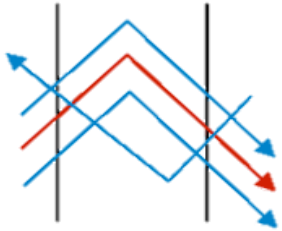
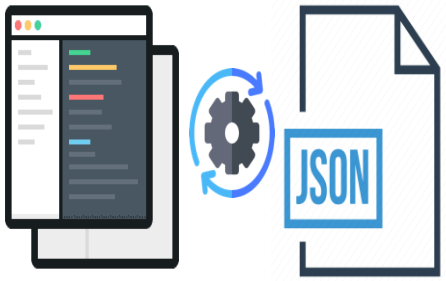
Raw Data Sources



Suricata Logs

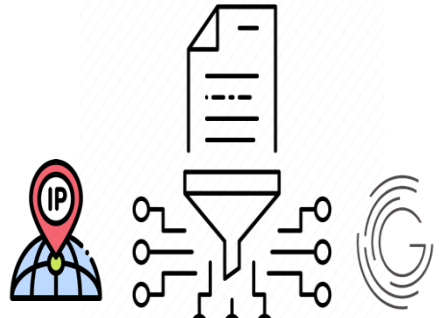
Docker Logs

Parsing & Pre-processing



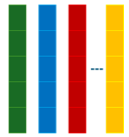
- Field Mapping
- Normalization
- Log Flattening

Filtering & Enrichment



GeoIP/ ASN

Threat Intel



Enriched Data

Clustering Analysis & Insights