
Advanced Log Analysis

1. Objective

This report contains the details of the task includes Log Correlation, Anomaly Detection, and Log Enrichment. The goal of this task is to:

- Develop skills to analyze and correlate logs to uncover complex threats and reduce false positives.

2. Introduction

Advanced log analysis is a process of analyzing the logs in-depth that means gathering logs from various sources, finding errors, unwanted traffic, and adding context to the logs like (adding geolocation to an IP).

3. Tools

- Elastic Security setup using documentation
<https://www.elastic.co/downloads/elasticsearch>
- Security Onion setup using documentation
<https://docs.securityonion.net/en/2.4/pro.html>
- Google Sheets

4. Log Correlation

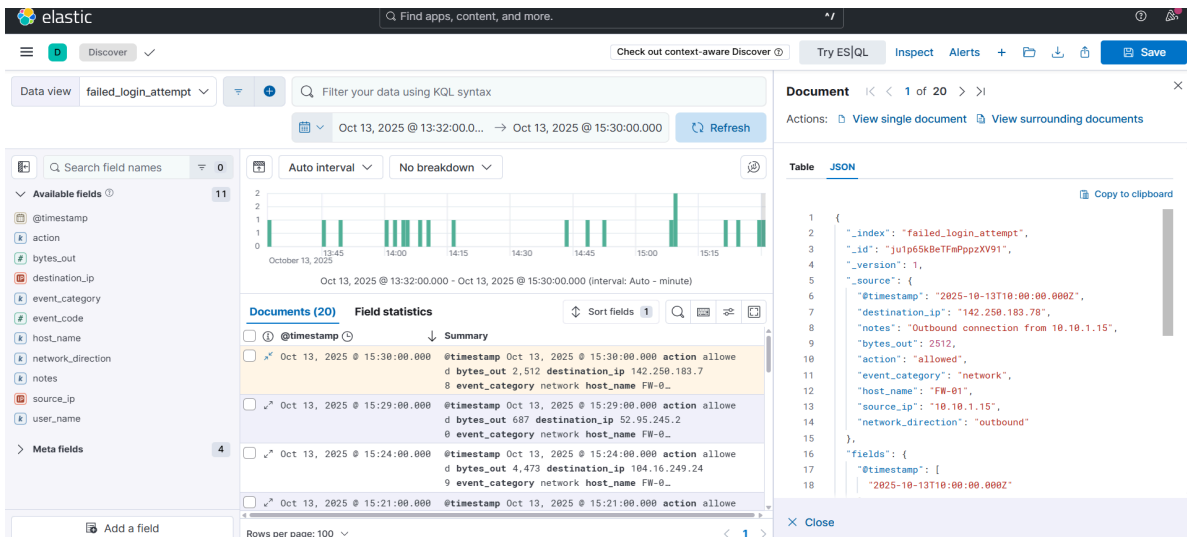
Log Correlation is a process of collecting or gathering logs from different sources and linking them to identify patterns. This log correlation is used to detect security threats, troubleshooting the problems to solve it by connecting different log entries that might not seem connected on their own.

Ingesting sample logs (e.g., from Boss of the SOC dataset) into elastic Security.

Correlating failed logins (Event ID 4625) with outbound traffic. Documenting metadata includes Event ID, Source IP, Destination IP, and Notes.

