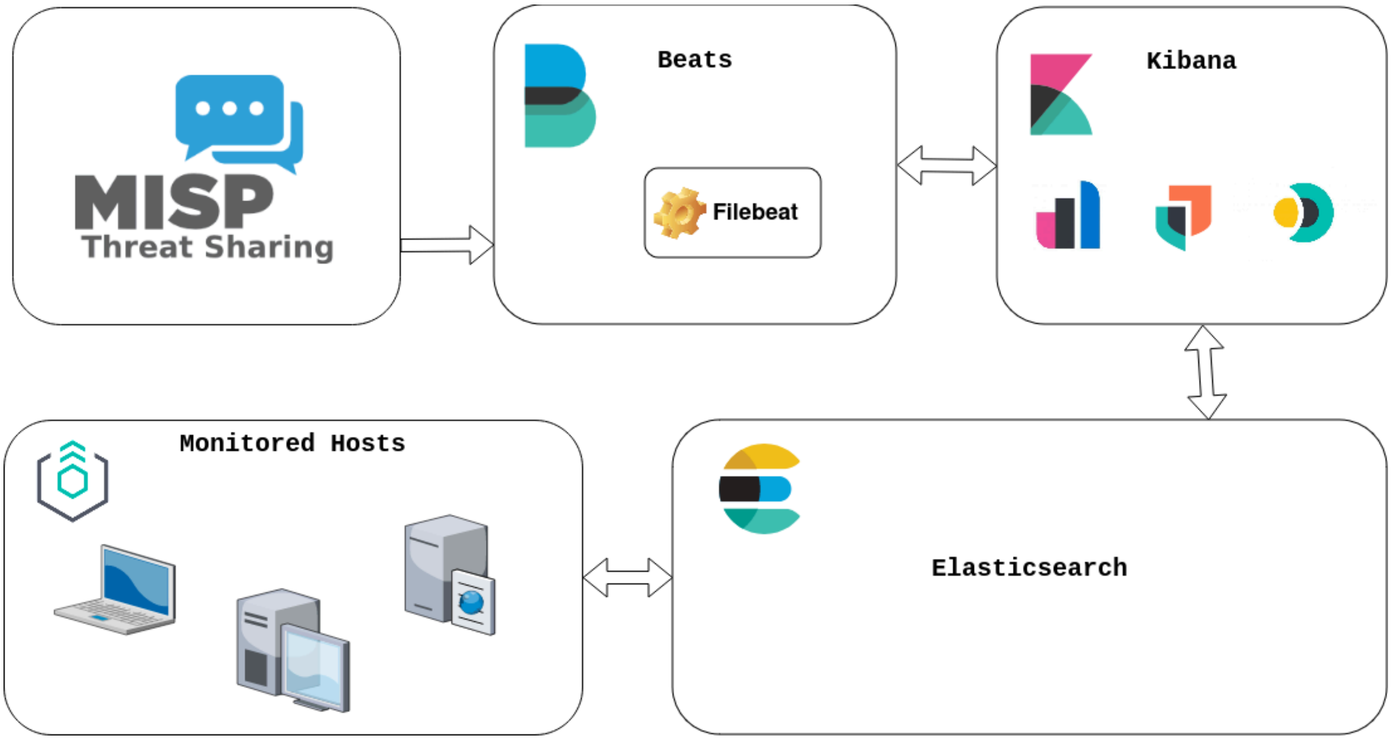
MISP - ELASTIC STACK - DOCKER LAB

BY LUCIANO RIGHETTI (/AUTHORS/LUCIANO-RIGHETTI) APRIL 5, 2024



MISP - Elastic Stack - Docker

This lab explains how to connect MISP to the Elastic Stack in order to leverage IOCs from MISP and trigger alerts based on user defined rules.

Elastic-MISP Overview Diagram

MISP is used to gather IOCs from different sources such as open source Threat Intelligence feeds.

Filebeat pulls IOCs from MISP and pushed them to the Elasticsearch instance via the Threat Intel module [1].

To simplify this guide Elastic Agent [2] in installed standalone mode is installed on the hosts we want to monitor, but Fleet [3] could be used instead.

Kibana [4] is used for exploring the IOCs, creating rules and visualizing the alerts.

Everything in this lab is run on Docker [5].

Installation

1. Clone the lab repository.

```
$ git clone https://github.com/righel/elastic-misp-docker-lab.git & cd elastic-misp-docker-lab
```

MISP

2. Create the .env file:

```
$ cp template.env .env
```

3. Start the MISP containers.

```
$ docker compose up -d
```

4. When MISP containers finish starting, create a sync user for Elastic on MISP.

   Using MISP CLI:

```
$ docker-compose exec misp-core app/Console/cake User create elastic@admin.test 5 1
$ docker-compose exec misp-core app/Console/cake User change_authkey elastic2@admin.test
Old authentication keys disabled and new key created: 06sDmKQK3E6MSJwsOhYT3N4NzfTpe53ruV0Bydf0
```

   Using MISP UI:

   Default MISP credentials

> User: admin@admin.test (mailto:admin@admin.test)
>
> Password: admin

Elastic Stack

> The yaml configuration files for Elasticsearch, Kibana and Filebeat are located in `elastic/config/` directory. You can review and change these settings before deploying Elastic Stack.

For adjusting the Filebeat MISP Threat Intel module, check `elastic/config/filebeat.yml`:

```
filebeat.modules:
  - module: threatintel
    misp:
      enabled: true
      var.input: httpjson
      var.url: "https://${MISP_HOST}/events/restSearch"
      var.api_token: "${MISP_ELASTIC_API_KEY}"
      var.first_interval: 24h
      var.interval: 10m
      var.ssl.verification_mode: none
      var.filters:
        type: ["md5", "sha256", "sha512", "url", "uri", "ip-src", "ip-dst", "hostname", "domain"]
        tags: ['workflow:state="complete"']
```

For more details refer to the official docs:

- https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-module-threatintel.html#misp (https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-module-threatintel.html#misp)

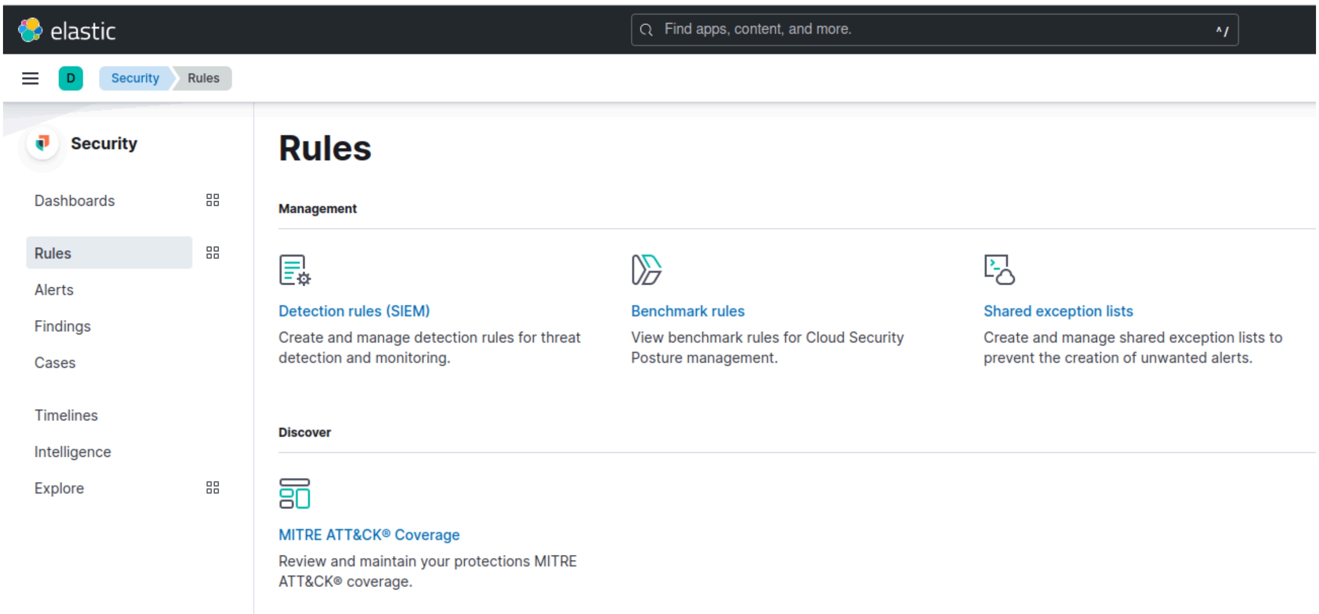
5. Modify some environment variables before firing up Elastic Stack.
   - `KIBANA_ENCRYPTION_KEY` : Has to be 32 chars string to set up `xpack.encryptedSavedObjects.encryptionKey` on Kibana.
   - `MISP_ELASTIC_API_KEY` : The MISP API key generated in step 4 for the sync user `elastic@admin.test` .
6. Start the Elastic Stack containers.

```
$ docker-compose -f docker-compose.elastic.yml -d
```

