| **Wk** | **Core Focus & Tasks (≈ 15 h)** | **Concrete Artifact(s) to Finish / Commit** |
| --- | --- | --- |
| 1 | • Download Win10 ISO,  create gold VM snapshot  • Init Git repo, add .gitignore  • *SICP 1.1-1.14*  • **Add VS Code Dev-Container (.devcontainer.json)** | Win10\_Ent\_Eval.iso,  snapshot\_win10-gold,  first Git commit,  sicp/ch1\_partA.scm  .devcontainer.json, |
| 2 | • Clone benign-ws01, attacker-ws01 VMs  • Install & harden Sysmon, enable auditing  • Add pre-commit + GitHub CI skeleton  • *SICP 1.15-1.29*  • **Promote dc-srv01 to Domain Controller (corp.local)** • **Create Ansible / DSC “infra-as-code” repo** | sysmon-config.xml, auditpol\_backup.csv, .github/workflows/ci.yml, sicp/ch1\_partB.scm  infra/ansible/, snapshot\_ad-gold, |
| 3 | • Spin up ELK stack; verify logs ingest  • Create Python 3.12 venv, requirements.txt  • Capture 5-min benign trace  • Blog note: “SICP §1 vs Python list-comps”  Docker guides  • **Add Windows Event Forwarding (WEF) collector** and subscriptions | elk.yml, sample Sysmon.evtx, requirements.txt, blog post link  wef\_collector.cfg, |
| 4 | • Write sysmon\_parser.py; draft feature\_schema.json• Init Feast repo + Redis• *SICP 2.1-2.20*  • **Init DVC / lakeFS for raw + parquet data** • **Early ethics / data-protection checklist** • **pytest suite for parser & Feast transforms** | parser script, schema file, feature\_repo/, .dvc/ config, ethics\_form.pdf, tests/test\_parser.py, sicp/ch2\_partA.scm |
| 5 | • Export first Parquet stream (≥10 MB)• Record Pass-the-Hash attack PoC logs• Finish Feast entities• *SICP 2.21-2.34*  • **Run Atomic Red Team pack + record attack traces (Pass-the-Hash etc.)** | /data/raw/attack-poc/…, sample .parquet, sicp/ch2\_partB.scm  atomic\_runbook.yaml, |
| 6 | • Train LogisticReg & RandomForest baselines• Wire MLflow autologging server• *SICP 3.1-3.12*  • **Deploy Suricata (IDS-only) on vSwitch; start Zeek-JSON feed**  • **Mini-presentation #1 (15 min)** | baseline\_eval.ipynb, static\_models.pkl, mlruns/, sicp/ch3\_partA.scm  suricata.yaml, slides\_week6.pdf, |
| 7 | • Add XGBoost & simple MLP baselines• Push results table to repo• *SICP 3.13-3.24* (streams intro) | updated baseline\_eval.ipynb, eval\_metrics.csv, sicp/ch3\_partB.scm |
| 8 | • Finalise baseline figure “ROC-AUC vs model”• Clean CI for notebooks (nbqa + blacken-notebooks)• *SICP 3.25-3.54*  • **Add smoke-test notebook to CI (papermill → pytest)** | metric\_over\_time.png, CI green badge, sicp/ch3\_partC.scm, ci\_notebook\_test.yml, |
| 9 | • Implement ADWIN drift detector; log detections• Begin incremental HoeffdingTree• *Write blog*: “Lazy Streams ⇔ Log Streams” | drift\_detector\_configs.yml, drift\_events.log, blog link |
| 10 | • Add HDDM + adaptive tree; measure detection delay• *SICP 4.1-4.20* (MCE start) | analysis notebook drift\_delay.ipynb, sicp/ch4\_partA.scm |
| 11 | • Integrate active-learning wrapper (uncertainty sampling)• Label-budget metrics• *SICP 4.21-4.40* | active\_learner.py, label\_stats.csv, sicp/ch4\_partB.scm |
| 12 | • Checkpoint online model every 50 k events• Feast stream wiring in River pipeline• *SICP 4.41-4.65* (MCE finished)  • **Mini-presentation #2** | online\_htree.chk, pipeline script updated, sicp/ch4\_mce.scm  slides\_week12.pdf |
| 13 | • Containerise FastAPI stub; deploy to Render (free tier)• Add Dockerfile + compose• *SICP slide-deck*: “Writing an Interpreter”  • **Add Trivy scan in CI for all Dockerfiles** | api\_main.py, Dockerfile, live URL, slide deck PDF, trivy\_ci.yml, |
| 14 | • **Prometheus exporter for latency + cost/resource (node-exporter, cadvisor) + drift alerts**• Grafana dashboard draft• *Start SICP 5.1-5.15* | metrics\_exporter.py, grafana\_dashboard.json, sicp/ch5\_partA.py |
