Advanced Log Analysis Report

1. Executive Summary

This report documents the correlation of authentication failures with outbound network activity, anomaly detection for high-volume data transfer, and log enrichment using GeoIP in Elastic Security. The objective was to identify suspicious behavior indicative of potential compromise or data exfiltration.

2. Environment & Tools

- **Log Sources:**
  - Windows Security Logs (Event ID 4625 – Failed Logon)
  - Network flow / firewall logs
- **Tools Used:**
  - Elastic Security (SIEM)
  - Google Sheets (documentation & correlation)

3. Log Correlation Analysis

Failed login attempts (Event ID 4625) were correlated with outbound traffic originating from the same source IP within a short time window (5 minutes).

Timestamp	Event ID	Source IP	Destination IP	Notes
2025-12-18 12:00:00	4625	10.0.2.8	10.0.2.22	Failed login followed by outbound traffic
2025-12-18 12:01:10	Network	10.0.2.8	10.0.2.22	High-volume data transfer detected

Table 1: Events Table

Analysis

- The source IP 10.0.2.8 generated multiple failed authentication attempts.
- Shortly after the failures, the same host initiated outbound traffic to 10.0.2.22.
- This sequence suggests possible credential abuse, lateral movement, or post authentication reconnaissance/exfiltration.

4. Anomaly Detection

Detection Rule (Elastic Security)

Rule Type: Threshold

Condition:

- bytes_out > 1MB
- Time window: 1 minute
- Grouped by: source.ip

Test Execution

A mock file transfer was performed from 10.0.2.22 > 10.0.2.8.

Result

- Elastic rule triggered successfully.
- Alert severity: High
- Traffic volume exceeded the defined threshold, confirming abnormal behavior.

5. Log Enrichment (GeoIP)

Enrichment Method

Elastic GeoIP processor was applied to network logs using the source.ip and destination.ip fields.

Enrichment Results

- Both IPs resolved to private/internal network ranges.
- No external geolocation was assigned, confirming internal lateral movement, not internet-based traffic.

6. Security Assessment

Indicators of Suspicious Activity

- Failed authentication attempts (Event ID 4625)
- Immediate outbound high-volume data transfer
- Same source IP involved across authentication and network anomalies

Potential MITRE ATT&CK Techniques

- T1110 – Brute Force / Credential Access
- T1078 – Valid Accounts (suspected)
- T1041 – Exfiltration Over Network Channel

7. Conclusion

Failed login attempts from 10.0.2.8 were correlated with high-volume outbound traffic to 10.0.2.22. Elastic anomaly detection confirmed abnormal data transfer exceeding thresholds. GeoIP enrichment identified internal lateral movement, indicating a potential compromised host attempting unauthorized access or data exfiltration.