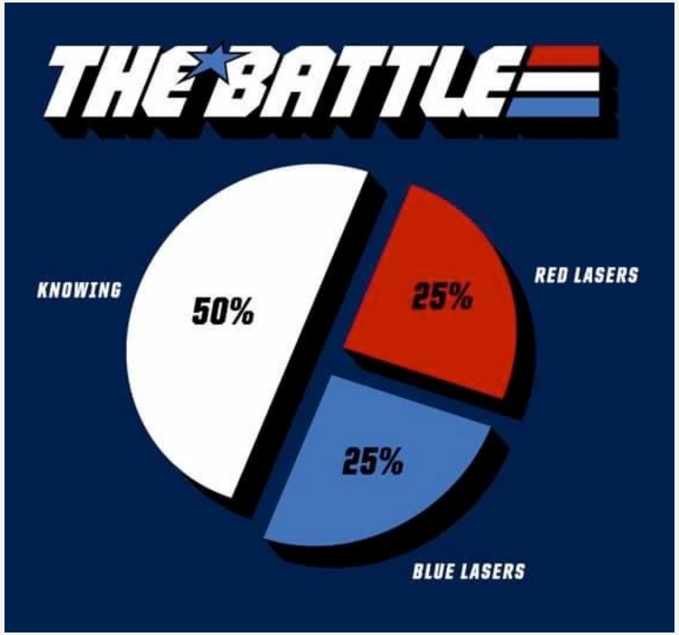
Enrich Your Data And Enrich Your Life

Presented by Pete Di Giorgio

Objectives

- Chat about situational understand and decision making
- Discuss data enrichment
- Engineer data enrichment to highlight "interesting" activity

Knowing is Half the Battle

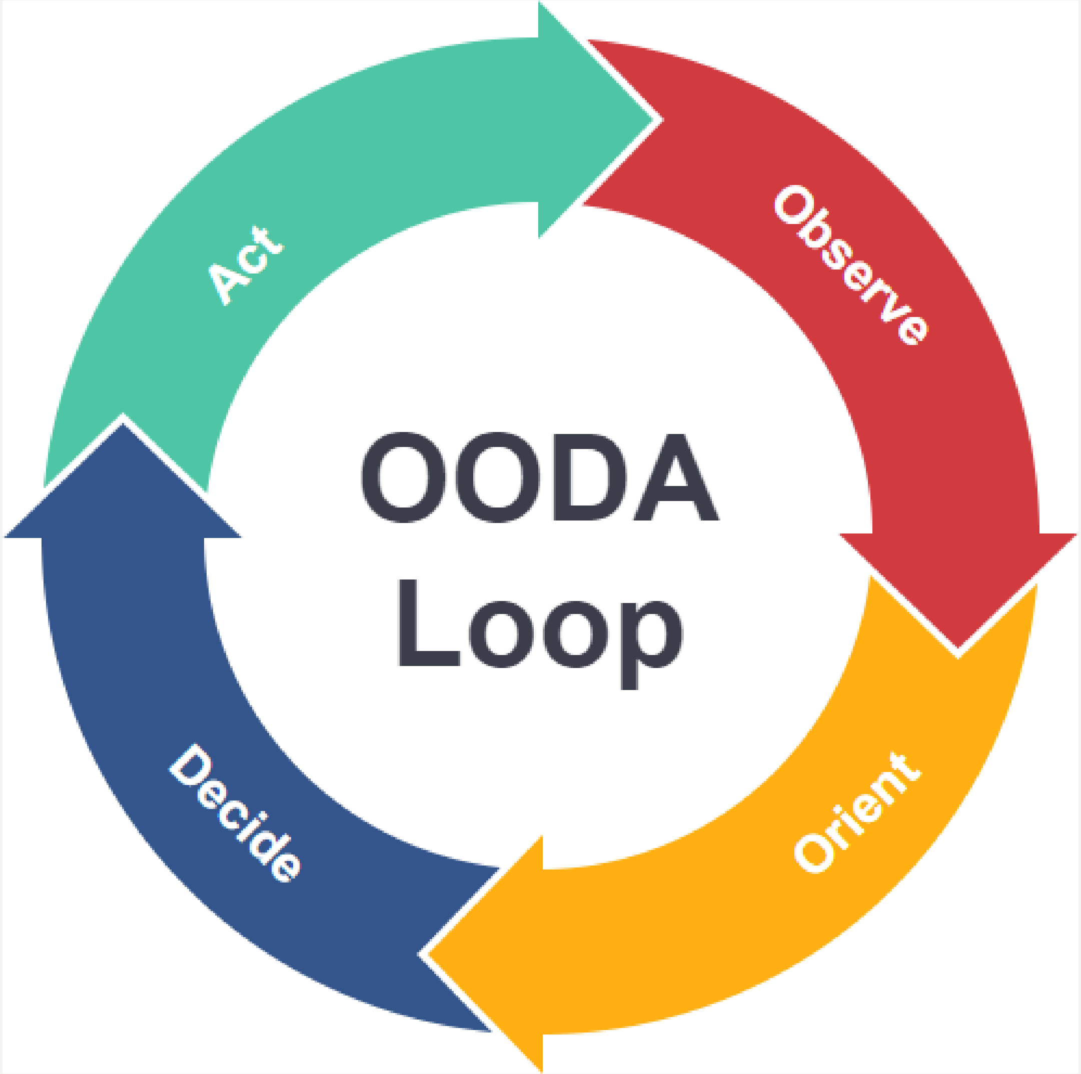


Gain situational understanding of an environment:

- Know Yourself
- Know Your Terrain
- Know Your Adversary

"If you know the enemy and know yourself, your victory will not stand in doubt: if you know Heaven and know Earth, you may make your victory complete"

–Sun Tzu


OODA
Loop
Observe
Orient
Decide
Act

Data Enrichment

improve or enhance the quality or value of.

–Oxford Languages

"Data enrichment refers to the process of appending or otherwise enhancing collected data with **relevant context obtained from additional sources.** “

–Eric D. Knapp, Joel Thomas Langill, in Industrial Network Security (Second Edition), 2015

