### Network Traffic → Zeek → Filebeat → Logstash → Elasticsearch → Kibana Optional Additions (Future Enhancements):

1. **ElastAlert (Alerting Tool):**
   * Set up alerts for suspicious activity (e.g., multiple failed logins, port scanning).
2. **Wazuh (Host-based Security Monitoring):**
   * For file integrity monitoring, vulnerability detection, and compliance reporting.