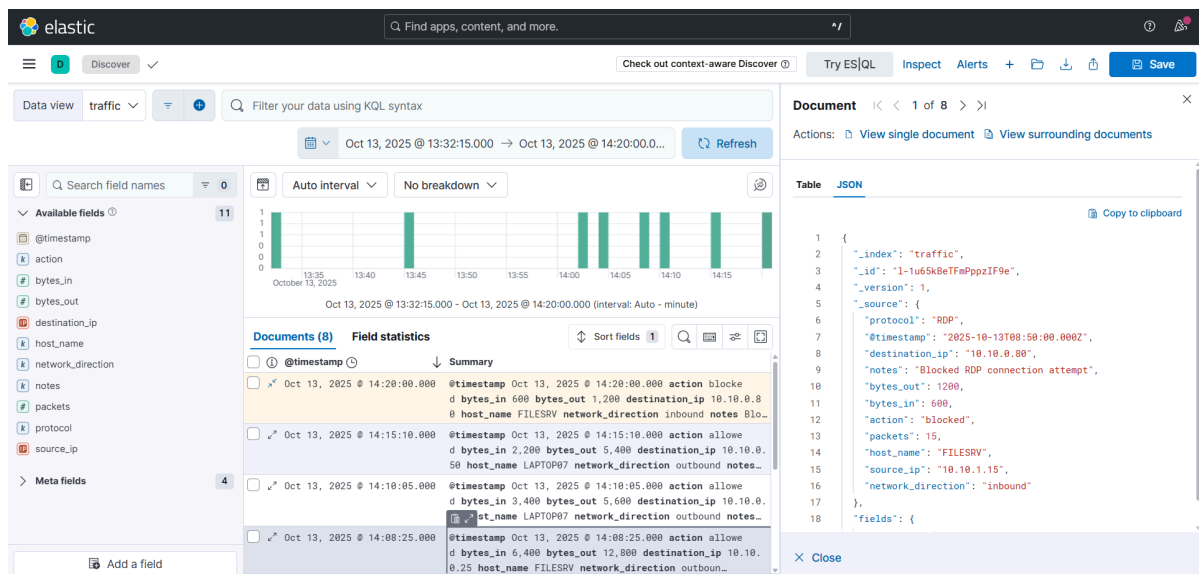
4.1 Ingesting Failed Login Data

Uploading failed login data that is Windows Event Security data it contains the login attempts I uploaded this dataset into Elastic Security and filtered with failed login attempts that it has an Event ID 4625.



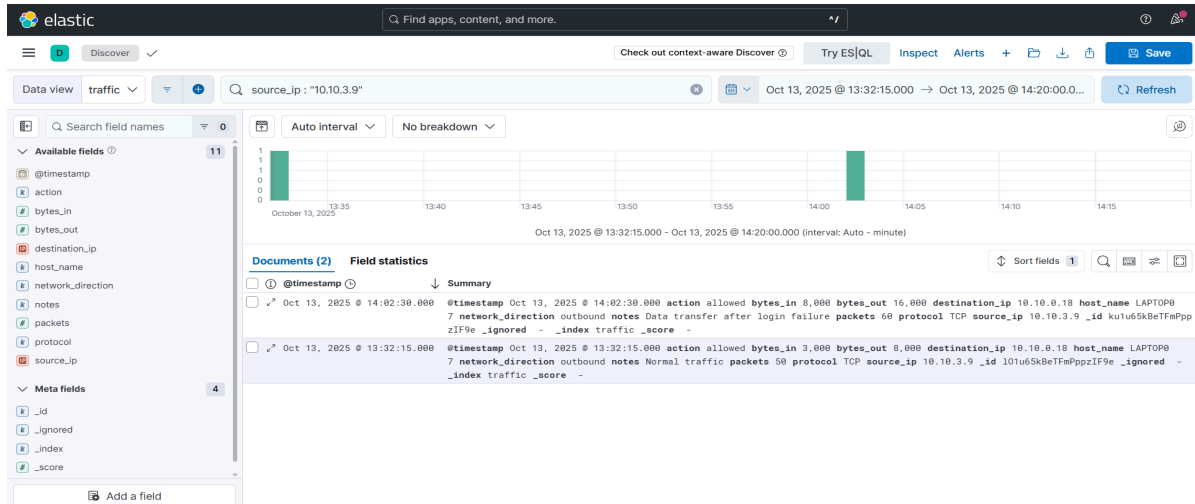
4.2 Ingesting Traffic Data

Uploading traffic data into Elastic Security that it contains the network traffic which is moving outside of the network.



