North Star Security - Mini-Range Lab 001

Resume Bullet and Interview Prompts

A free SOC-style investigation lab for practicing alert triage, log review, evidence notes, and incident reporting.

Use this after completing the lab and report.

Resume bullet formula

Investigated [event/finding] using [evidence sources], documented [deliverable], and recommended [action/outcome].

Example resume bullet

Investigated a simulated suspicious SSH login by analyzing authentication logs, VPN records, and user context; built a timeline, separated confirmed evidence from unknowns, and produced an incident report with containment and validation recommendations.

Short LinkedIn / portfolio summary

Completed a North Star mini-range investigation focused on suspicious login activity. Reviewed SSH authentication logs, VPN records, and user-directory context to identify a successful login after repeated failures, document evidence, and write a SOC-style incident report with recommended next steps.

Interview story prompt

Use this structure:

1. What was the alert?
2. What evidence did you review?
3. What did you confirm?
4. What stayed unknown?
5. What did you recommend?
6. What did you learn about reporting and evidence?

Example interview answer

I investigated a simulated suspicious login alert where multiple failed SSH attempts were followed by a successful password login for a real user account. I reviewed the authentication log, VPN log, and user-directory context, then built a timeline showing failed attempts, successful login, session start, and a failed sudo attempt. I concluded that the activity should be treated as suspected unauthorized access, but I avoided claiming full compromise because the lab evidence did not include user validation or endpoint telemetry. My recommended next steps were to validate with the user, reset credentials if unverified, review host activity, enable MFA, and search for the source IP across other logs. The main lesson was to separate confirmed evidence from assumptions and write the report so another analyst could review it.