Now you can use MISP and the Elastic Stack.

Creating Kibana detection rules

1. Go to *Kibana* > *Security* > *Rules* and click on *Detection rules (SIEM)*



Rules

Management

Detection rules (SIEM)
Create and manage detection rules for threat detection and monitoring.

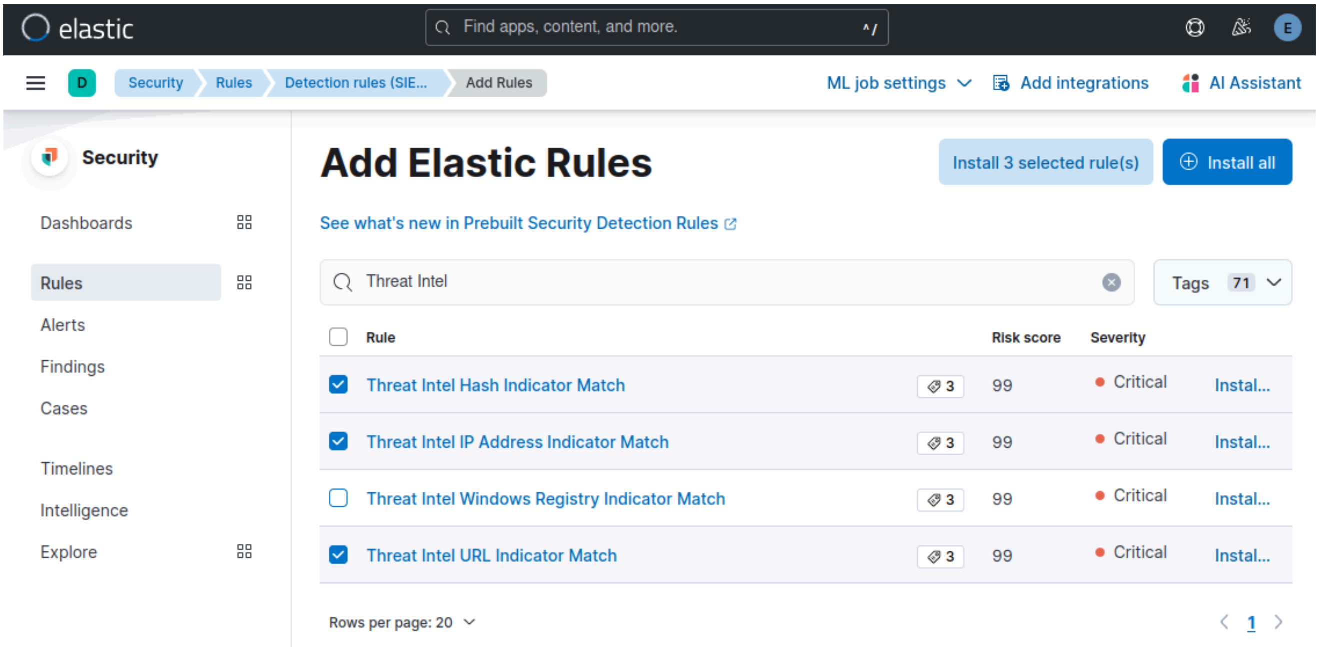
Benchmark rules
View benchmark rules for Cloud Security Posture management.

Shared exception lists
Create and manage shared exception lists to prevent the creation of unwanted alerts.

Discover

MITRE ATT&CK® Coverage
Review and maintain your protections MITRE ATT&CK® coverage.

2. Click on
   ⊕ Add Elastic rules 1083
   and search for *Threat Intel*, and select the rules you are interested on.



Add Elastic Rules

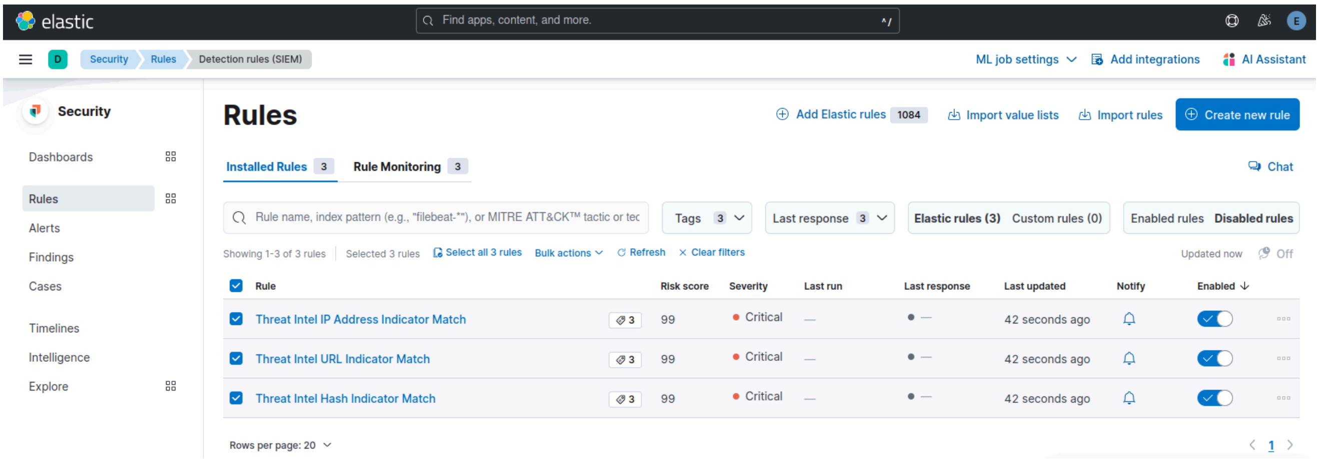
Threat Intel

	Rule		Risk score	Severity	
☑	Threat Intel Hash Indicator Match	3	99	● Critical	Instal...
☑	Threat Intel IP Address Indicator Match	3	99	● Critical	Instal...
□	Threat Intel Windows Registry Indicator Match	3	99	● Critical	Instal...
☑	Threat Intel URL Indicator Match	3	99	● Critical	Instal...

3. Click on

   Install 3 selected rule(s)

4. Go back to *Kibana* > *Security* > *Rules* and click on *Detection rules (SIEM)*, click on the *Disabled rules* filter to show the recently installed rules (by default they are disabled), and enable them.