Common Techniques

1. Append
2. Segment
3. Derive
4. Manipulate
5. Extract
6. Categorize

A Couple of Thoughts

1. Provide context
2. Support decisions
3. Reduce swivel chair correlation
4. Keep computational cost low

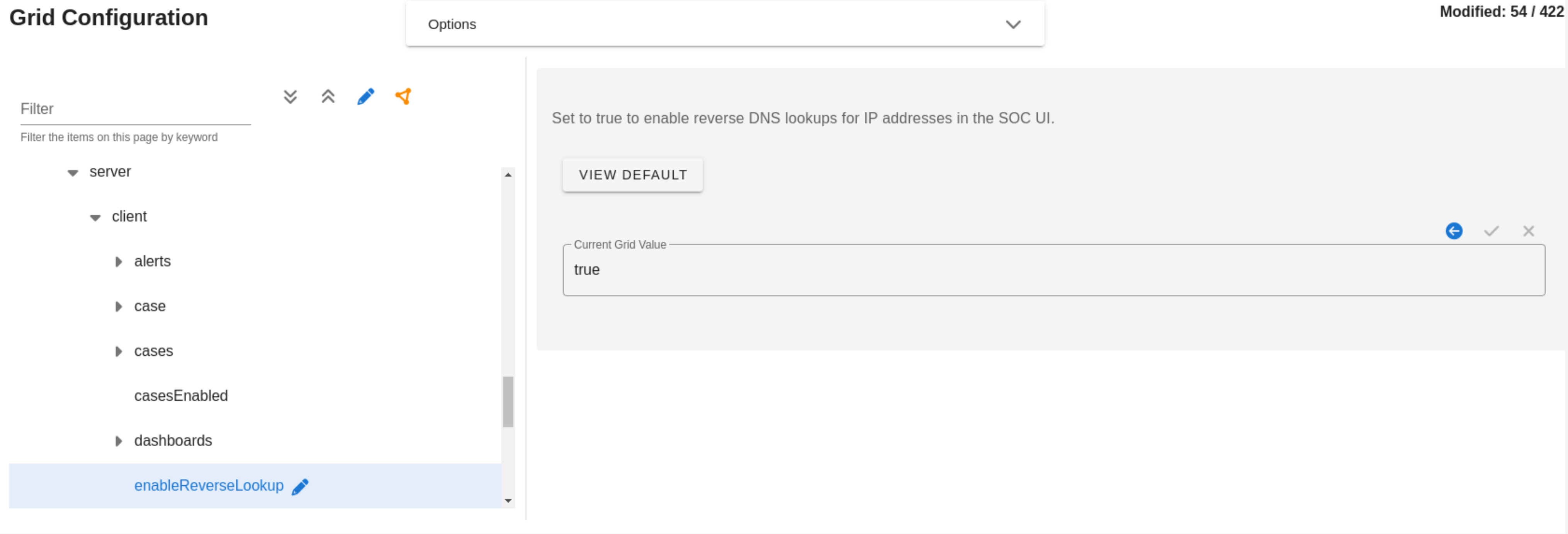
Lets do this!

1. DNS Reverse Lookups in Security Onion Console
2. Domain

DNS Reverse Lookup

Enable reverse DNS lookups in Security Onion Console:

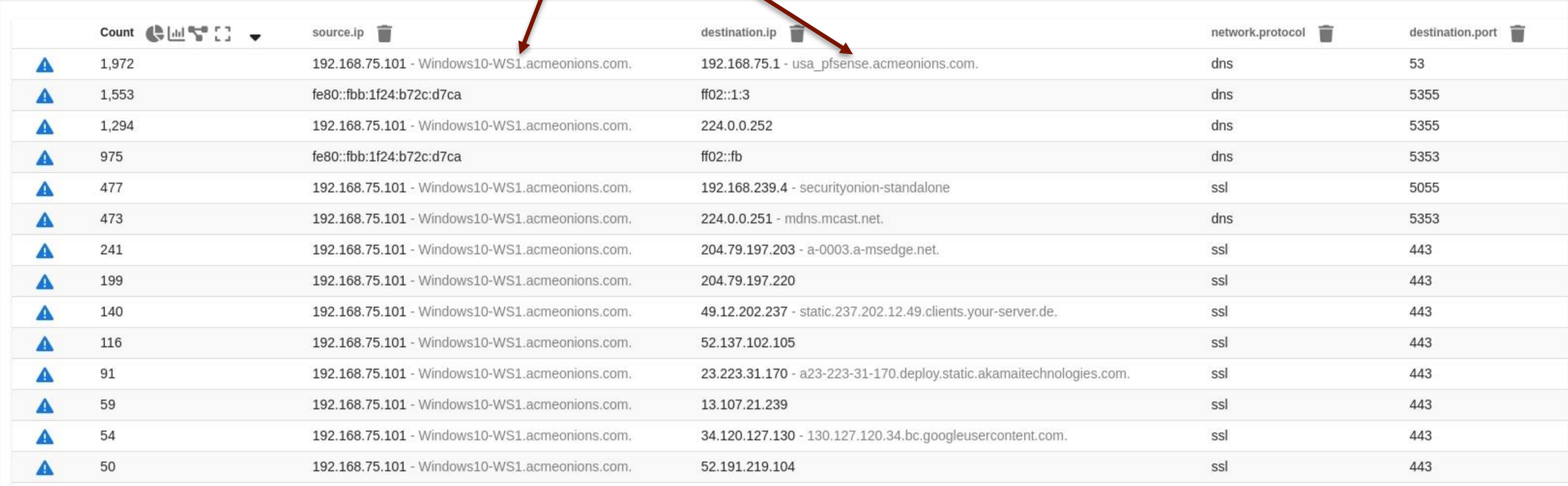
Administration –> Configuration –> soc –> config –> server –> client –> enableReverseLookup



Set to true to enable reverse DNS lookups for IP addresses in the SOC UI.

