Enrichment pipeline

Week 2.5 - Lab

Day 5 – Enrichment Pipelines & Tuning Playbooks

Lead: *Muhammad Tayyab*
Athar Imran
Buildables Cybersecurity Fellow

9th of *September, 2025 - Tuesday*

In this lab, we design and then validate an enrichment pipeline using Logstash. We ingested IPs through the pipeline, and then Logstash enriches them using GeoIP and ThreatIntel. This way, we can get more valuable information in the alert.

Pipeline Design:

Input:

Logstash ingests logs from input.json via the file input plugin. This file contains IP lists.

Filters:

GeoIP Enrichment:

First, we added the MaxMind GeoLite2 database. It extracts geolocation details (country, city, lat/lon) from the source_ip field.

Output:

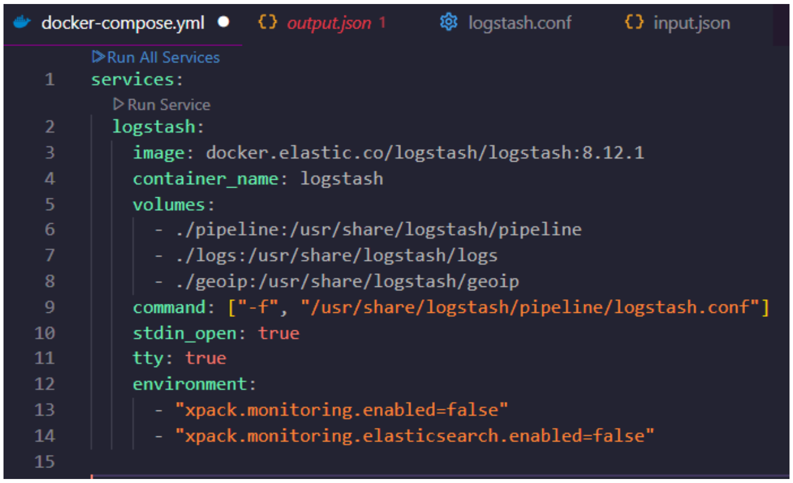
Those enriched events are written to output.json in JSON format.

Execution:

Docker-compose.yml:

This file runs Logstash with mounted volumes:

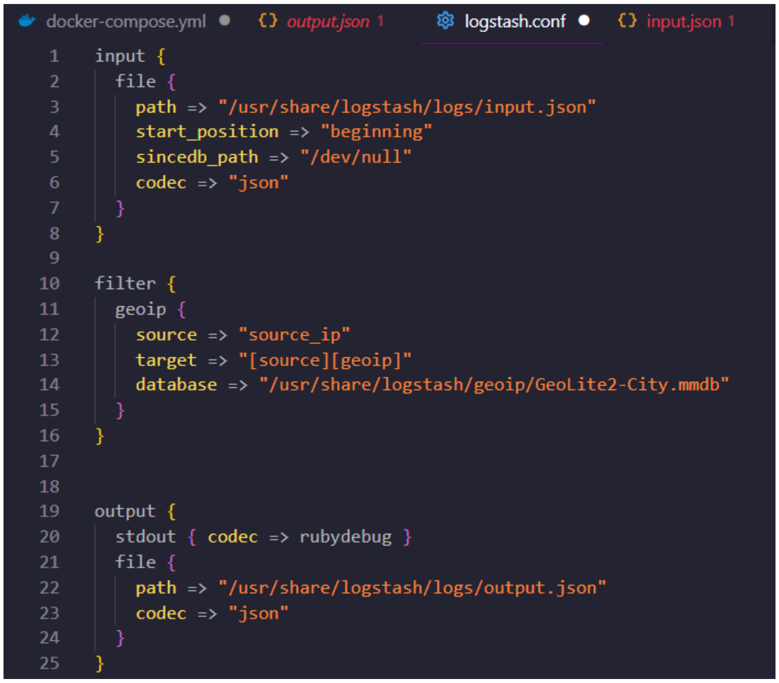
- /pipeline: Logstash config
- /logs :input/output data
- /geoip :MaxMind database



```yaml
services:
  logstash:
    image: docker.elastic.co/logstash/logstash:8.12.1
    container_name: logstash
    volumes:
      - ./pipeline:/usr/share/logstash/pipeline
      - ./logs:/usr/share/logstash/logs
      - ./geoip:/usr/share/logstash/geoip
    command: ["-f", "/usr/share/logstash/pipeline/logstash.conf"]
    stdin_open: true
    tty: true
    environment:
      - "xpack.monitoring.enabled=false"
      - "xpack.monitoring.elasticsearch.enabled=false"

```

logstash.conf:



```
input {
  file {
    path => "/usr/share/logstash/logs/input.json"
    start_position => "beginning"
    sincedb_path => "/dev/null"
    codec => "json"
  }
}

filter {
  geoip {
    source => "source_ip"
    target => "[source][geoip]"
    database => "/usr/share/logstash/geoip/GeoLite2-City.mmdb"
  }
}


output {
  stdout { codec => rubydebug }
  file {
    path => "/usr/share/logstash/logs/output.json"
    codec => "json"
  }
}
```

This file takes input from a JSON file specified. Then it applies filters on the parsed Source IP. Lastly, it gives the enriched output on the location specifed as JSON.

