A free place to practise being a security analyst.

ShiftLab lets you work a made-up security shift. Alerts come in, you investigate, decide what is going on and write the report. It is built for people who want a cyber security career and have never done the job.

WHAT IT IS
A practice site where you work fictional security alerts.

WHO IT IS FOR
Students, career switchers and new Level 1 analysts.

COST
Free. Try it as a guest, no signup.

YOU NEED
No experience and nothing to install.

The problem: beginners rarely get to practise the actual job

A SOC (Security Operations Centre) is the team that watches a company's computers for attacks. The first person to look at each warning is a Level 1 analyst. It is the usual way into the field, and it is hard to prepare for.

28%

Too many alerts, too few people. Security tools raise far more warnings than a team can read. In one 2026 survey, teams left on average 28% of alerts uninvestigated, mostly for lack of time or staff.

Source 1

Up to 1 yr

New hires take months to become useful. In a 2022 survey of 1,250 hiring managers, 37% said entry-level staff work independently within six months. Half said it takes up to a year.

Source 2

Facts, not decisions

Learning material stops short of the job. A lot of beginner material explains what phishing or a stolen password is. The daily work is different: look at messy evidence, decide, and explain your decision.

Author's experience

The figures come from industry surveys. The 2026 survey was paid for by a security company and its answers are self-reported, so read the numbers as a guide, not as a measurement.

What ShiftLab does about it: you practise the decision, not just the vocabulary

Every alert in ShiftLab follows the same four steps a real Level 1 analyst follows. You do it yourself, at your own speed, with hints available and nothing real at risk.

1. **An alert arrives.** You see what the security tool reported, who or what it involves, and when.
2. **Look at the evidence.** Search the logs, check a suspicious link or address, read the forwarded email.
3. **Make the call.** False alarm, real attack, or hand it to a senior analyst (this is called escalating).
4. **Write it up.** Explain your reasoning in a short report. You get a score, what you missed and what really happened.

An example: one alert, start to finish

MADE-UP EXAMPLE, NOT AN ALERT ON THE SITE

Alert: Employee opened a link from a text message claiming to be a parcel company.

1. The alert The web filter noticed an employee's computer visiting a site that looks like a delivery company's page.

2. Evidence The web address is not the delivery company's real address. The site was created two days ago. The page asks for card details.

3. The call Real attack. This is phishing. The open question is whether the employee typed in anything, so check the log of what they sent and escalate if they did.

4. The report A few plain sentences: what happened, what is confirmed, what is still unknown, and what should happen next.

How it helps you

- **Practise the real routine:** Triage, investigate, decide, report. The same cycle you would repeat all day in the job.
- **Make mistakes safely:** Everything is fictional. A wrong call costs you a lower score, not a company's data.
- **Learn from feedback:** After each report you see what you missed and what really happened, then try a similar alert.
- **Get faster under pressure:** Timed drills such as a six-alert shift and a triage sprint train you to pick what matters first.
- **Prepare for the AI era:** Practise checking an AI assistant's summary and finding where it went wrong.
- **Have something to talk about:** Closed cases and written reports give you real examples to describe in an interview.

Who it is for

ShiftLab is for you if you are

- A student aiming for a SOC or other blue-team job
- Changing careers into cyber security
- Self-taught and want practice beyond videos
- A new Level 1 analyst who wants more repetitions

It is not

- A certificate or a course
- A tool for advanced malware or forensics work
- Real company data or real attack tools

Four levels, getting harder: Beginner, Intermediate, Hard, AI Era.

Why I made it

I am a third-year computer science student, and I want to work as a SOC Level 1 analyst. I studied from videos and hands-on labs, and they taught me the words.

What I could not find was a free place to practise the job itself: alert after alert, messy evidence, and a decision I had to make and explain. So I started building one.

Every alert, person and company in ShiftLab is made up and written from scratch. I built it first to practise myself, then to make the same practice easier to find for the next student. I am still adding alerts and fixing things, and I want your honest feedback.

Sai Daswadkar

Try it free as a guest. No signup needed. `shiftlab.blueteam-labs.workers.dev`

Sources: 1. Prophet Security, State of AI in Security Operations (August 2026), as reported by Expert Insights. 250 security professionals; paid for by a security vendor. 2. (ISC)², 2022 Cybersecurity Hiring Managers study (survey run December 2021, 1,250 hiring managers). Harbor & Pine Logistics and everyone in it are made up.