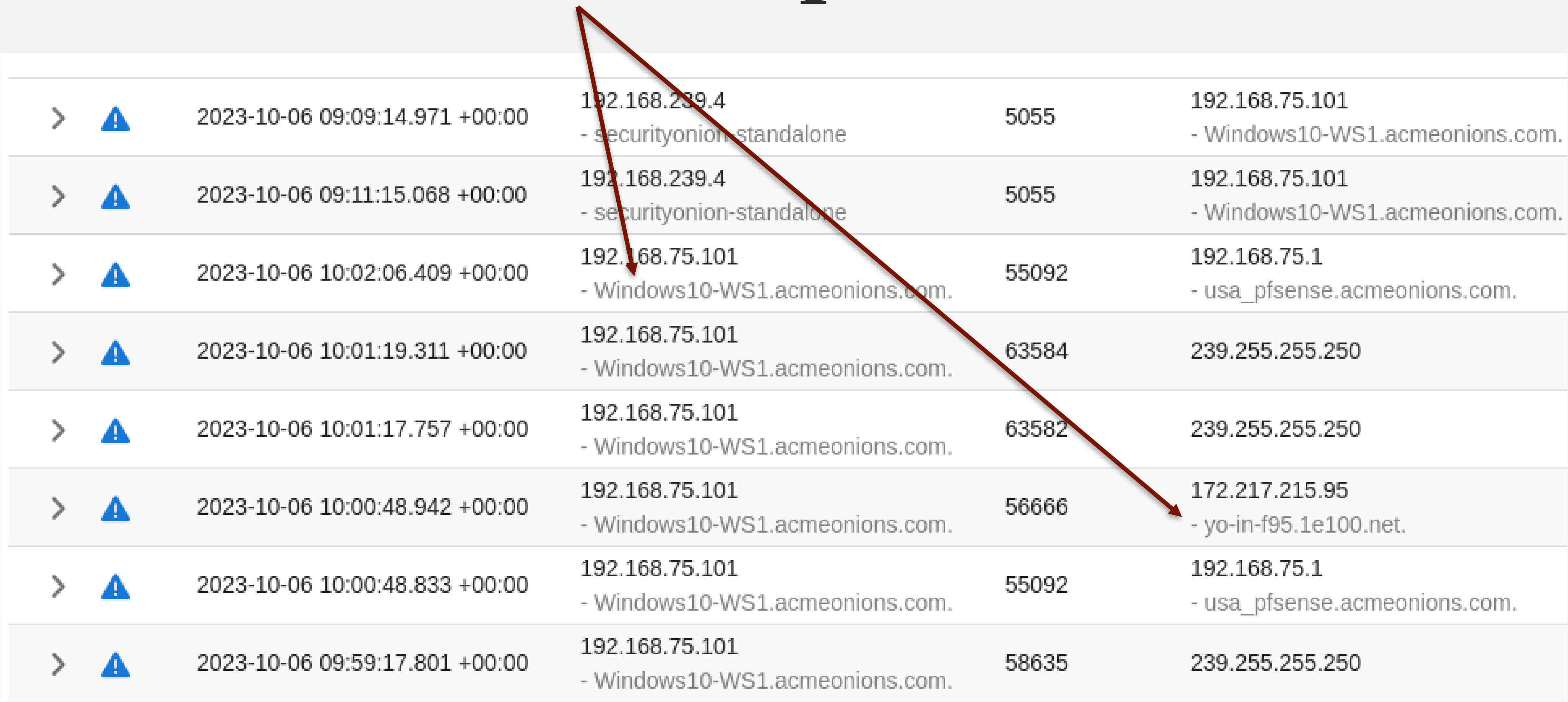
Current Grid Value: true

DNS Reverse Lookup



	Count	source.ip	destination.ip	network.protocol	destination.port
⚠	1,972	192.168.75.101 - Windows10-WS1.acmeonions.com.	192.168.75.1 - usa_pfsense.acmeonions.com.	dns	53
⚠	1,553	fe80::fbb:1f24:b72c:d7ca	ff02::1:3	dns	5355
⚠	1,294	192.168.75.101 - Windows10-WS1.acmeonions.com.	224.0.0.252	dns	5355
⚠	975	fe80::fbb:1f24:b72c:d7ca	ff02::fb	dns	5353
⚠	477	192.168.75.101 - Windows10-WS1.acmeonions.com.	192.168.239.4 - securityonion-standalone	ssl	5055
⚠	473	192.168.75.101 - Windows10-WS1.acmeonions.com.	224.0.0.251 - mdns.mcast.net.	dns	5353
⚠	241	192.168.75.101 - Windows10-WS1.acmeonions.com.	204.79.197.203 - a-0003.a-msedge.net.	ssl	443
⚠	199	192.168.75.101 - Windows10-WS1.acmeonions.com.	204.79.197.220	ssl	443
⚠	140	192.168.75.101 - Windows10-WS1.acmeonions.com.	49.12.202.237 - static.237.202.12.49.clients.your-server.de.	ssl	443
⚠	116	192.168.75.101 - Windows10-WS1.acmeonions.com.	52.137.102.105	ssl	443
⚠	91	192.168.75.101 - Windows10-WS1.acmeonions.com.	23.223.31.170 - a23-223-31-170.deploy.static.akamaitechnologies.com.	ssl	443
⚠	59	192.168.75.101 - Windows10-WS1.acmeonions.com.	13.107.21.239	ssl	443
⚠	54	192.168.75.101 - Windows10-WS1.acmeonions.com.	34.120.127.130 - 130.127.120.34.bc.googleusercontent.com.	ssl	443
⚠	50	192.168.75.101 - Windows10-WS1.acmeonions.com.	52.191.219.104	ssl	443

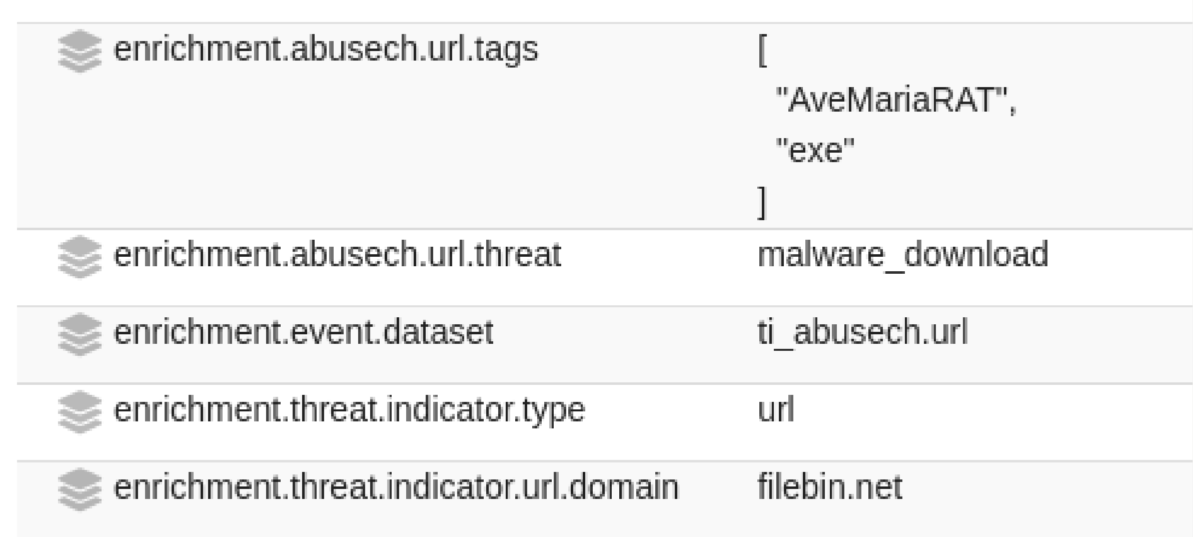
DNS Reverse Lookup



›	⚠	2023-10-06 09:09:14.971 +00:00	192.168.239.4 - securityonion-standalone	5055	192.168.75.101 - Windows10-WS1.acmeonions.com.
›	⚠	2023-10-06 09:11:15.068 +00:00	192.168.239.4 - securityonion-standalone	5055	192.168.75.101 - Windows10-WS1.acmeonions.com.
›	⚠	2023-10-06 10:02:06.409 +00:00	192.168.75.101 - Windows10-WS1.acmeonions.com.	55092	192.168.75.1 - usa_pfsense.acmeonions.com.
›	⚠	2023-10-06 10:01:19.311 +00:00	192.168.75.101 - Windows10-WS1.acmeonions.com.	63584	239.255.255.250
›	⚠	2023-10-06 10:01:17.757 +00:00	192.168.75.101 - Windows10-WS1.acmeonions.com.	63582	239.255.255.250
›	⚠	2023-10-06 10:00:48.942 +00:00	192.168.75.101 - Windows10-WS1.acmeonions.com.	56666	172.217.215.95 - yo-in-f95.1e100.net.
›	⚠	2023-10-06 10:00:48.833 +00:00	192.168.75.101 - Windows10-WS1.acmeonions.com.	55092	192.168.75.1 - usa_pfsense.acmeonions.com.
›	⚠	2023-10-06 09:59:17.801 +00:00	192.168.75.101 - Windows10-WS1.acmeonions.com.	58635	239.255.255.250