Rules

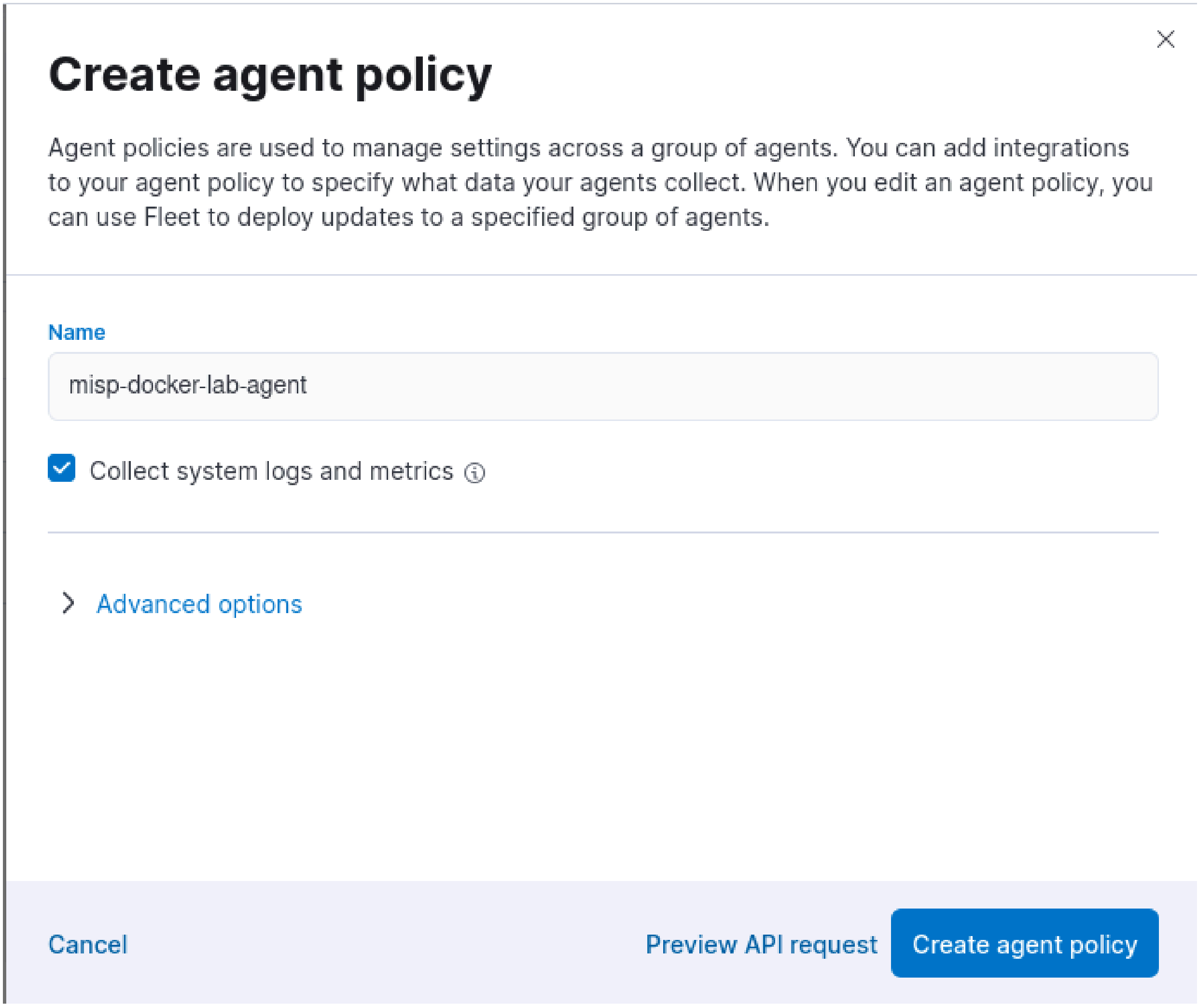
☑	Rule		Risk score	Severity	Last run	Last response	Last updated	Notify	Enabled
☑	Threat Intel IP Address Indicator Match	3	99	● Critical	—	● —	42 seconds ago		✓
☑	Threat Intel URL Indicator Match	3	99	● Critical	—	● —	42 seconds ago		✓
☑	Threat Intel Hash Indicator Match	3	99	● Critical	—	● —	42 seconds ago		✓

Now Elastic will generate alerts if it detects any hash, url or domain matching with MISP IOCs.

Demo

Install Elastic Agent (standalone)

1. Go to *Kibana* > *Management* > *Fleet* and switch to the *Agent policies* tab and click on the *Create agent policy* button.



Create agent policy

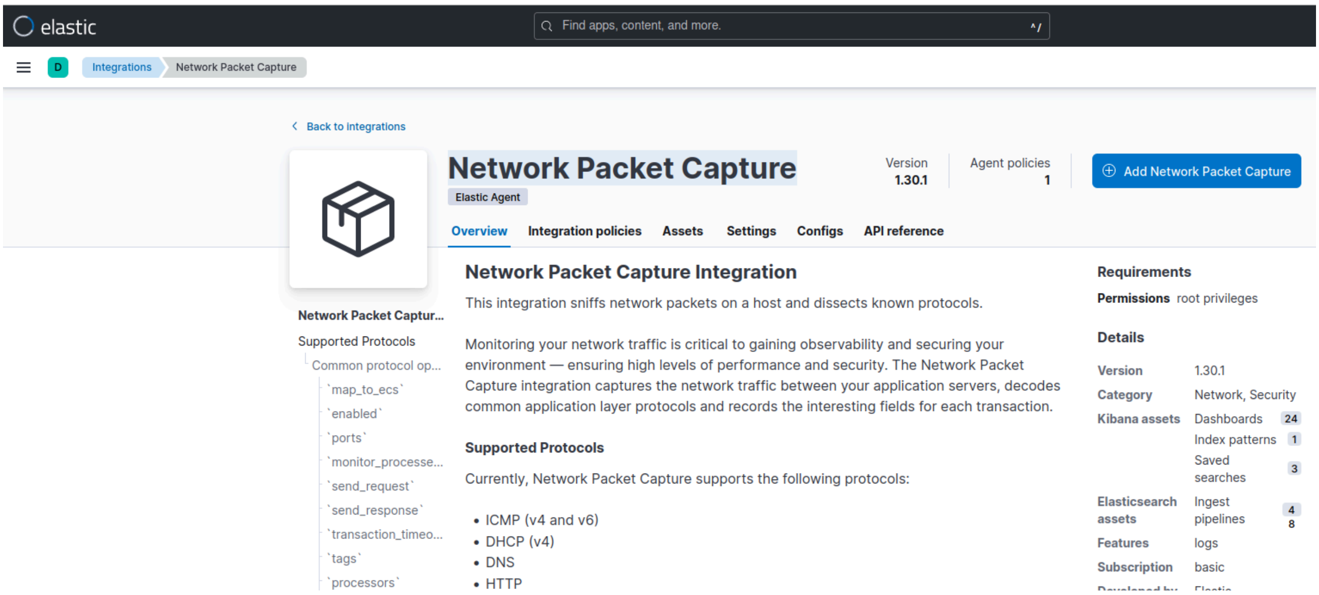
Agent policies are used to manage settings across a group of agents. You can add integrations to your agent policy to specify what data your agents collect. When you edit an agent policy, you can use Fleet to deploy updates to a specified group of agents.