| 15 | • Prefect flow: daily drift-check & retrain trigger• Unit tests for flow; CI passes• *SICP 5.16-5.30*  • **GitHub Actions nightly “concept-drift smoke badge”** | prefect\_flow.py, tests/test\_flow.py, sicp/ch5\_partB.py |
| 16 | • Build evaluation folds (abrupt, gradual, recurring)• Run full online evaluation; capture ops metrics | eval\_fold\_specs.yml, eval\_ops.csv, sicp/ch5\_partC.py |
| 17 | • Optimise inference latency; add Redis cache• Update Grafana “p99 latency” panel | latency\_vs\_load.png, modified dashboard JSON |
| 18 | • Implement GNN baseline; train & save weights• *SICP 5.31-5.45*  • **Mini-presentation #3** | gnn\_model.pt, gnn\_vs\_online.ipynb, sicp/ch5\_partD.py  slides\_week18.pdf, |
| 19 | • Router for A/B testing onlineHT vs GNN; 2-day experiment• **Reflection essay** “SICP ↔ MLOps” | router\_ab.py, ab\_results.csv, Medium essay link |
| 20 | • Analyse A/B results; update Grafana• Medium post #2 “Deploying a Drift-Aware IDS” | dashboard screenshot, blog post link |
| 21 | • Package dataset + code; push to Zenodo• Create CITATION.cff; finish ethics PDF | Zenodo DOI badge, ethics approval PDF |
| 22 | • Draft journal Intro & Methods; compile figs | article\_draft\_v1.tex, figure folder |
| 23 | • Draft Results & Discussion; table polish | results\_table.tex, updated draft |
| 24 | • Internal review; submit to co-authors• Start thesis chapter outlines  Mini presentation | marked-up PDF from co-authors, thesis/outline.md |
| 25 | • Write dissertation Ch 2-3 (Threat Model & Theory) | thesis/ch02.tex, thesis/ch03.tex |
| 26 | • Write Ch 4 (Data Pipeline) | thesis/ch04.tex, pipeline diagram SVG |
| 27 | • Write Ch 5 (Static Baselines) | thesis/ch05.tex |
| 28 | • Write Ch 6 (Drift-Aware Framework) | thesis/ch06.tex, architecture figure |
| 29 | • Write Ch 7 (Evaluation + Ops metrics) | thesis/ch07.tex, combined tables |
| 30 | • Compile full draft; supervisor feedback  Mini presentation | thesis\_draft\_v1.pdf, comment log |
| 31 | • Revise thesis; generate defence slides | thesis\_final.pdf, defence\_slides.pptx |
| 32 | • Record 5-min demo video of live system | Video link in README |
| 33 | • Submit journal (Computers & Security); address reviewer Q1-Q2 | submission confirmation, response letter |
| 34 | • Clean repo; add Zenodo & CI badges; Medium post #3 “Lessons Learned” | updated README.md, blog link |
| 35 | • Present work at local ML meetup; share slides | Meetup slide deck PDF |
| 36 | • Buffer / polish: improve docs, fix tech-debt  Mini presentation | doc updates, issue tracker cleared |
| 37 | • Journal minor revisions (if any); push camera-ready | article\_camera\_ready.pdf |
| 38 | • Thesis defence & final university submission | signed approval form, final PDF in repository |
| 39 | • Job-search sprint: one-pager system diagram + refreshed CV | LM\_IDS\_architecture.pdf, updated CV |

**How to Use the Table**

* **Weekly ritual** – Every Monday morning move that row’s tasks into “In Progress” (15 h budget).
* **Artifacts** – Attach the files/links to the Trello card before moving it to “Done”.
* **SICP cadence** – 3–4 h of the 15 h block stays reserved for *SICP* until week 19, after which the freed time shifts to writing & polish.

Follow the sequence and you’ll finish nine months with:

* a drift-aware IDS running in the cloud, fully monitored and auto-retraining,
* a reproducible PhD dataset + thesis draft,
* a submitted (or accepted) journal article, and
* a deep-CS portfolio that demonstrates *both* theory (*SICP*) and production-grade practice.

Good luck—feel free to ping me when a week’s artifacts are ready and we’ll refine the next sprint!