Enrichment with Threat Intelligence

1. Elastic Agent integrations
2. Enrich Index
3. Enrich Policy
4. Ingest Pipeline



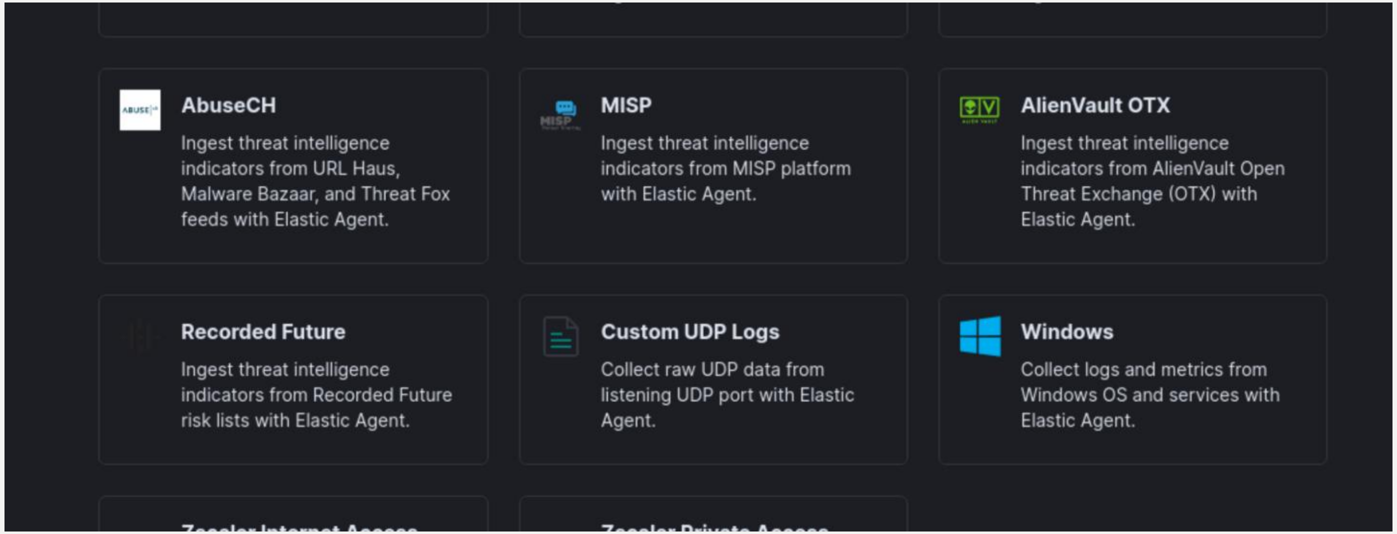
enrichment.abusech.url.tags	["AveMariaRAT", "exe"]
enrichment.abusech.url.threat	malware_download
enrichment.event.dataset	ti_abusech.url
enrichment.threat.indicator.type	url
enrichment.threat.indicator.url.domain	filebin.net

Wes Lambert has a great article here: https://glue.ghost.io/leveraging-threat-intel-for-event-enrichment-in-security-onion/

Threat Intelligence Integrations

1. AbuseCH
2. AlienVault OTX
3. Recorded Future
4. MISP
5. Anomali
6. Cybersixgill
7. Maltiverse
8. Mimecast
9. ThreatQuotient

Supported in 2.4.20



AbuseCH
Ingest threat intelligence indicators from URL Haus, Malware Bazaar, and Threat Fox feeds with Elastic Agent.

MISP
Ingest threat intelligence indicators from MISP platform with Elastic Agent.

AlienVault OTX
Ingest threat intelligence indicators from AlienVault Open Threat Exchange (OTX) with Elastic Agent.

Recorded Future
Ingest threat intelligence indicators from Recorded Future risk lists with Elastic Agent.

Custom UDP Logs
Collect raw UDP data from listening UDP port with Elastic Agent.

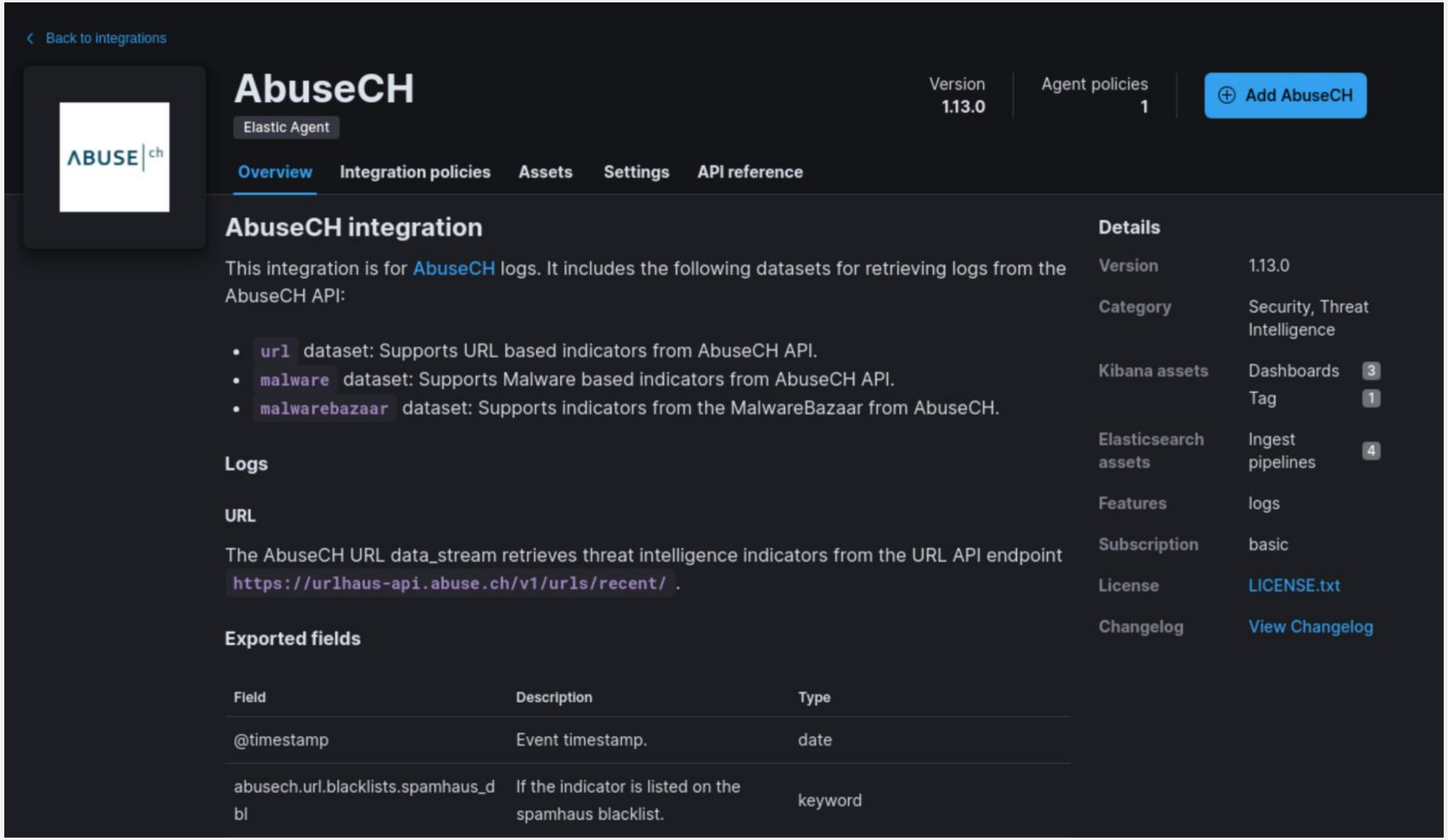
Windows
Collect logs and metrics from Windows OS and services with Elastic Agent.

Zscaler Internet Access

Zscaler Private Access

Threat Intelligence Integrations

- AbuseCH



AbuseCH

AbuseCH integration

This integration is for AbuseCH logs. It includes the following datasets for retrieving logs from the AbuseCH API:

- `url` dataset: Supports URL based indicators from AbuseCH API.
- `malware` dataset: Supports Malware based indicators from AbuseCH API.
- `malwarebazaar` dataset: Supports indicators from the MalwareBazaar from AbuseCH.

