Advanced Log Analysis

Objective

This task focuses on **advanced log analysis techniques** used in a Security Operations Center (SOC). The goal is to practice **log correlation, anomaly detection, and log enrichment** using SIEM tools and to document findings in a structured, analyst-friendly format.

Tools Used

- **Elastic Security (SIEM)** – Log ingestion, correlation, and detection
- **Security Onion** – Log monitoring (conceptual reference)
- **Google Sheets / Excel** – Documentation and reporting
- **Boss of the SOC (BOTS) Dataset** – Sample security logs

Task Overview

1. Log Correlation

Purpose:
Identify suspicious activity by correlating multiple log sources.

Activity Performed:

- Analyzed Windows Security Logs for **failed login attempts** (Event ID 4625)
- Correlated failed logins with **outbound network/DNS traffic**
- Identified potential post-compromise behavior

Correlation Table:

Timestamp	Event ID	Source IP	Destination IP	Notes
2025-08-18 12:00:00	4625	192.168.1.100	8.8.8.8	Suspicious DNS request

2. Anomaly Detection

Purpose:
Detect abnormal behavior that deviates from baseline activity.

Detection Rule (Conceptual):

```
Trigger alert if bytes_out > 1MB within 1 minute
```

Test Scenario:

- Simulated high-volume outbound file transfer
- Rule successfully triggered an alert

SOC Use Case:

- Data exfiltration detection
- Unauthorized uploads
- Malware command-and-control communication

3. Log Enrichment (GeoIP)

Purpose:
Add contextual intelligence to raw log data.

Enrichment Applied:

- GeoIP lookup on destination IP addresses
- Added country and city information

Example:

IP Address	Country	City
8.8.8.8	USA	Mountain View

SOC Benefit:
GeoIP enrichment helps analysts quickly determine whether traffic is external, unusual, or potentially malicious.

Summary (50 Words)

Log correlation revealed a failed login attempt followed by outbound DNS traffic from the same source IP, indicating suspicious behavior. An anomaly detection rule identified high-volume data transfer suggesting potential data exfiltration. GeoIP enrichment added valuable context, improving investigation accuracy and supporting escalation decisions.