Name

misp-docker-lab-agent

☑ Collect system logs and metrics

2. Click on the policy to access it and click on *Add integration* and search for *Network Packet Capture*, click on it and click on *Add Network Packet Capture*



Network Packet Capture

Elastic Agent

Version 1.30.1 | Agent policies 1

Network Packet Capture Integration

This integration sniffs network packets on a host and dissects known protocols.

Monitoring your network traffic is critical to gaining observability and securing your environment — ensuring high levels of performance and security. The Network Packet Capture integration captures the network traffic between your application servers, decodes common application layer protocols and records the interesting fields for each transaction.

Supported Protocols

Currently, Network Packet Capture supports the following protocols:

- ICMP (v4 and v6)
- DHCP (v4)
- DNS
- HTTP

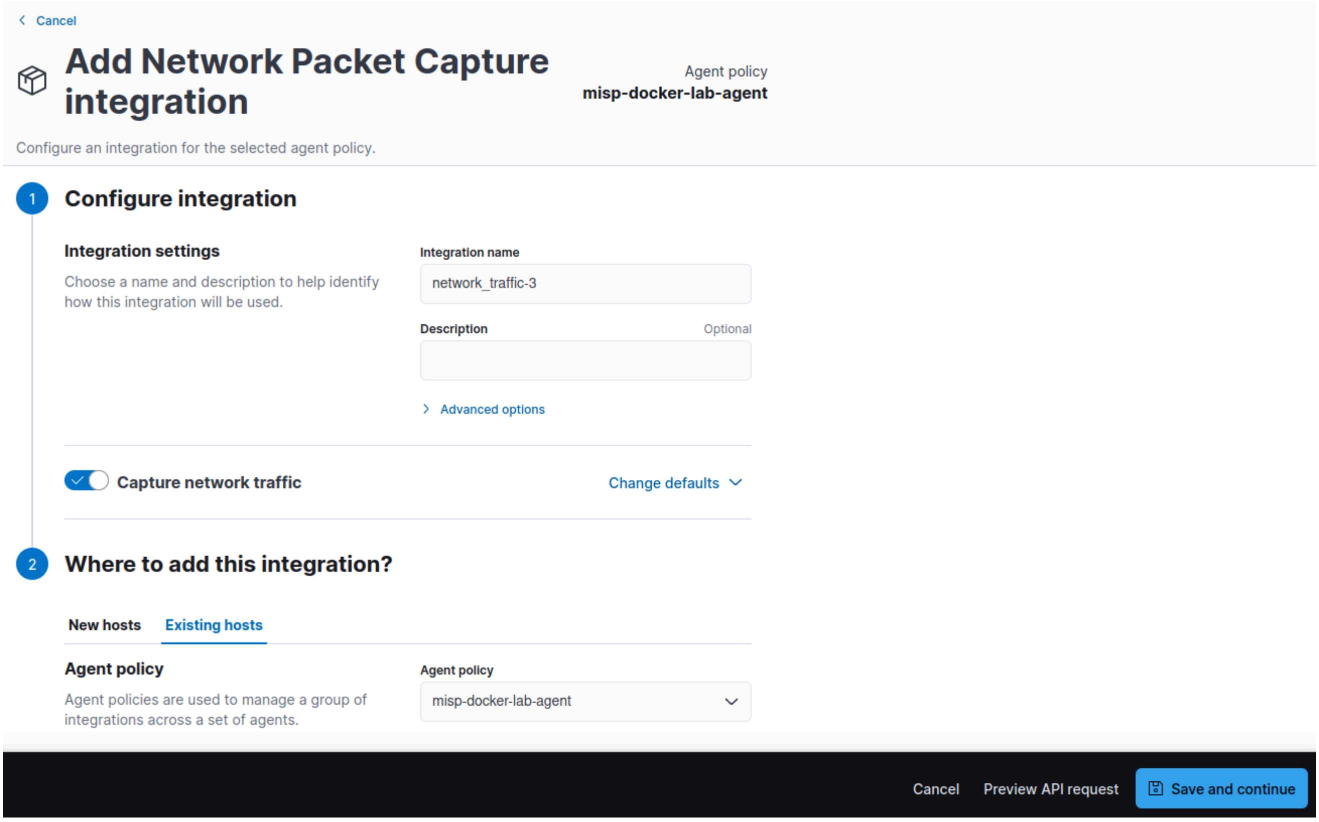
Requirements

Permissions root privileges

Details

Version	1.30.1	
Category	Network, Security	
Kibana assets	Dashboards	24
	Index patterns	1
	Saved searches	3
Elasticsearch assets	Ingest pipelines	4 8
Features	logs	
Subscription	basic	

3. Configure the Network Packet Capture integration if needed.



Add Network Packet Capture integration

Agent policy
misp-docker-lab-agent

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: network_traffic-3

Description (Optional):

› Advanced options

☑ Capture network traffic — Change defaults

2 Where to add this integration?

New hosts | Existing hosts

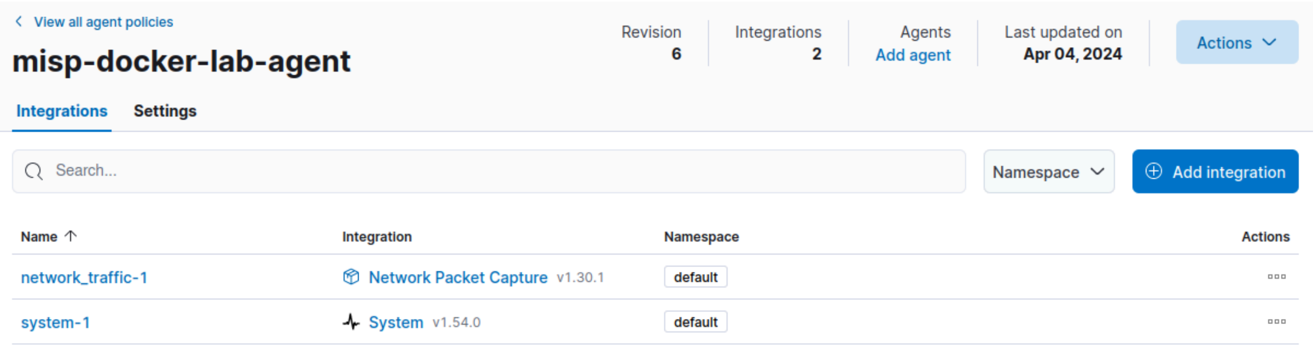
Agent policy

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

Agent policy: misp-docker-lab-agent

Click on *Save and continue*.

> If prompted to add a Elastic Agent, click on *Add Elastic Agent later*.

