Anomaly Detection Summary

Elastic rule detected abnormal file transfer (1MB in 1 min).
Alert triggered and documented.