4.3 Correlating Failed Logins With Outbound Traffic

I analyzed failed logins and network traffic in the elastic search with patterns and using kibana Query language I found the one IP address in both the log data that IP at first tried to login to the system and later it sent the traffic outside of the network. The source IP address is 10.10.3.9



4.3 Metadata of the log data

After performing the correlation of both logs I found the IP address that did login attempt and also sent the traffic to the outside of the network. I documented the metadata of the analysis that includes Timestamp, Event ID, Source IP, Destination IP, and Notes.

| Timestamp | Event ID | Source IP | Destination IP | Notes |
|------------------------------|----------|-----------|----------------|--|
| 2025-10-13 T08:32:30:000Z | 4625 | 10.10.3.9 | 10.10.0.18 | After login failed Traffic sent to outside of the network. |

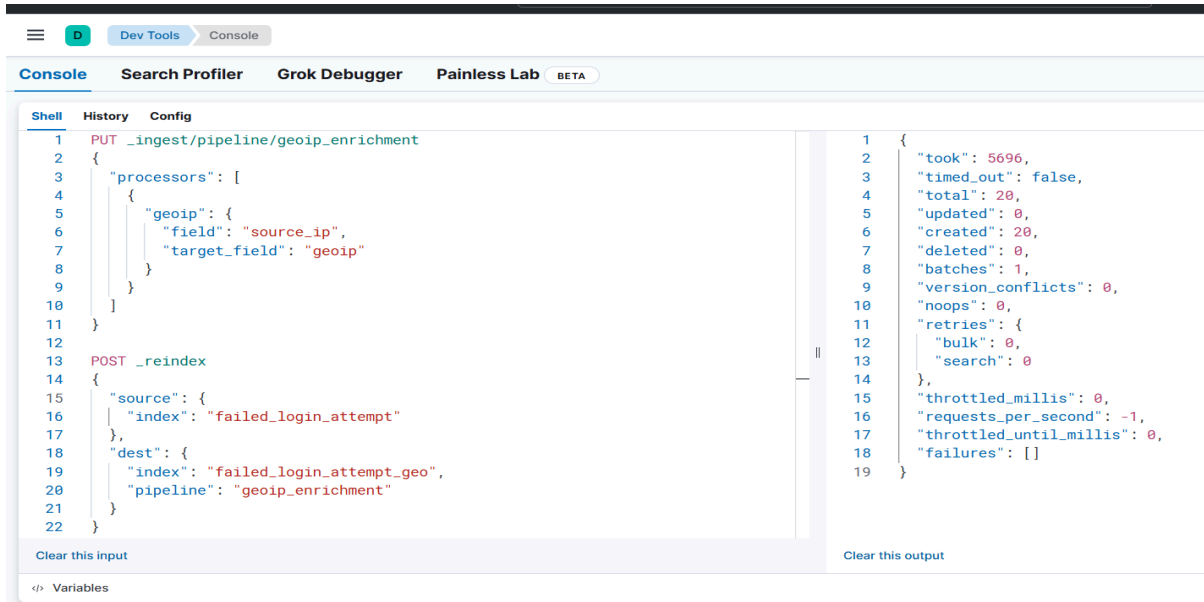
5. Anomaly Detection

Created an Elastic rule to detect high-volume data transfers (e.g., bytes_out > 1MB in 1m). Tested with a mock file transfer.



6. Log Enrichment

Log Enrichment means adding some context to the log data to make it more meaningful analysis. For this enrichment I used a GeoIP plugin process in the Elasticsearch to an IP address that finds geolocation using map in the Elasticsearch.



```

1 PUT _ingest/pipeline/geoip-enrichment
2 {
3   "processors": [
4     {
5       "geoip": {
6         "field": "source_ip",
7         "target_field": "geoip"
8       }
9     }
10  ]
11 }
12
13 POST _reindex
14 {
15   "source": {
16     "index": "failed_login_attempt"
17   },
18   "dest": {
19     "index": "failed_login_attempt_geo",
20     "pipeline": "geoip-enrichment"
21   }
22 }
  
```

```

1 {
2   "took": 5696,
3   "timed_out": false,
4   "total": 20,
5   "updated": 0,
6   "created": 20,
7   "deleted": 0,
8   "batches": 1,
9   "version_conflicts": 0,
10  "noops": 0,
11  "retries": {
12    "bulk": 0,
13    "search": 0
14  },
15  "throttled_millis": 0,
16  "requests_per_second": -1,
17  "throttled_until_millis": 0,
18  "failures": []
19 }
  
```

After creation of above plugin then use it as an layer in the map then it will show the Location of IP address in the map.