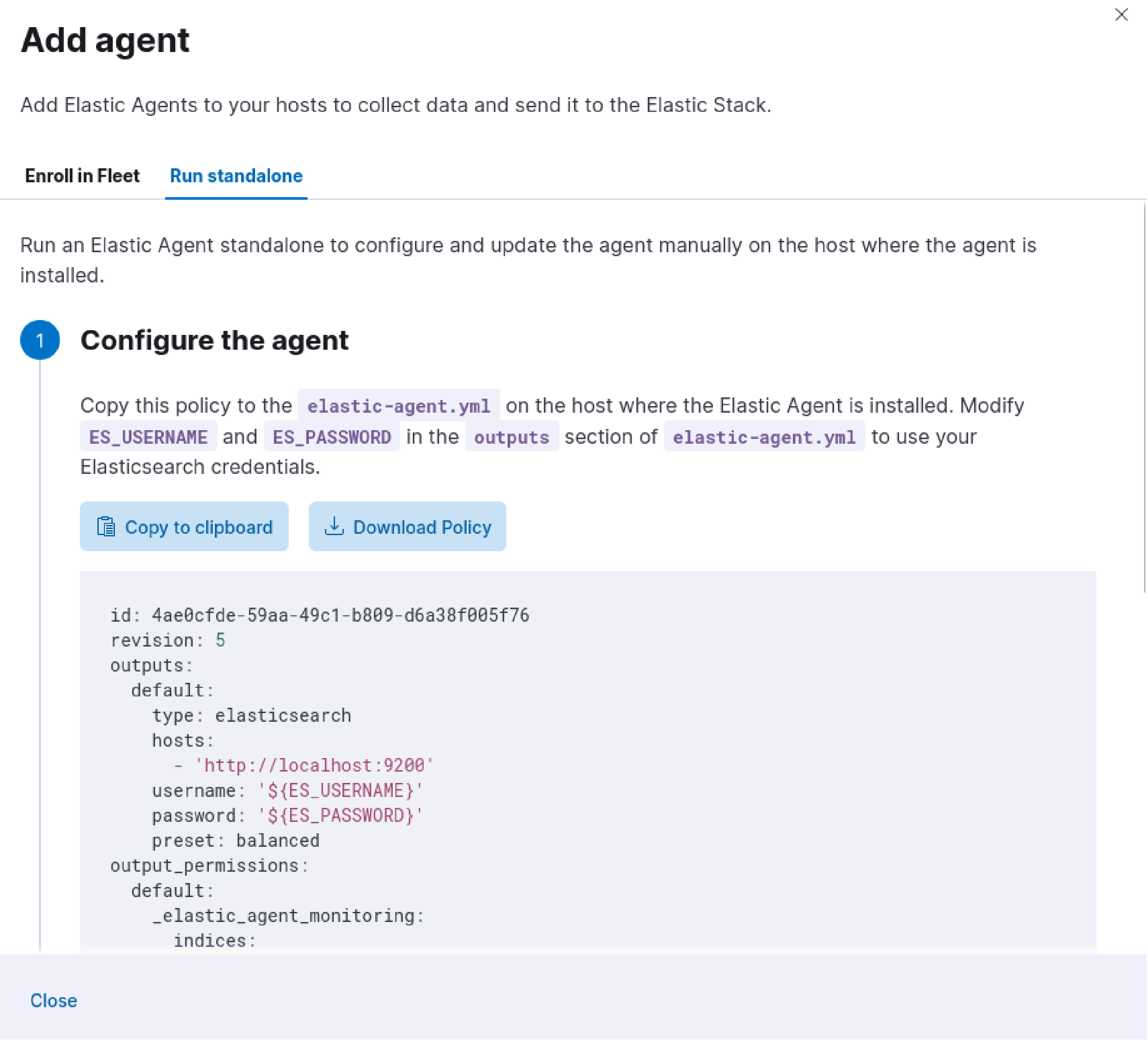


misp-docker-lab-agent

Revision	Integrations	Agents	Last updated on
6	2	Add agent	Apr 04, 2024

Name ↑	Integration	Namespace	Actions
network_traffic-1	Network Packet Capture v1.30.1	default	···
system-1	System v1.54.0	default	···

4. Click on *Actions* > *Add agent*, switch to the *Run standalone* tab.



Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.

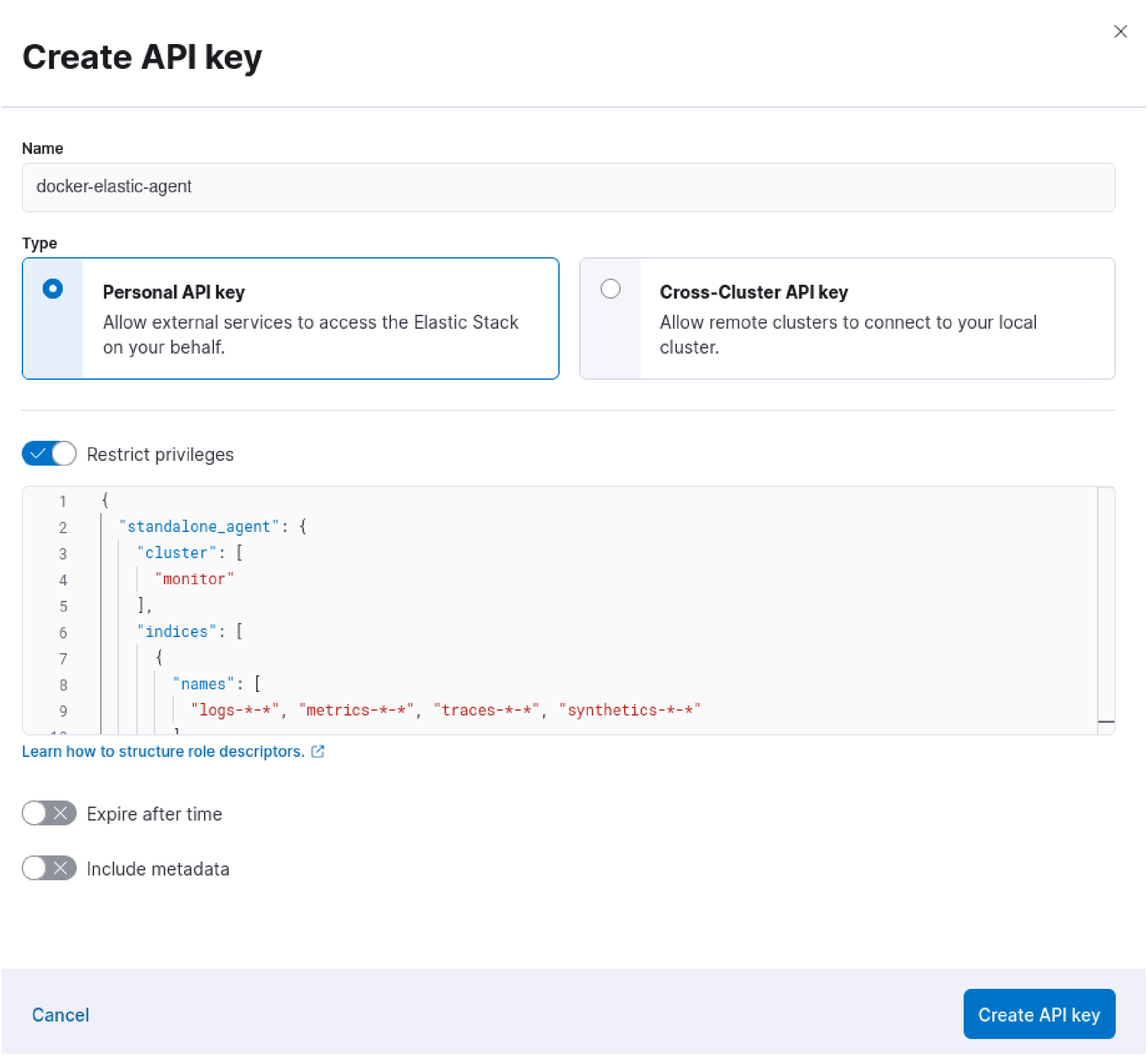
Run an Elastic Agent standalone to configure and update the agent manually on the host where the agent is installed.

Copy this policy to the `elastic-agent.yml` on the host where the Elastic Agent is installed. Modify `ES_USERNAME` and `ES_PASSWORD` in the `outputs` section of `elastic-agent.yml` to use your Elasticsearch credentials.

```
id: 4ae0cfde-59aa-49c1-b809-d6a38f005f76
revision: 5
outputs:
  default:
    type: elasticsearch
    hosts:
      - 'http://localhost:9200'
    username: '${ES_USERNAME}'
    password: '${ES_PASSWORD}'
    preset: balanced
output_permissions:
  default:
    _elastic_agent_monitoring:
      indices:
```

Click on *Download Policy*.