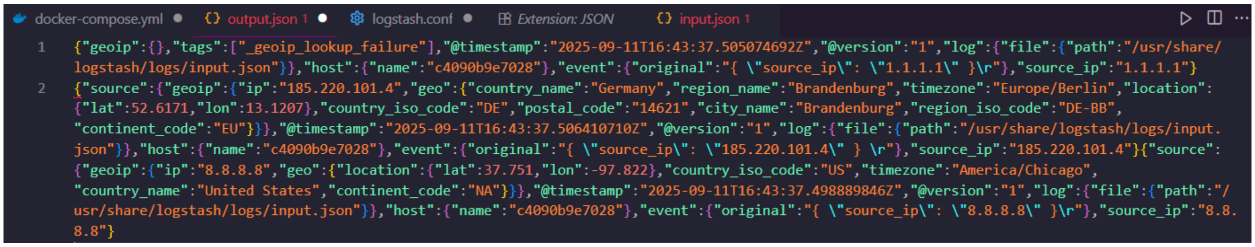
Input.json:

Inset list of target IPs:

Results:

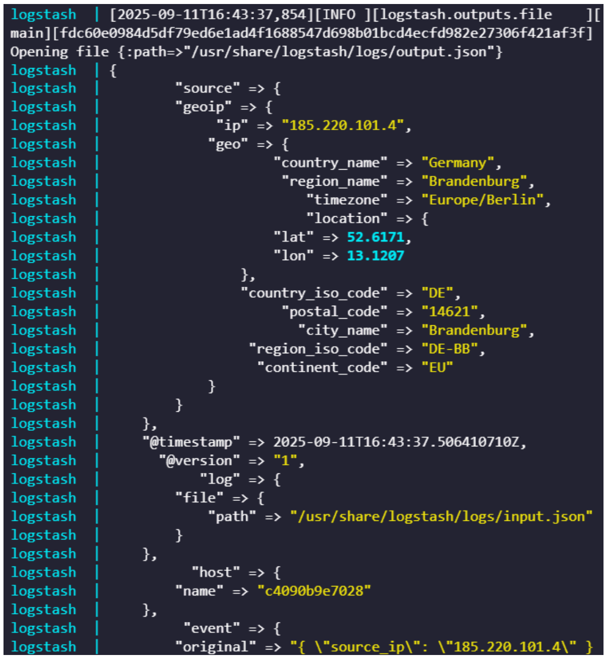
Run with: docker-compose up

Result saves in:



```
{"geoip":{},"tags":["_geoip_lookup_failure"],"@timestamp":"2025-09-11T16:43:37.505074692Z","@version":"1","log":{"file":{"path":"/usr/share/
logstash/logs/input.json"}},"host":{"name":"c4090b9e7028"},"event":{"original":"{ \"source_ip\": \"1.1.1.1\" }\r"},"source_ip":"1.1.1.1"}
{"source":{"geoip":{"ip":"185.220.101.4","geo":{"country_name":"Germany","region_name":"Brandenburg","timezone":"Europe/Berlin","location":
{"lat":52.6171,"lon":13.1207},"country_iso_code":"DE","postal_code":"14621","city_name":"Brandenburg","region_iso_code":"DE-BB",
"continent_code":"EU"}}},"@timestamp":"2025-09-11T16:43:37.506410710Z","@version":"1","log":{"file":{"path":"/usr/share/logstash/logs/input.
json"}},"host":{"name":"c4090b9e7028"},"event":{"original":"{ \"source_ip\": \"185.220.101.4\" } \r"},"source_ip":"185.220.101.4"}{"source":
{"geoip":{"ip":"8.8.8.8","geo":{"location":{"lat":37.751,"lon":-97.822},"country_iso_code":"US","timezone":"America/Chicago",
"country_name":"United States","continent_code":"NA"}}},"@timestamp":"2025-09-11T16:43:37.498889846Z","@version":"1","log":{"file":{"path":"/
usr/share/logstash/logs/input.json"}},"host":{"name":"c4090b9e7028"},"event":{"original":"{ \"source_ip\": \"8.8.8.8\" }\r"},"source_ip":"8.8.
8.8"}
```

Otherwise:



```
logstash  | [2025-09-11T16:43:37,854][INFO ][logstash.outputs.file    ][
main][fdc60e0984d5df79ed6e1ad4f1688547d698b01bcd4ecfd982e27306f421af3f]
Opening file {:path=>"/usr/share/logstash/logs/output.json"}
logstash  | {
logstash  |         "source" => {
logstash  |         "geoip" => {
logstash  |              "ip" => "185.220.101.4",
logstash  |             "geo" => {
logstash  |                     "country_name" => "Germany",
logstash  |                      "region_name" => "Brandenburg",
logstash  |                         "timezone" => "Europe/Berlin",
logstash  |                         "location" => {
logstash  |                     "lat" => 52.6171,
logstash  |                     "lon" => 13.1207
logstash  |                 },
logstash  |                 "country_iso_code" => "DE",
logstash  |                      "postal_code" => "14621",
logstash  |                        "city_name" => "Brandenburg",
logstash  |                  "region_iso_code" => "DE-BB",
logstash  |                   "continent_code" => "EU"
logstash  |             }
logstash  |         }
logstash  |     },
logstash  |     "@timestamp" => 2025-09-11T16:43:37.506410710Z,
logstash  |       "@version" => "1",
logstash  |            "log" => {
logstash  |         "file" => {
logstash  |             "path" => "/usr/share/logstash/logs/input.json"
logstash  |         }
logstash  |     },
logstash  |          "host" => {
logstash  |         "name" => "c4090b9e7028"
logstash  |     },
logstash  |         "event" => {
logstash  |         "original" => "{ \"source_ip\": \"185.220.101.4\" }
```