Logs

URL

The AbuseCH URL data_stream retrieves threat intelligence indicators from the URL API endpoint `https://urlhaus-api.abuse.ch/v1/urls/recent/`.

Exported fields

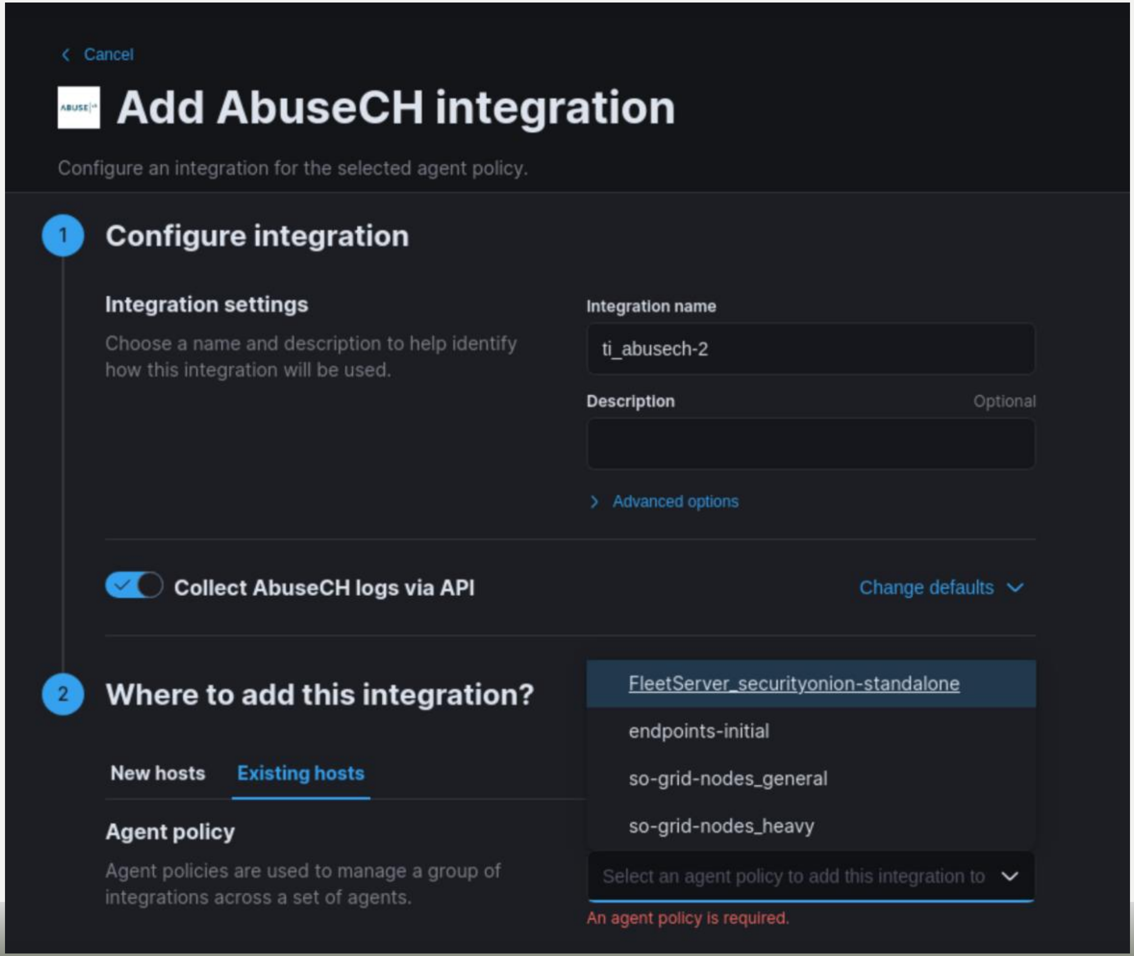
Field	Description	Type
@timestamp	Event timestamp.	date
abusech.url.blacklists.spamhaus_dbl	If the indicator is listed on the spamhaus blacklist.	keyword

Details

Version	1.13.0
Category	Security, Threat Intelligence
Kibana assets	Dashboards 3 Tag 1
Elasticsearch assets	Ingest pipelines 4
Features	logs
Subscription	basic
License	LICENSE.txt
Changelog	View Changelog

Threat Intelligence Integrations

- AbuseCH



< Cancel

Add AbuseCH integration

Configure an integration for the selected agent policy.

1 Configure integration

Integration settings

Choose a name and description to help identify how this integration will be used.

Integration name: ti_abusech-2

Description (Optional):

> Advanced options

☑ Collect AbuseCH logs via API

Change defaults

2 Where to add this integration?

New hosts | Existing hosts

Agent policy

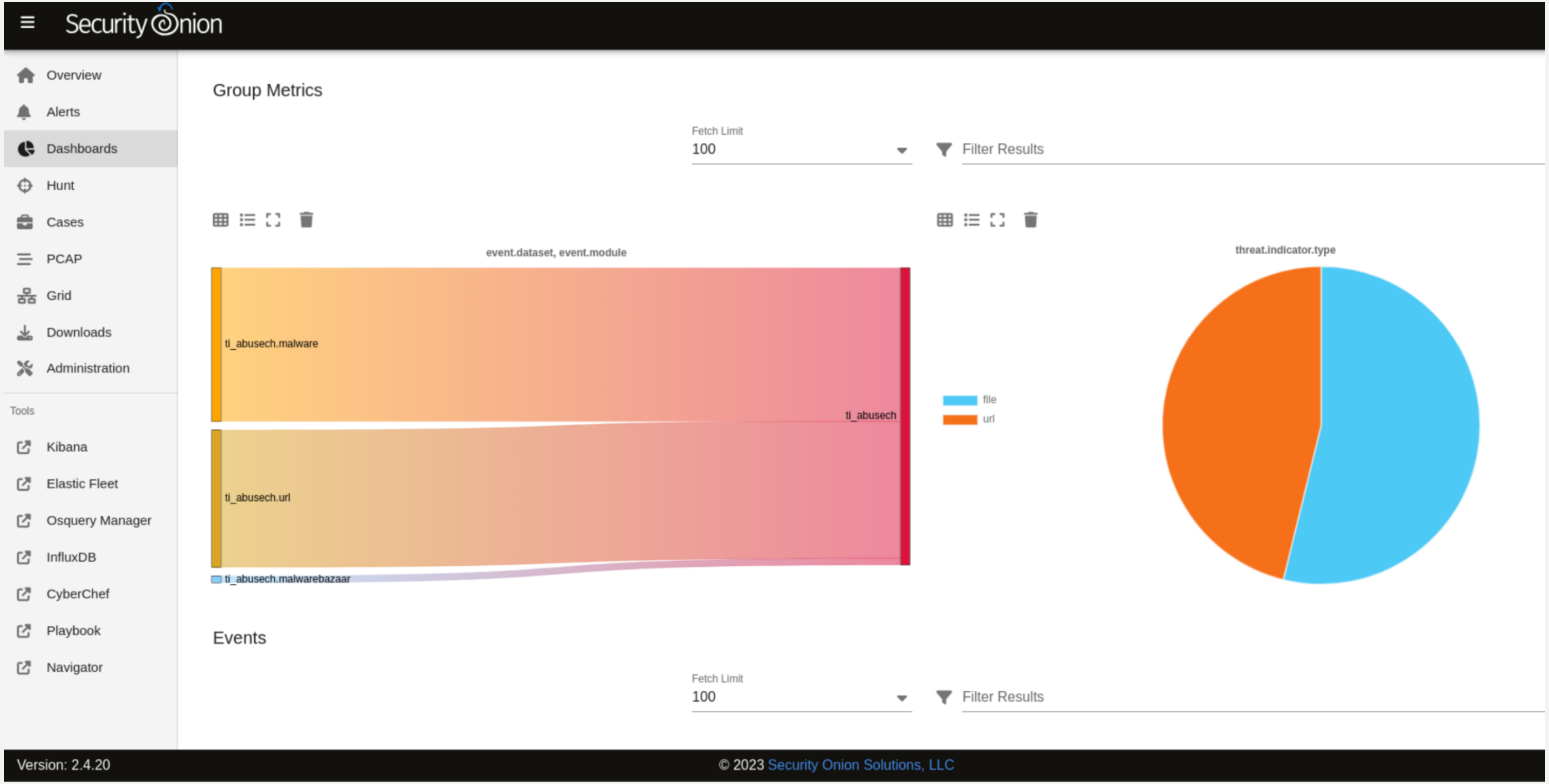
Agent policies are used to manage a group of integrations across a set of agents.

