Lab — Syslog Parsing

- Ingest syslog lines

- Extract events (link flaps, config changes)

- Summarize per device

Objectives

- Parse `common/fixtures/syslog.log`

- Normalize to JSON events

- Count by severity and device

Steps

1. `python day2_cli_to_data/04_syslog_parse.py`

2. Inspect `common/outputs/syslog_events.json`

3. Print summary counts

Validation

- Output JSON exists and non-empty
- At least one event per device

Stretch

- Extract timestamps → ISO-8601
- Add "type" (link, config, auth)