5. Create an API key for the Elastic Agent communication to Elasticsearch [6]. Navigate to *Kibana* > *Stack Management* > *API keys* and click Create API key.



Create API key

Name

docker-elastic-agent

Type

● **Personal API key**
Allow external services to access the Elastic Stack on your behalf.

○ **Cross-Cluster API key**
Allow remote clusters to connect to your local cluster.

✓ Restrict privileges

```
{
  "standalone_agent": {
    "cluster": [
      "monitor"
    ],
    "indices": [
      {
        "names": [
          "logs-*-*", "metrics-*-*", "traces-*-*", "synthetics-*-*"
```

Learn how to structure role descriptors.

Expire after time

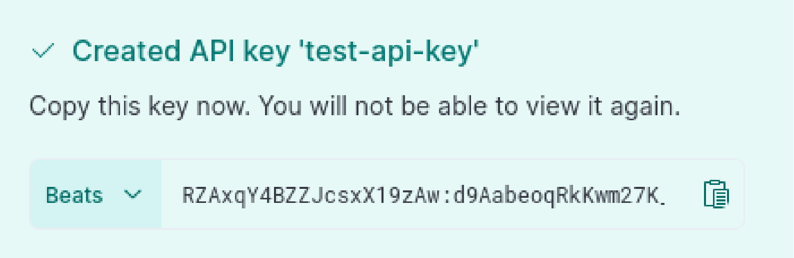
Include metadata

1. Enable the *Restrict privileges* toggle and copy the following configuration.

```
{
  "standalone_agent": {
    "cluster": [
      "monitor"
    ],
    "indices": [
      {
        "names": [
          "logs-*-*", "metrics-*-*", "traces-*-*", "synthetics-*-*"
        ],
        "privileges": [
          "auto_configure", "create_doc"
        ]
      }
    ]
  }
}
```

2. Click on *Create API key*.

3. Select *Beats* and copy the API key.



Created API key 'test-api-key'

Copy this key now. You will not be able to view it again.

RZAxqY4BZZJcsxX19zAw:d9AabeoqRkKwm27K_

6. Open the `elastic-agent.yml` configuration downloaded on step 5 and modify the `outputs` section it to use API authentication and change the Elasticsearch host from `localhost` to `elasticsearch`.

```
outputs:
  default:
    type: elasticsearch
    hosts:
      - 'http://elasticsearch:9200'
    api_key: 'RZAxqY4BZZJcsxX19zAw:d9AabeoqRkKwm27K_KEgKA'
    preset: balanced
```

7. Install Elastic Agent in the host we want to monitor. Start an Ubuntu container and plug it to the MISP-Elastic Stack lab network.

```
$ docker run -it --network=elastic-misp-docker-lab_default --name=my_monitored_host ubuntu
```

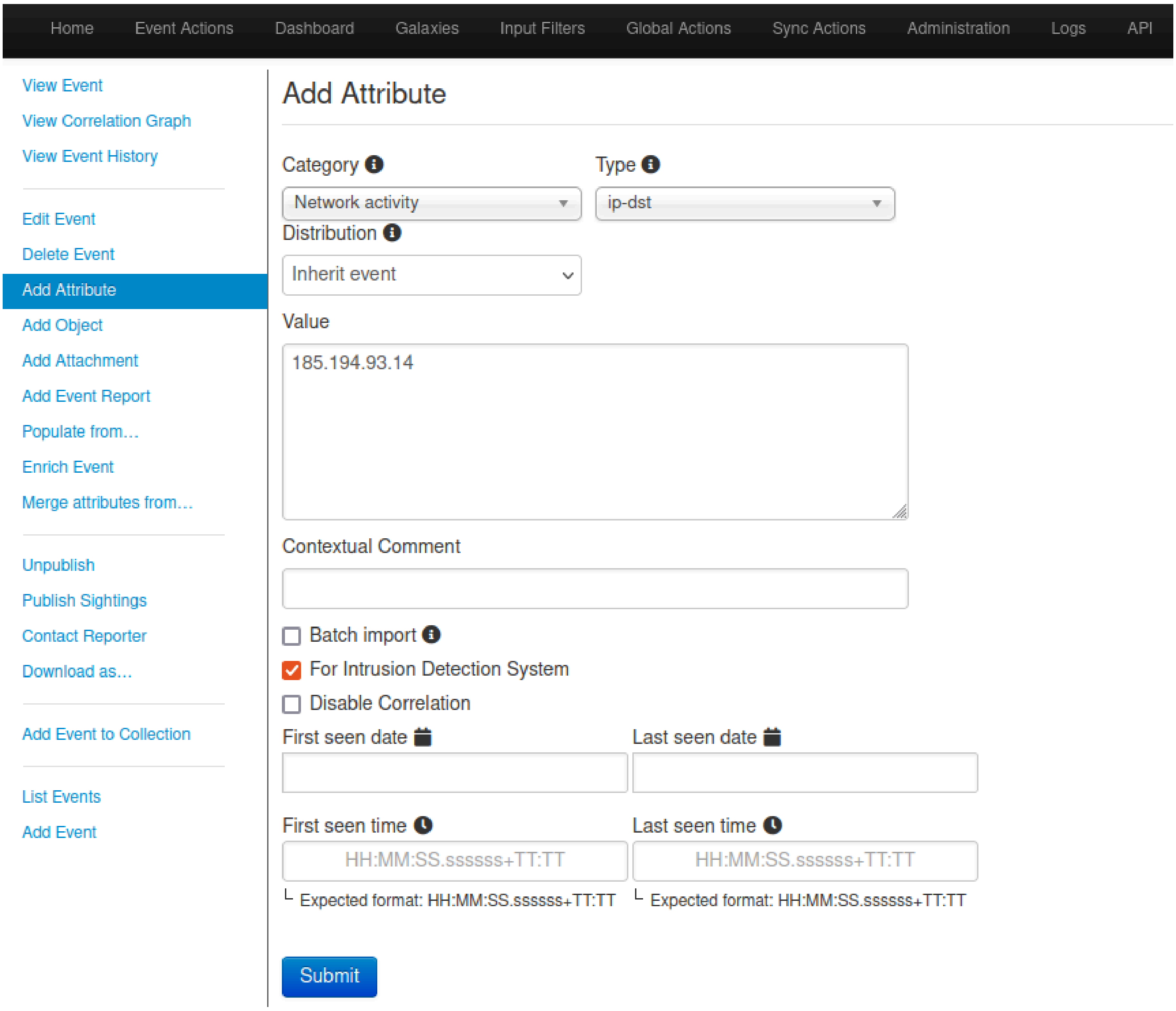
8. Follow the steps to install the standalone Elastic Agent [7].

```
$ curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.13.
1-linux-x86_64.tar.gz
root@be44a9a86e24:/# apt update
...
root@be44a9a86e24:/# apt install curl -y
...
root@be44a9a86e24:/# cd /tmp
root@be44a9a86e24:/# curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/
elastic-agent-8.13.1-linux-x86_64.tar.gz
root@be44a9a86e24:/# tar xzvf elastic-agent-8.13.1-linux-x86_64.tar.gz
...

# from a different terminal, copy the elastic-agent.yml config file into the container
docker cp elastic-agent.yml my_monitored_host:/tmp/elastic-agent-8.13.1-linux-x86_64/elasti
c-agent.yml

# back on the docker terminal, install the agent
root@be44a9a86e24:/# cd elastic-agent-8.13.1-linux-x86_64/
root@be44a9a86e24:/# ./elastic-agent install
    Elastic Agent will be installed at /opt/Elastic/Agent and will run as a service. Do you
want to continue? [Y/n]:Y
    Do you want to enroll this Agent into Fleet? [Y/n]:n
    [=   ] Service Started  [32s] Elastic Agent successfully installed, starting enrollmen
t.
    [=   ] Done  [32s]
    Elastic Agent has been successfully installed.
```

Done. Now the docker container is being monitored by the Elastic Agent and the metrics are being pushed to Elasticsearch.

