ADVANCE LOG ANALYSIS

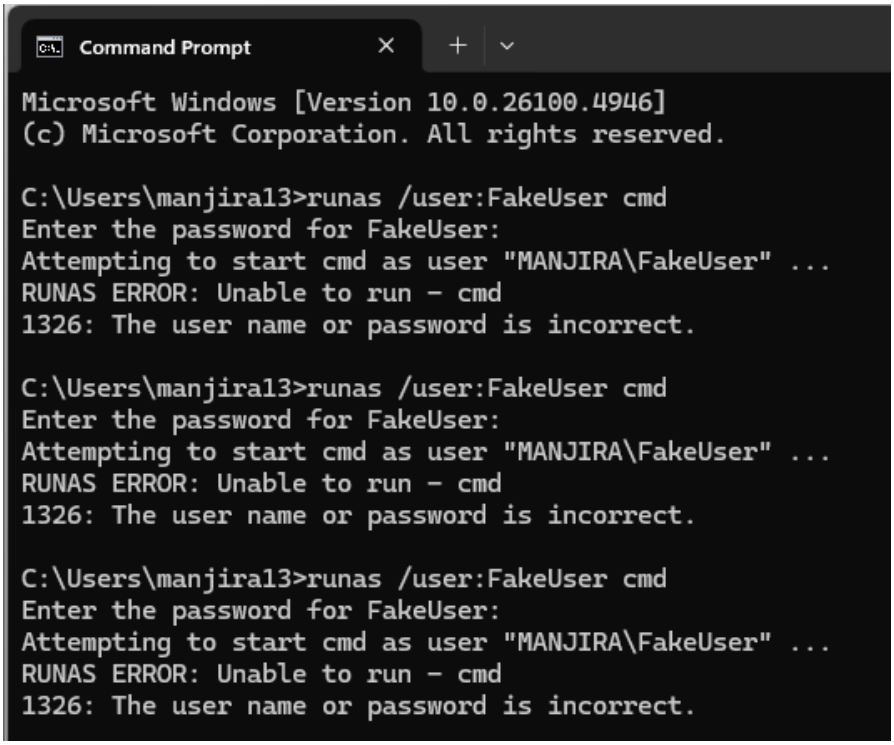
Introduction

This document outlines the process of performing advanced log analysis using Elastic Security, and Google Sheets. The tasks include log correlation, anomaly detection, and enrichment of log data using GeoIP. The purpose is to detect suspicious activities, analyze data flows, and enhance logs with contextual information for improved monitoring and decision-making.

Log Correlation

- **Simulating Failed Logins:**

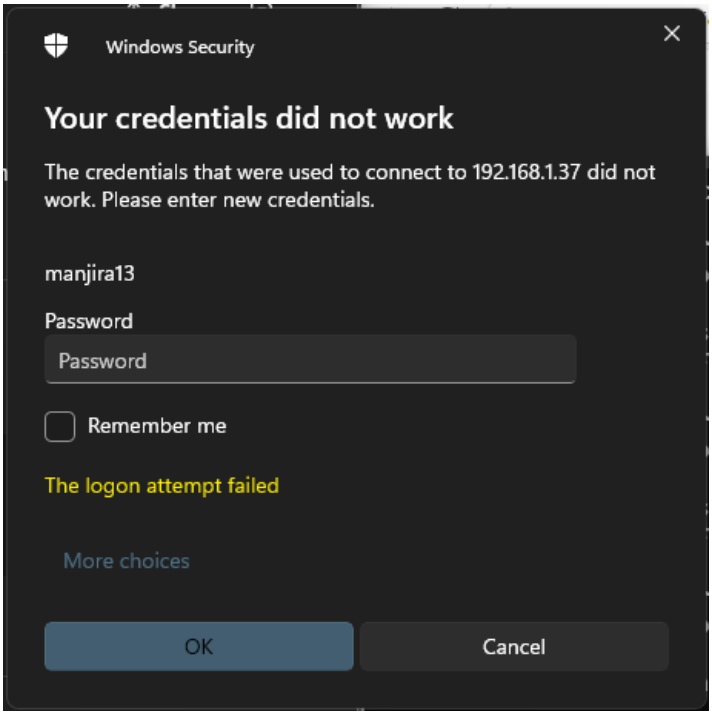
1. **Command Line Attempt (Windows):** 3 times to generate multiple failed login events.



```
Microsoft Windows [Version 10.0.26100.4946]
(c) Microsoft Corporation. All rights reserved.

C:\Users\manjira13>runas /user:FakeUser cmd
Enter the password for FakeUser:
Attempting to start cmd as user "MANJIRA\FakeUser" ...
RUNAS ERROR: Unable to run - cmd
1326: The user name or password is incorrect.

C:\Users\manjira13>runas /user:FakeUser cmd
Enter the password for FakeUser:
Attempting to start cmd as user "MANJIRA\FakeUser" ...
RUNAS ERROR: Unable to run - cmd
1326: The user name or password is incorrect.

C:\Users\manjira13>runas /user:FakeUser cmd
Enter the password for FakeUser:
Attempting to start cmd as user "MANJIRA\FakeUser" ...
RUNAS ERROR: Unable to run - cmd
1326: The user name or password is incorrect.
```

