

About This Class

Agentic Security

Welcome

Introductions

- Your name and team
- Would you consider your AI skills to be beginner, intermediate, or expert? Why?

Welcome

Procedures

- You may pair up
- Questions are welcome and encouraged

Modules

Day 1:

1. **LLM Fundamentals** — what an LLM actually is, tokens to the API
2. **Agents** — tools plus a loop; the pi harness and extending it
3. **Agentic Coding** — good code out of an agent; build ShareBox to spec

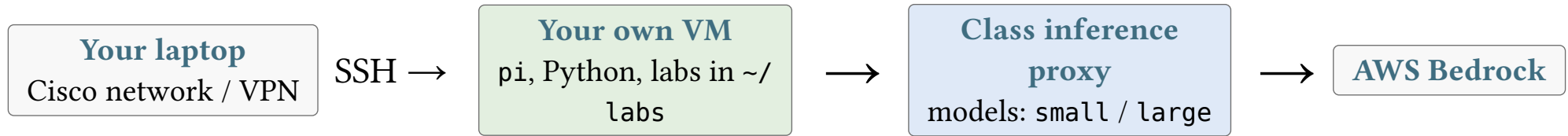
Day 2:

1. **Agent Security** — injection, the lethal trifecta, the defense menu
2. **Security Review** — models as auditors; findings must be exploited

3. **Capstone** — implement Foundry-lite; run it against the vulnbox

Lab Environment

The Shape of It



- **Day 2 targets are personal:** your own SmartMail instances and your own vulnbox, with your own flags
- A **class S3 bucket** moves files around: lab materials, your portal page, reports
- Containment is deliberate: the VM has almost no internet egress — several labs depend on that boundary

More Lab Details

- Be on the **Cisco network or VPN** — the lab only accepts Cisco IP ranges
- Sign in at the class site's **student portal** to download your SSH key and see all your credentials: hostname, API key, Day-2 target URLs
- Two model aliases: `small` (fast, cheap — Day 1 building) and `large` (stronger — Day 2 attacking and auditing)
- Your key has a **hard spend cap** and a **rate limit**; HTTP 429s are normal under load — back off and retry
- Nothing you build here leaves the lab network

Class Website

agenticsecurity.aws.cloud.asig.io



Scan it, or just type it — everything for the class starts here.

II DEMO — the class website

- The homepage: the schedule table and prerequisites
- This deck's page on the site: the written environment tour — come back to it whenever you're lost
- A module page: the slides embedded up top, the lab below them, hints collapsed
- Where solutions live (also collapsed — try first)
- The **student portal**: your key, your credentials, your targets
- The **CTF leaderboard**: register once, submit every flag you capture

Every lab page is self-contained; hints and solutions are collapsed by default.