Testing

1. Go to MISP, create a new Event an add a *ip-dst* type attribute. 2.



Add Attribute

Category: Network activity

Type: ip-dst

Distribution: Inherit event

Value: 185.194.93.14

Contextual Comment:

□ Batch import

☑ For Intrusion Detection System

□ Disable Correlation

First seen date:

Last seen date:

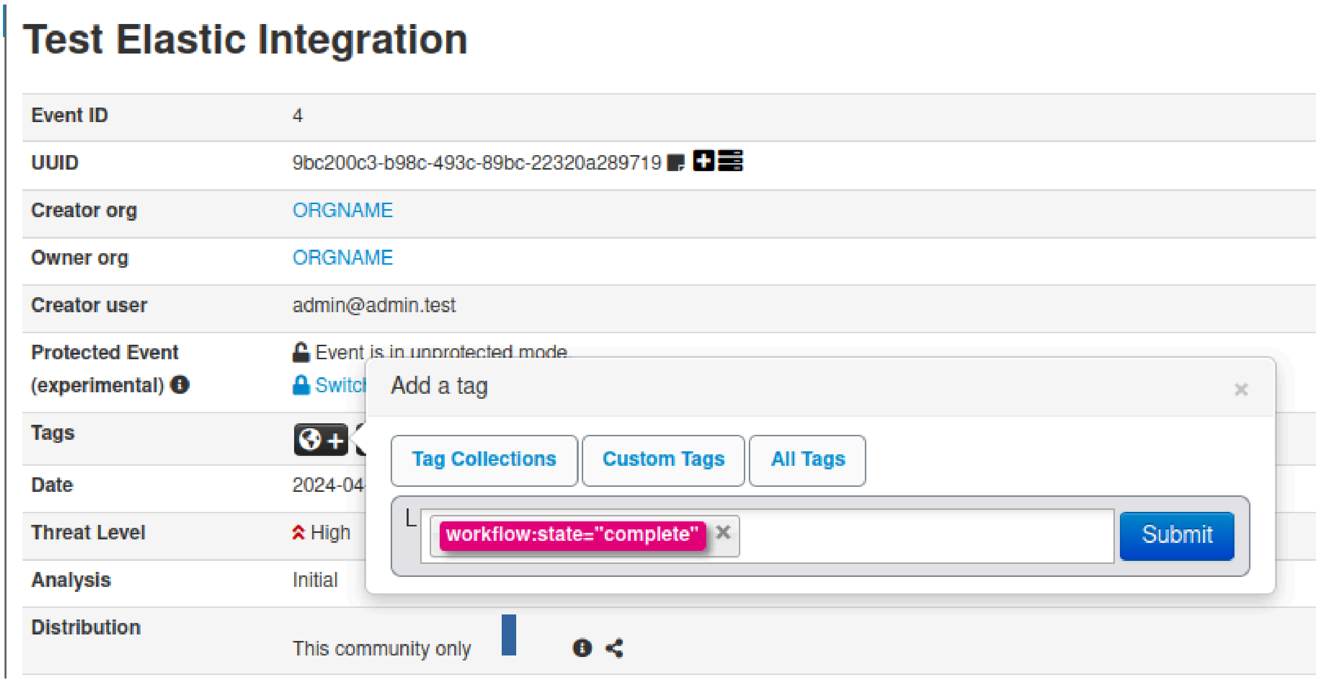
First seen time: HH:MM:SS.ssssss+TT:TT

└ Expected format: HH:MM:SS.ssssss+TT:TT

Last seen time: HH:MM:SS.ssssss+TT:TT

└ Expected format: HH:MM:SS.ssssss+TT:TT

2. Add the *workflow:state="complete"* tag to the event to it is picked up by Elasticsearch.



Test Elastic Integration

Event ID	4
UUID	9bc200c3-b98c-493c-89bc-22320a289719
Creator org	ORGNAME
Owner org	ORGNAME
Creator user	admin@admin.test
Protected Event (experimental)	Event is in unprotected mode. Switc
Tags	
Date	2024-04
Threat Level	High
Analysis	Initial
Distribution	This community only

workflow:state="complete"

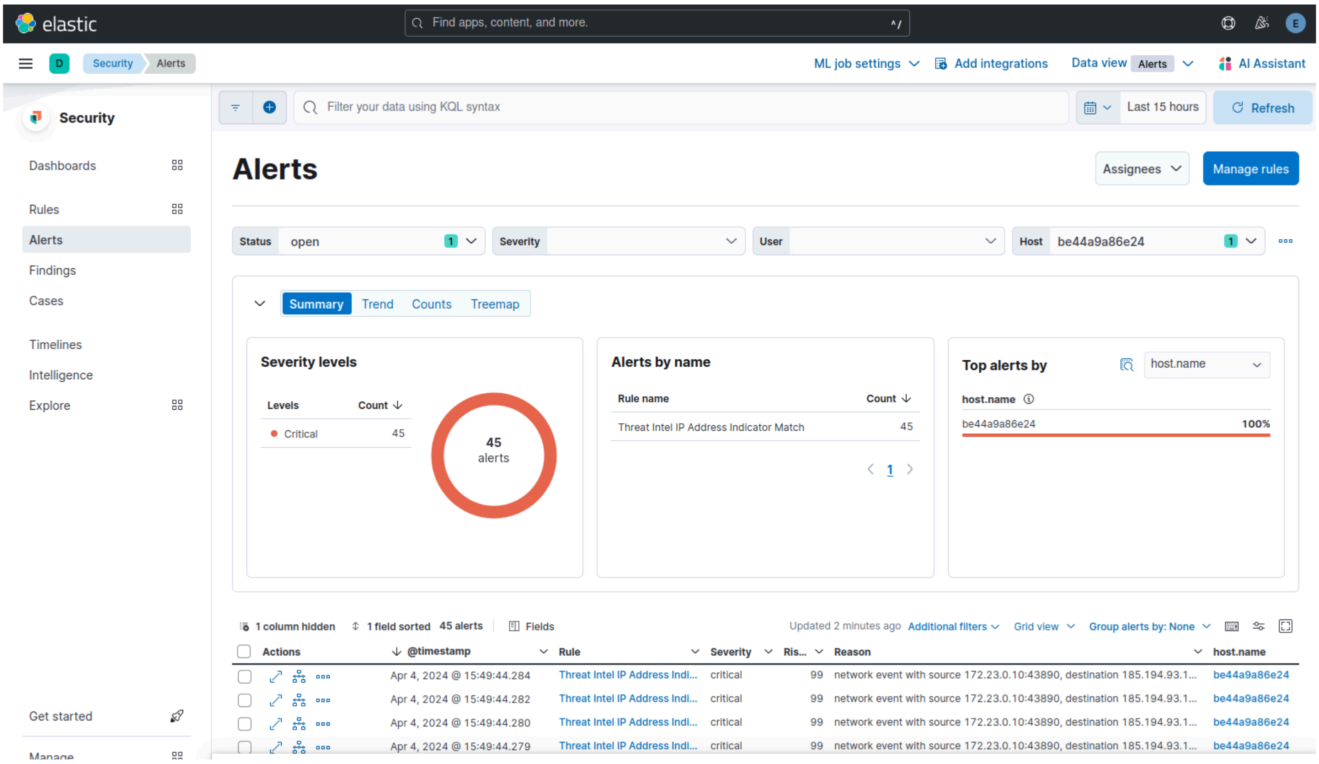
3. Publish the Event.