1: FakeUser Login Attempts

2. **Lock Screen Login Attempt:** Entered incorrect credentials multiple times at the Windows lock screen.
3. **RDP Login Attempt:** Attempted remote login with incorrect username/password.



2: RDP Login Attempts

- **Ingest Logs into Elastic Security:**

Load simulated failed login logs using Filebeat to Kibana.

3: Failed Login Attempts Hits

- **Analyze Failed Logins:**

Filter Event ID 4625 in Kibana.

Identify corresponding outbound traffic from the same source IP.

- **Example correlated log entry:**

Timestamp	Event ID	Source IP	Destination IP	Notes
2025-09-02 01:57:20	4625	192.168.1.37	8.8.8.8	Suspicious DNS request

```
PS C:\Program Files\Winlogbeat> Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4625 -or $_.Id -eq 4624} |
>> Select-Object TimeCreated, Id, @{Name='SourceIP';Expression={($_.Properties[18].Value)}}, Message |
>> Format-Table -AutoSize
>>

TimeCreated             Id SourceIP                       Message
-----------             -- --------                       -------
9/2/2025 11:29:44 AM  4625 C:\Windows\System32\svchost.exe An account failed to log on....
9/2/2025 11:29:40 AM  4625 C:\Windows\System32\svchost.exe An account failed to log on....
9/2/2025 11:29:36 AM  4625 C:\Windows\System32\svchost.exe An account failed to log on....
9/2/2025 11:28:06 AM  4625 -                               An account failed to log on....
9/2/2025 11:27:23 AM  4625 -                               An account failed to log on....
9/2/2025 11:27:20 AM  4625 -                               An account failed to log on....
9/2/2025 11:23:29 AM  4625 C:\Windows\System32\svchost.exe An account failed to log on....
9/2/2025 11:23:18 AM  4625 C:\Windows\System32\svchost.exe An account failed to log on....
9/2/2025 11:23:06 AM  4625 C:\Windows\System32\svchost.exe An account failed to log on....
```