FleetServer_securityonion-standalone
endpoints-initial
so-grid-nodes_general
so-grid-nodes_heavy

Select an agent policy to add this integration to

An agent policy is required.

Threat Intelligence Integrations



Group Metrics

Fetch Limit
100

Filter Results

Events

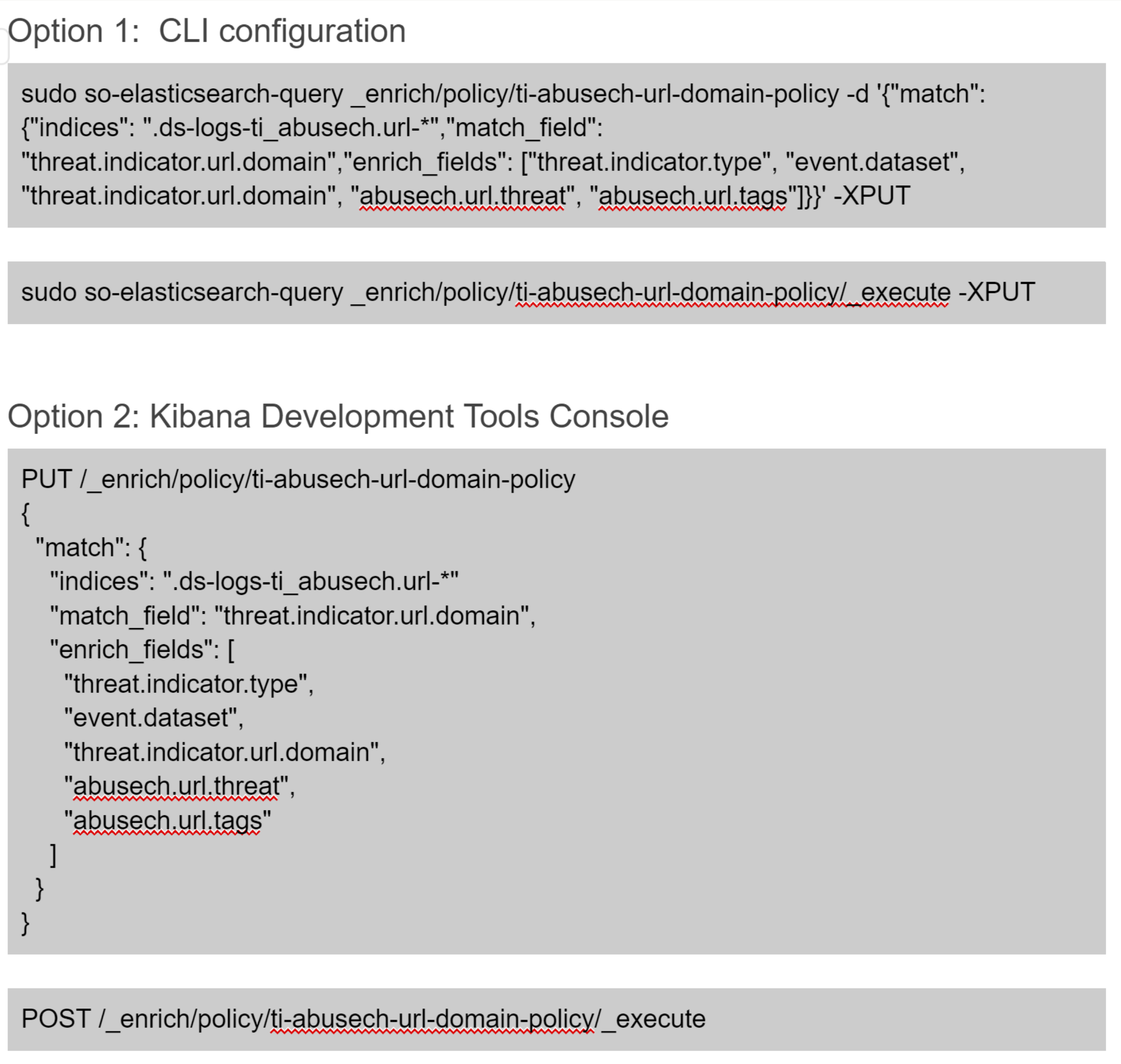
Fetch Limit
100

Filter Results

Version: 2.4.20

© 2023 Security Onion Solutions, LLC

Enrich Policy



Option 1: CLI configuration

```
sudo so-elasticsearch-query _enrich/policy/ti-abusech-url-domain-policy -d '{"match":
{"indices": ".ds-logs-ti_abusech.url-*","match_field":
"threat.indicator.url.domain","enrich_fields": ["threat.indicator.type", "event.dataset",
"threat.indicator.url.domain", "abusech.url.threat", "abusech.url.tags"]}}' -XPUT
```