> Depending on the `vars.interval` set on the Threat Intel module in the `filebeat.yml` configuration file, it may take some time for the IOC to get into Elasticsearch.

4. From your monitored docker host, generate traffic to one of the MISP IOCs.

```
root@be44a9a86e24:/# curl -I https://circl.lu
...
```

5. Navigate to *Kibana* > *Security* > *Alerts*, you should now see some alerts triggered by the *Threat Intel IP Address Indicator Match*.



Alerts

Status: open | Severity | User | Host: be44a9a86e24

Levels	Count
Critical	45

Rule name	Count
Threat Intel IP Address Indicator Match	45

host.name	
be44a9a86e24	100%

45 alerts

Actions	@timestamp	Rule	Severity	Ris...	Reason	host.name
	Apr 4, 2024 @ 15:49:44.284	Threat Intel IP Address Indi...	critical	99	network event with source 172.23.0.10:43890, destination 185.194.93.1...	be44a9a86e24
	Apr 4, 2024 @ 15:49:44.282	Threat Intel IP Address Indi...	critical	99	network event with source 172.23.0.10:43890, destination 185.194.93.1...	be44a9a86e24
	Apr 4, 2024 @ 15:49:44.280	Threat Intel IP Address Indi...	critical	99	network event with source 172.23.0.10:43890, destination 185.194.93.1...	be44a9a86e24
	Apr 4, 2024 @ 15:49:44.279	Threat Intel IP Address Indi...	critical	99	network event with source 172.23.0.10:43890, destination 185.194.93.1...	be44a9a86e24

> By default Elastic runs these detection rules every 4 hours, you can configure the internal reduce

Done! Now you will get alerts on Kibana when an event in one of your monitored hosts matches a MISP IOC.

---

1. https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-module-threatintel.html (https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-module-threatintel.html) ↩
2. https://www.elastic.co/guide/en/fleet/current/install-standalone-elastic-agent.html (https://www.elastic.co/guide/en/fleet/current/install-standalone-elastic-agent.html) ↩
3. https://www.elastic.co/guide/en/fleet/current/fleet-overview.html (https://www.elastic.co/guide/en/fleet/current/fleet-overview.html) ↩
4. https://www.elastic.co/kibana (https://www.elastic.co/kibana) ↩
5. https://github.com/righel/elastic-misp-docker-lab (https://github.com/righel/elastic-misp-docker-lab) ↩
6. https://www.elastic.co/guide/en/fleet/current/grant-access-to-elasticsearch.html (https://www.elastic.co/guide/en/fleet/current/grant-access-to-elasticsearch.html) ↩

7. https://www.elastic.co/guide/en/fleet/current/install-standalone-elastic-agent.html (https://www.elastic.co/guide/en/fleet/current/install-standalone-elastic-agent.html) ↩

SEARCH

Search

TAGS

ALERTS (/TAGS/ALERTS) ANALYST NOTES (/TAGS/ANALYST-NOTES)

ANALYST OPINIONS (/TAGS/ANALYST-OPINIONS) AUTOMATION (/TAGS/AUTOMATION)

AZURE (/TAGS/AZURE) BLOOM FILTER (/TAGS/BLOOM-FILTER) BOT (/TAGS/BOT)

CACTI (/TAGS/CACTI) CLUSTER (/TAGS/CLUSTER) COGNITIVE SECURITY (/TAGS/COGNITIVE-SECURITY)

COLLECTING (/TAGS/COLLECTING) CRAWLING (/TAGS/CRAWLING) CURATION (/TAGS/CURATION)

DISINFORMATION (/TAGS/DISINFORMATION) DOCKER (/TAGS/DOCKER) EDR (/TAGS/EDR)

ELASTIC (/TAGS/ELASTIC) ELASTICSEARCH (/TAGS/ELASTICSEARCH) FILEBEAT (/TAGS/FILEBEAT)

GALAXY (/TAGS/GALAXY) HARFANGLAB (/TAGS/HARFANGLAB) HONEYPOT (/TAGS/HONEYPOT)

IMPORT SCRIPT (/TAGS/IMPORT-SCRIPT) INFORMATION OPERATIONS (/TAGS/INFORMATION-OPERATIONS)

INFORMATION SHARING (/TAGS/INFORMATION-SHARING) INTEGRATION (/TAGS/INTEGRATION)

JUPYTER (/TAGS/JUPYTER) KUNAI (/TAGS/KUNAI) MASTODON (/TAGS/MASTODON)

MICROSOFT (/TAGS/MICROSOFT) MISP (/TAGS/MISP) MISP STANDARD (/TAGS/MISP-STANDARD)

MISP-MODULES (/TAGS/MISP-MODULES) MODULES (/TAGS/MODULES)

MONITORING (/TAGS/MONITORING) NOTEBOOKS (/TAGS/NOTEBOOKS) OBJECT (/TAGS/OBJECT)

OBJECTS (/TAGS/OBJECTS) OPENNMS (/TAGS/OPENNMS) PLAYBOOKS (/TAGS/PLAYBOOKS)

POPPY (/TAGS/POPPY) PROCEDURE (/TAGS/PROCEDURE) RELEASE (/TAGS/RELEASE)

SCRAPING (/TAGS/SCRAPING) SENTINEL (/TAGS/SENTINEL) SHARING (/TAGS/SHARING)

SIGINT (/TAGS/SIGINT) SIGMF (/TAGS/SIGMF) SIGNAL INTELLIGENCE (/TAGS/SIGNAL-INTELLIGENCE)

STIX (/TAGS/STIX) THREAT INTELLIGENCE (/TAGS/THREAT-INTELLIGENCE) TWITTER (/TAGS/TWITTER)

YETI (/TAGS/YETI)

ABOUT US

About us (/who/)

(https://www.misp-standard.org/)

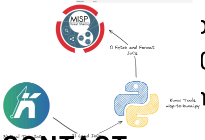
(/thanks)

RECENT POSTS

MISP 2.4.192 RELEASED WITH MANY PERFORMANCE IMPROVEMENT, FIXES AND UPDATES. (HTTPS://WWW.MISP-PROJECT.ORG/2024/05/07/MISP.2.4.192.RELEASED.HTML/)

o-
05/07/MISP.2.4.192.released.html/)

MISP 2.4.190 (AND 2.4.191) RELEASED WITH NEW FEED IMPROVEMENT, WORKFLOWS AND A NEW BENCHMARKING SUITE. (HTTPS://WWW.MISP-PROJECT.ORG/2024/04/22/MISP.2.4.190-2.4.191-RELEASED.HTML/)



o-
04/22/MISP.2.4.190-
html/)

USING YOUR MISP IOCS IN KUNAI (THE OPEN SOURCE EDR FOR LINUX) (HTTPS://WWW.MISP-PROJECT.ORG/2024/04/19/USING-YOUR-MISP-IOCS-IN-KUNAI.HTML/)

(https://www.misp-project.org/2024/04/19/Using-Your-MISP-IoCs-in-Kunai.html/)

CONTACT

GO TO CONTACT PAGE (/SUPPORT)

Template by Bootstrapious (https://bootstrapious.com/p/universal-business-e-commerce-template). Ported to Hugo by DevCows (https://github.com/devcows/hugo-universal-theme). Mastodon (https://misp-community.org/@misp)