Advanced Log Analysis Report

Log Correlation

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

Log Correlation Analysis

Multiple failed login attempts (Event ID 4625) were observed from source IP 192.168.1.100. Shortly after authentication failures, outbound DNS traffic to 8.8.8.8 was detected from the same host. Correlating authentication logs with network activity helps identify potential brute-force attempts followed by external communication, indicating possible system compromise.

Anomaly Detection

Anomaly Detection Rule

Rule Name: High Volume Data Transfer Detection
Platform: Elastic Security

Rule Condition:
Trigger an alert if outbound traffic exceeds 1MB within 1 minute
(bytes_out > 1MB in 1m).

Purpose:
This rule is designed to detect abnormal data transfers that may indicate data exfiltration, malware activity, or unauthorized usage.

Test Scenario

A mock file transfer of approximately 2MB was performed within 45 seconds. The anomaly detection rule triggered an alert successfully, validating the effectiveness of the detection logic.

Log Enrichment Using GeoIP

GeoIP enrichment was applied to network logs to add geographic context to IP addresses. External destination IP 8.8.8.8 was resolved to a U.S.-based DNS service. Enrichment provides analysts with contextual awareness, helping distinguish internal traffic from suspicious external communications during investigations.