LAYOFFLINK · CAREER HELP

What a resume review looks like

A sample, so you know exactly what you get before you ask. Everything in this document is a fictional example.

FICTIONAL EXAMPLE

What you receive

1. **A marked-up copy of your resume.** Every change is numbered and explained, so you know what to fix and why. (Page 2 shows a sample.)
2. **What works and what to fix first.** Not a long list of everything. The few changes that will matter most for the role you want.
3. **Keywords and tools to add.** The terms recruiters and screening software look for in security roles, matched to the job you are aiming at.
4. **A short plan, if you book the call.** A one-page 30/60/90 plan built from your profile and the skills self-check you send me. (Page 3 shows a sample.)

How it goes

1. **You send a short request** with your situation, goal and skills.
2. **I reply by email** and you send your resume.
3. **You get your feedback** within the time stated on the page.
4. **You tell me how it went.** Honest feedback helps the next person.

Please know. I cannot promise a job or an interview. This is advice and feedback, not a placement service. Your resume and details are used only for your request and never shared or sold.

Sample: the marked-up resume

FICTIONAL EXAMPLE Alex Sample is not a real person.

Alex Sample

IT Support Analyst · Pune, India

SUMMARY

Hardworking IT professional looking for a challenging role [1] in a reputed company.

EXPERIENCE

Handled various security alerts [2] and escalated tickets. Reduced false alarms by 35% by tuning 12 Splunk rules [3].

SKILLS

Windows, Linux, Splunk [4], ticketing tools, phishing triage.

CERTIFICATIONS

CompTIA Security+ (listed at the bottom) [5]

PROJECTS

Home lab with Security Onion and Wazuh (not mentioned yet) [6]

1. Say what you want. Replace it with: "SOC analyst with 3 years of alert triage in a 24x7 team." Name the role.

2. Too vague. Which alerts, and how many? Try: "Triaged about 60 alerts a shift; escalated 3 to 5 real incidents a week."

3. Keep this. A measurable result is what recruiters remember.

4. Show how you used it. "Splunk" alone is only a keyword. "Built searches and dashboards in Splunk" is evidence.

5. Move it up. Put the certificate next to your summary, where it is seen first.

6. Add it. A home lab is real proof of interest. Add one line on what you built and what you learned.

Overall (sample feedback). Strong raw material: real tuning work and a good certificate. The resume hides it. Fix the summary, add numbers to the alert work and move the certificate up, and this reads like a SOC analyst, not a general IT role.

Sample: the one-page roadmap

FICTIONAL EXAMPLE You get this after a 30-minute call, built around your profile.

Goal: SOC analyst (L1) in a mid-size company within 3 months. **Starting point:** 3 years IT support, Security+, Splunk basics.

DAYS 1–30

Fix the base

- Rewrite the resume summary and skills
- Finish 2 SOC labs and note what you did
- Update LinkedIn headline and About

DAYS 31–60

Build proof

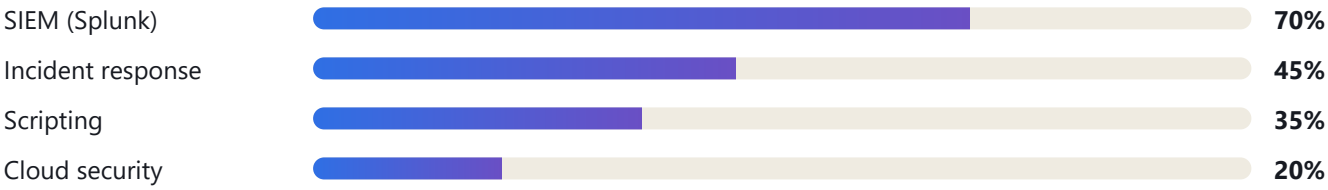
- Write 2 short incident-style reports
- Practise 20 common interview questions
- Apply to 10 matched roles a week

DAYS 61–90

Get interviews

- Two mock interviews with feedback
- Follow up with recruiters and referrals
- Review what is not working and adjust

Gaps to close first (from the skills self-check)



Three things to do this week

- Send the updated resume to one trusted person for a read.
- Finish one incident-response lab and write five lines about it.
- Pick three open roles and compare the keywords with your resume.

Ready for yours? Request a review or a call at **layofflink.com/career-help**. The free skills self-assessment spreadsheet is in the same kit, and filling it in first makes the call much more useful.