Log Correlation Table and Summary

A. Purpose

To show that the monitoring system (Wazuh) links a local user action (Failed login — Windows Event ID **4625**) with a network consequence (outbound network activity — Wazuh Event ID **61109**). This proves endpoint and network correlation for incident detection.

B. Log 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**

C. Explanation

- 4625 (Failed Login): Recorded when an interactive login attempt fails. Can indicate brute-force attempts, credential errors, or an attacker probing accounts.

D. Summary

Logs were ingested into Elastic Security and correlated to link failed logins with outbound DNS traffic. A custom rule detected high-volume data transfers using network.bytes_out thresholds. GeoIP enrichment added country and city details to IP destination 8.8.8.8, improving contextual understanding of events and supporting faster incident investigation.