4: Corelated Logs from Event Viewer

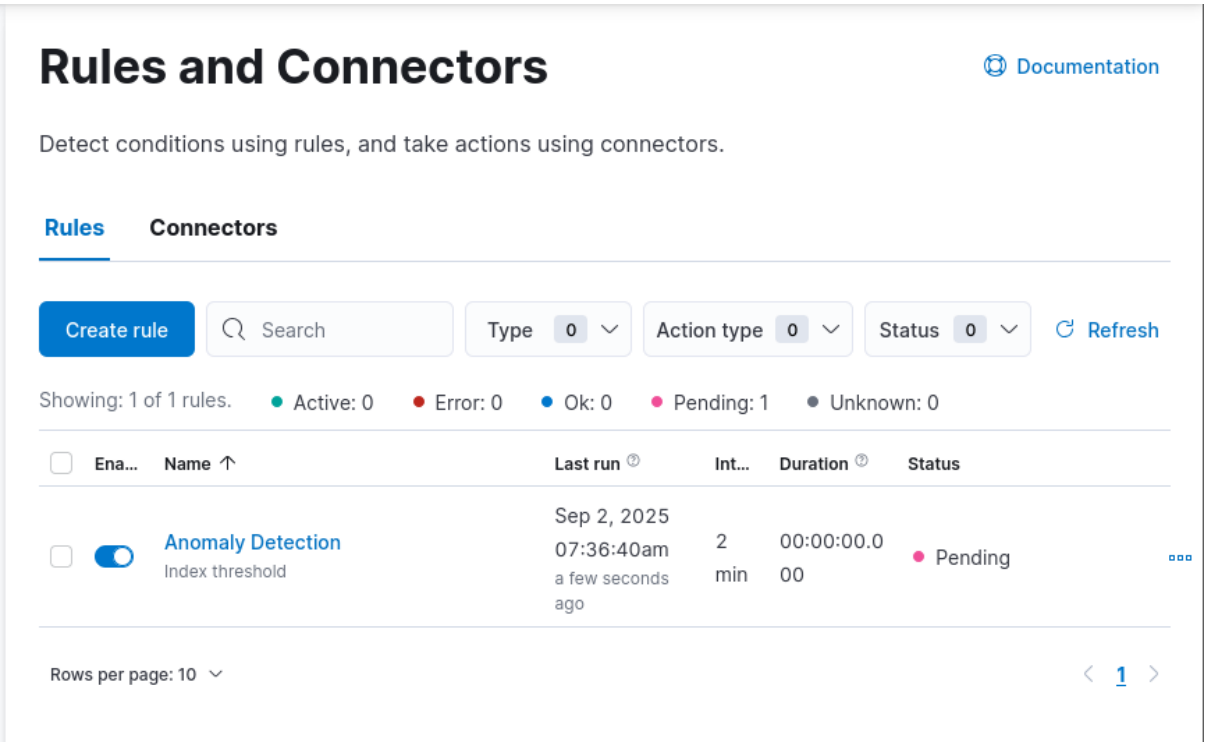
Anomaly Detection

- **Create Elastic Rule:**

1. Detect high-volume data transfers using a threshold.
2. Example: bytes_out > 1MB within 1 minute.
3. Test Rule with Mock Data:
4. Index mock logs into Elasticsearch using Filebeat:

```
POST logs-test/_doc
{
  "@timestamp": "2025-09-02T12:15:00Z",
  "source.ip": "192.168.1.39",
  "destination.ip": "8.8.8.8",
  "network.bytes_out": 2500000
}
```

5. Verify the rule triggers an alert for the high-volume transfer.



5: Anomaly Detection

Log Enrichment

1. Create GeoIP Pipeline:
2. Add geolocation info to IP addresses:

```
PUT _ingest/pipeline/geoip_pipeline
{
  "description": "Add GeoIP info",
  "processors": [
    {
      "geoip": {
        "field": "source.ip",
        "target_field": "source.geo",
        "database_file": "GeoLite2-City.mmdb"
      }
    }
  ]
```

}

3. Verify GeoIP Data:

History Settings Help

```
PUT _ingest/pipeline/geoip_pipeline
{
  "description": "Add GeoIP info",
  "processors": [
    {
      "geoip": {
        "field": "source.ip",
        "target_field": "source.geo",
        "database_file": "GeoLite2-City
          .mmdb"
      }
    }
  ]
}

GET logs-test/_search?pretty&q=*
```

```
      "_score" : 1.0,
      "_source" : {
        "@timestamp" : "2025-09-02T12:15:00Z",
        "source.ip" : "192.168.1.39",
        "destination.ip" : "8.8.8.8",
        "network.bytes_out" : 2500000
      }
    },
    {
      "_index" : "logs-test",
      "_type" : "_doc",
      "_id" : "DF4_CpkBLr-_94d2Jhrh",
      "_score" : 1.0,
      "_source" : {
        "@timestamp" : "2025-09-02T12:15:00Z",
        "source.ip" : "192.168.1.39",
        "destination.ip" : "8.8.8.8",
        "network.bytes_out" : 2500000
      }
    },
    {
      "_index" : "logs-test",
      "_type" : "_doc",
      "_id" : "DV4_CpkBLr-_94d2eBrK",
      "_score" : 1.0,
      "_source" : {
        "@timestamp" : "2025-09-02T12:15:00Z",
        "source.ip" : "192.168.1.39",
        "destination.ip" : "8.8.8.8",
        "network.bytes_out" : 2500000
      }
```

6: Log Enrichment

Check source.geo field for enriched location details (city, country, coordinates). The location details can be determined through the public IP.

Summary of Findings (50 words):

The GeoIP enrichment successfully added location data to IP addresses. The source IP 192.168.1.39 is now associated with geolocation fields such as city, region, and country. This contextual information enhances analysis, enabling faster identification of suspicious or anomalous activities, improving incident response accuracy and decision-making.

Troubleshooting

- Rule Not Triggering: Verify index patterns and time range.
- GeoIP Not Enriching: Ensure GeoLite2-City.mmdb is present in Elasticsearch config directory and pipeline is correctly applied.

- Failed Log Ingestion: Check Filebeat logs for errors and validate configuration using filebeat test config and filebeat test output.

References:

- Elastic Security Documentation: https://www.elastic.co/guide/en/security/current/index.html
- Filebeat Reference: https://www.elastic.co/guide/en/beats/filebeat/current/index.html
- GeoIP Ingest Processor: https://www.elastic.co/guide/en/elasticsearch/reference/current/geoip-processor.html