```
security-log-analysis/
    ├── logs/
    │   └── sample.log                  # Example input file with raw logs
    ├── output/
    │   └── suspicious_events.txt        # Generated output listing alerts
    ├── src/
    │   ├── parse.py                     # Contains parse_log_line (log
parser)
    │   ├── anomaly.py                   # Contains
detect_threshold_anomalies (threshold-based detection)
    │   ├── correlation.py               # Contains correlate_events (event
correlation rules)
    │   ├── ml_anomaly.py                # Contains MLAnomalyDetector class
+ feature extraction
    │   └── main.py                      # Orchestrator that ties
everything together
    ├── requirements.txt
    └── README.md
```