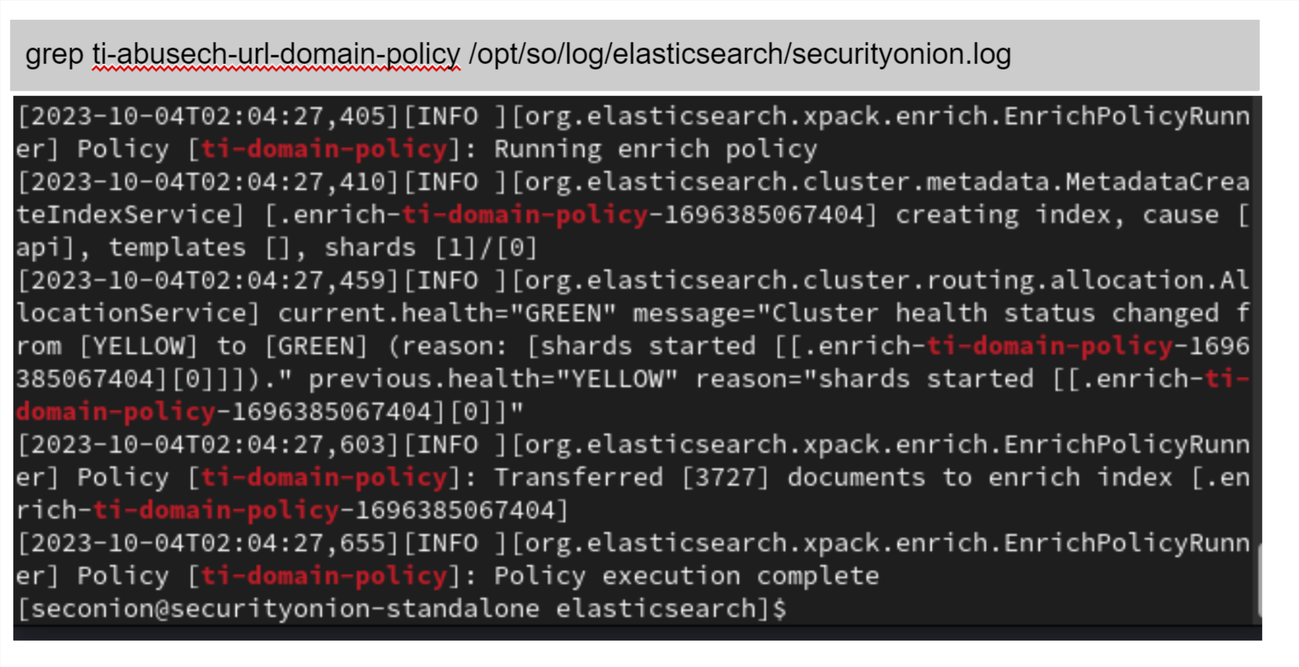
```
sudo so-elasticsearch-query _enrich/policy/ti-abusech-url-domain-policy/_execute -XPUT
```

Option 2: Kibana Development Tools Console

```
PUT /_enrich/policy/ti-abusech-url-domain-policy
{
  "match": {
    "indices": ".ds-logs-ti_abusech.url-*"
    "match_field": "threat.indicator.url.domain",
    "enrich_fields": [
      "threat.indicator.type",
      "event.dataset",
      "threat.indicator.url.domain",
      "abusech.url.threat",
      "abusech.url.tags"
    ]
  }
}
```

```
POST /_enrich/policy/ti-abusech-url-domain-policy/_execute
```

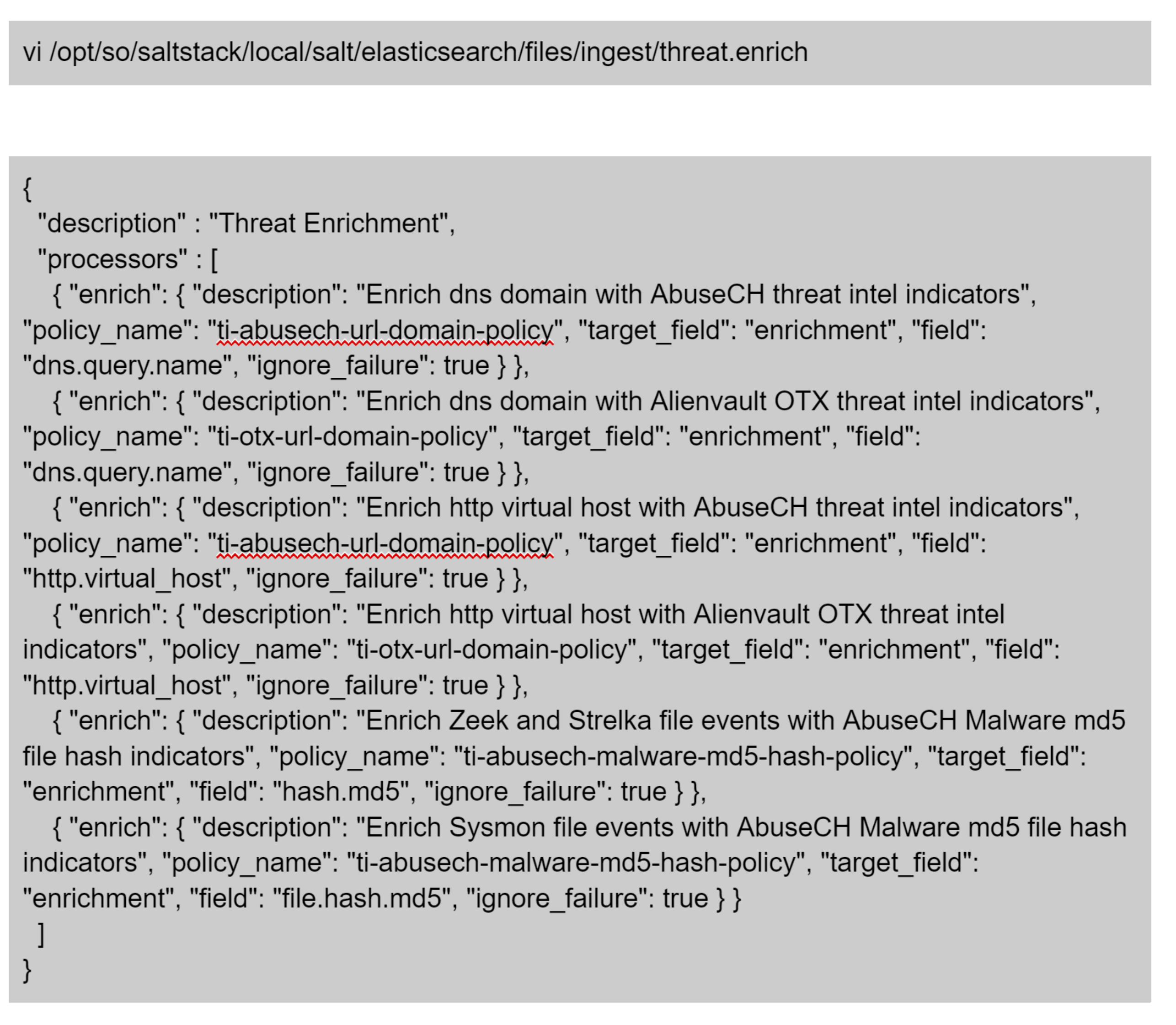
Enrich Policy



```
grep ti-abusech-url-domain-policy /opt/so/log/elasticsearch/securityonion.log
```

```
[2023-10-04T02:04:27,405][INFO ][org.elasticsearch.xpack.enrich.EnrichPolicyRunn
er] Policy [ti-domain-policy]: Running enrich policy
[2023-10-04T02:04:27,410][INFO ][org.elasticsearch.cluster.metadata.MetadataCrea
teIndexService] [.enrich-ti-domain-policy-1696385067404] creating index, cause [
api], templates [], shards [1]/[0]
[2023-10-04T02:04:27,459][INFO ][org.elasticsearch.cluster.routing.allocation.Al
locationService] current.health="GREEN" message="Cluster health status changed f
rom [YELLOW] to [GREEN] (reason: [shards started [[.enrich-ti-domain-policy-1696
385067404][0]]])." previous.health="YELLOW" reason="shards started [[.enrich-ti-
domain-policy-1696385067404][0]]"
[2023-10-04T02:04:27,603][INFO ][org.elasticsearch.xpack.enrich.EnrichPolicyRunn
er] Policy [ti-domain-policy]: Transferred [3727] documents to enrich index [.en
rich-ti-domain-policy-1696385067404]
[2023-10-04T02:04:27,655][INFO ][org.elasticsearch.xpack.enrich.EnrichPolicyRunn
er] Policy [ti-domain-policy]: Policy execution complete
[seconion@securityonion-standalone elasticsearch]$
```

