num_hits: 40
num_matches: 40
related: {
  "ip": [
    "10.10.196.49",
    "10.10.24.106"
  ]
}
service: {
  "type": "zeek"
}
source: {
  "address": "10.10.196.49",
  "ip": "10.10.196.49",
  "port": 33546
}
tags: [
  "zeek.dns",
  "_geolip_expired_database"
]
zeek: {
  "dns": {
    "AA": false,
    "RA": false,
    "RD": false,
    "TC": false,
    "TTLs": [
      3600
    ],
    "answers": [
      "0.0.0.0"
    ],
    "query": "myanmarfuturescience.com",
    "rcode": 0,
    "rcode_name": "NOERROR",
    "rejected": false,
    "trans_id": "628001"
  },
  "session_id": "C2yPzG4sF03802N58"
}
INFO:elastalert:Ran dns_sinkhole from 2023-02-16 00:00 UTC to 2023-06-19 14:46 UTC: 0 query hits (0 already seen), 40 matches, 40 alerts sent
^C
user@threatintel:~/elastalert$
```

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

```
File Actions Edit View Help
kali@kali: ~ x user@threatintel: ~/elastalert x
INFO:elastalert:Queried rule dns_sinkhole from 2023-06-19 14:15 UTC to 2023-06-19 14:30 UTC: 0 / 0 hits
INFO:elastalert:Queried rule dns_sinkhole from 2023-06-19 14:30 UTC to 2023-06-19 14:45 UTC: 0 / 0 hits
INFO:elastalert:Queried rule dns_sinkhole from 2023-06-19 14:45 UTC to 2023-06-19 14:46 UTC: 0 / 0 hits
"original": {"ts": "1676541957.09678", "uid": "CSKqFxmRADUqV0Kpg", "id.orig_h": "10.10.196.49", "id.orig_p": 47895, "id.resp_h": "10.10.24.106", "id.resp_p": 53, "proto": "udp", "trans_id": 4847, "query": "twizt.ru", "rcode": 0, "rcode_name": "NOERROR", "AA": false, "TC": false, "RD": false, "RA": false, "Z": 0, "answers": [{"0.0.0.0"}], "TTLs": [3600.0], "rejected": false},
"original": {"ts": "1676541962.0518", "uid": "C9KqFxmRADUqV0Kpg", "id.orig_h": "10.10.196.49", "id.orig_p": 51034, "id.resp_h": "10.10.24.106", "id.resp_p": 53, "proto": "udp", "trans_id": 1232, "query": "twizt.ru", "rcode": 0, "rcode_name": "NOERROR", "AA": false, "TC": false, "RD": false, "RA": false, "Z": 0, "answers": [{"0.0.0.0"}], "TTLs": [3600.0], "rejected": false},
"original": {"ts": "1676542013.349713", "uid": "CFDnK3ymdydF2hok", "id.orig_h": "10.10.196.49", "id.orig_p": 39969, "id.resp_h": "10.10.24.106", "id.resp_p": 53, "proto": "udp", "trans_id": 13964, "query": "twizt.ru", "rcode": 0, "rcode_name": "NOERROR", "AA": false, "TC": false, "RD": false, "RA": false, "Z": 0, "answers": [{"0.0.0.0"}], "TTLs": [3600.0], "rejected": false},
"original": {"ts": "1676541967.0518", "uid": "C9KqFxmRADUqV0Kpg", "id.orig_h": "10.10.196.49", "id.orig_p": 46258, "id.resp_h": "10.10.24.106", "id.resp_p": 53, "proto": "udp", "trans_id": 7513, "query": "twizt.ru", "rcode": 0, "rcode_name": "NOERROR", "AA": false, "TC": false, "RD": false, "RA": false, "Z": 0, "answers": [{"0.0.0.0"}], "TTLs": [3600.0], "rejected": false},
"original": {"ts": "1676542015.037963", "uid": "C9KqFxmRADUqV0Kpg", "id.orig_h": "10.10.196.49", "id.orig_p": 56458, "id.resp_h": "10.10.24.106", "id.resp_p": 53, "proto": "udp", "trans_id": 19721, "query": "twizt.ru", "rcode": 0, "rcode_name": "NOERROR", "AA": false, "TC": false, "RD": false, "RA": false, "Z": 0, "answers": [{"0.0.0.0"}], "TTLs": [3600.0], "rejected": false},
"original": {"ts": "1676542010.380566", "uid": "C9KqFxmRADUqV0Kpg", "id.orig_h": "10.10.196.49", "id.orig_p": 41919, "id.resp_h": "10.10.24.106", "id.resp_p": 53, "proto": "udp", "trans_id": 13278, "query": "twizt.ru", "rcode": 0, "rcode_name": "NOERROR", "AA": false, "TC": false, "RD": false, "RA": false, "Z": 0, "answers": [{"0.0.0.0"}], "TTLs": [3600.0], "rejected": false},
user@threatintel:~/elastalert$ more output.txt |grep ".ru"
```

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

```
File Actions Edit View Help
kali@kali: ~ x user@threatintel: ~/elastalert x
user@threatintel:~/elastalert$ grep query output.txt | grep -Eo '[a-zA-Z0-9.-]+\.[a-zA-Z]{2,}' | sort -u
ball-kit.click
bar.com
foo.bar.com
id.orig
id.resp
myanmarfuturescience.com
twizt.ru
uradlimited.com
www.ingetic.cl
user@threatintel:~/elastalert$
```



TryHackMe

Dashboard

Learn

Compete

Other

Access Machines

23

Go Premium

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#