Ingest Pipeline

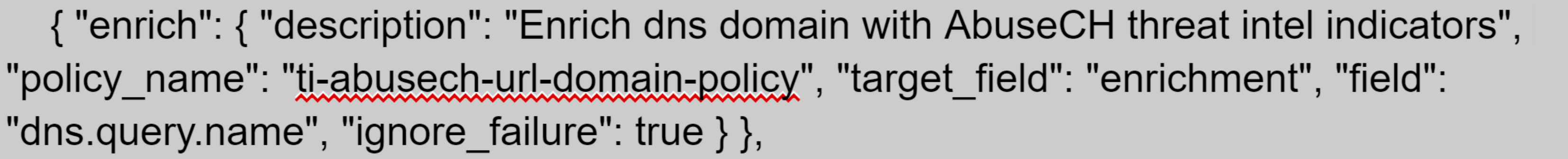


```
vi /opt/so/saltstack/local/salt/elasticsearch/files/ingest/threat.enrich
```

```
{
  "description" : "Threat Enrichment",
  "processors" : [
    { "enrich": { "description": "Enrich dns domain with AbuseCH threat intel indicators",
"policy_name": "ti-abusech-url-domain-policy", "target_field": "enrichment", "field":
"dns.query.name", "ignore_failure": true } },
    { "enrich": { "description": "Enrich dns domain with Alienvault OTX threat intel indicators",
"policy_name": "ti-otx-url-domain-policy", "target_field": "enrichment", "field":
"dns.query.name", "ignore_failure": true } },
    { "enrich": { "description": "Enrich http virtual host with AbuseCH threat intel indicators",
"policy_name": "ti-abusech-url-domain-policy", "target_field": "enrichment", "field":
"http.virtual_host", "ignore_failure": true } },
    { "enrich": { "description": "Enrich http virtual host with Alienvault OTX threat intel
indicators", "policy_name": "ti-otx-url-domain-policy", "target_field": "enrichment", "field":
"http.virtual_host", "ignore_failure": true } },
    { "enrich": { "description": "Enrich Zeek and Strelka file events with AbuseCH Malware md5
file hash indicators", "policy_name": "ti-abusech-malware-md5-hash-policy", "target_field":
"enrichment", "field": "hash.md5", "ignore_failure": true } },
    { "enrich": { "description": "Enrich Sysmon file events with AbuseCH Malware md5 file hash
indicators", "policy_name": "ti-abusech-malware-md5-hash-policy", "target_field":
"enrichment", "field": "file.hash.md5", "ignore_failure": true } }
  ]
}
```

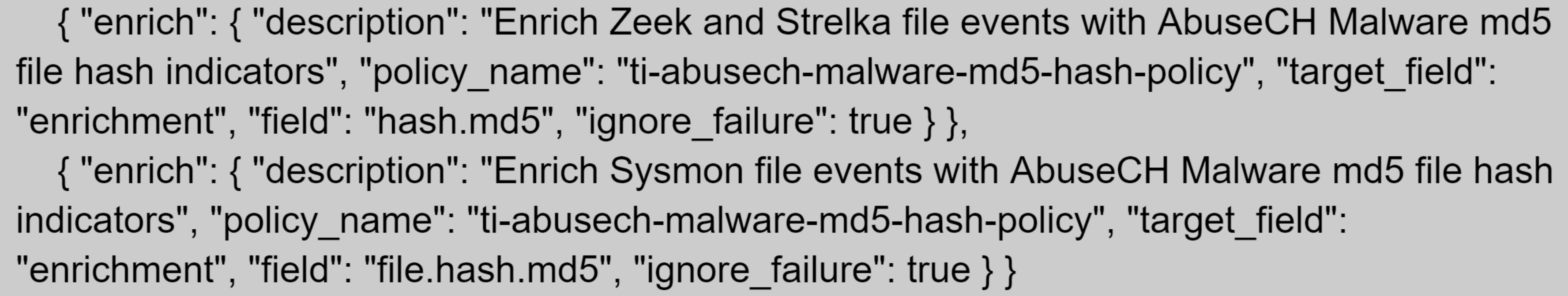
Ingest Pipeline

Enrich DNS name query with AbuseCH URL indicators



```
   { "enrich": { "description": "Enrich dns domain with AbuseCH threat intel indicators",
"policy_name": "ti-abusech-url-domain-policy", "target_field": "enrichment", "field":
"dns.query.name", "ignore_failure": true } },
```

Enrich Zeek, Strelka, and Sysmon file events with AbuseCH malware

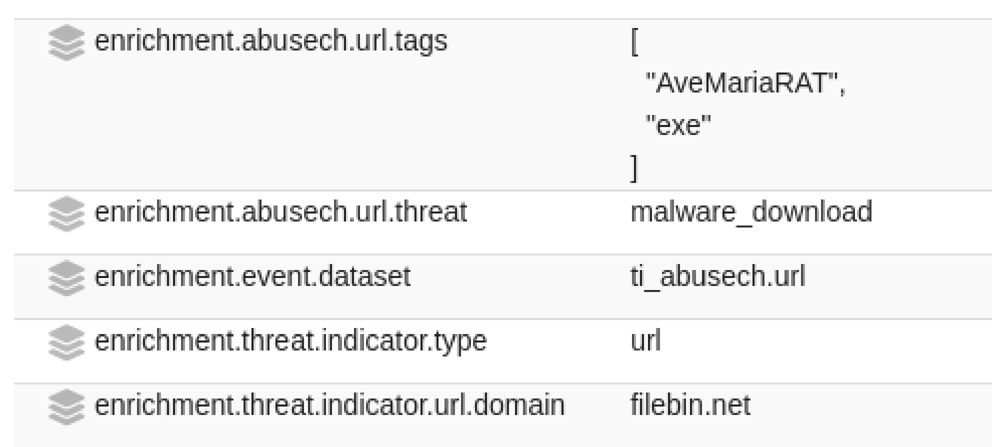


```
   { "enrich": { "description": "Enrich Zeek and Strelka file events with AbuseCH Malware md5
file hash indicators", "policy_name": "ti-abusech-malware-md5-hash-policy", "target_field":
"enrichment", "field": "hash.md5", "ignore_failure": true } },
   { "enrich": { "description": "Enrich Sysmon file events with AbuseCH Malware md5 file hash
indicators", "policy_name": "ti-abusech-malware-md5-hash-policy", "target_field":
"enrichment", "field": "file.hash.md5", "ignore_failure": true } }
```

Bring it all together

1. Restart Elasticsearch
2. Add ingest pipeline to active index

```
sudo so-elasticsearch-query .ds-logs-zeek-so-2023.10.06-000001/_settings
-d'{"index":{"final_pipeline": "threat.enrich"}}' -XPUT
```



enrichment.abusech.url.tags	["AveMariaRAT", "exe"]
enrichment.abusech.url.threat	malware_download
enrichment.event.dataset	ti_abusech.url
enrichment.threat.indicator.type	url
enrichment.threat.indicator.url.domain	filebin.net

Summary

- Discussed data enrichment
- Explored Security Onion 2 integrations for data enrichment
- Had fun!