

Cybersecurity Report Writing Starter Kit

Combined kit: reports, evidence notes, portfolio writeups, and resume bullets.

North Star Security

Use this starter kit to turn cybersecurity work into evidence people can understand: reports, evidence notes, portfolio writeups, and resume bullets.

1. Incident report template

Incident title:

Date/time discovered:

Analyst:

Severity: Low / Medium / High / Critical

Executive summary

Write 3-5 sentences explaining what happened, what evidence supports it, impact, and recommended next step.

Timeline

Time Event Evidence

Evidence reviewed

- Alert name / ID:
- Log source:
- Source IP / user / hostname:
- Screenshots or exports:
- Notes:

Findings

- What happened:
- What is confirmed:
- What is suspected:
- What is unknown:

Impact

Explain business or operational impact in plain language.

Recommended actions

1. Immediate containment or validation step
2. Remediation step
3. Follow-up monitoring or documentation step

2. Vulnerability report template

Finding:

Affected asset:

Severity:

Evidence:

Cybersecurity Report Writing Starter Kit

Combined kit: reports, evidence notes, portfolio writeups, and resume bullets.

Risk summary

Explain why this matters without exaggerating.

Technical detail

Describe what was found and how it was identified.

Business impact

Explain what could happen if the issue is exploited or left unresolved.

Recommendation

Write clear remediation steps, including owner and priority when known.

3. Evidence checklist

For each investigation, finding, lab, or portfolio claim, collect:

- Question, alert, finding, or project objective
- System, user, source, or asset scope
- Screenshot, export, or log sample
- Date captured
- What the evidence proves
- What remains unknown or assumed
- Recommended next step
- Portfolio or interview story note

4. Evidence answer framework

Use this pattern:

1. Direct answer: what you found or concluded
2. Scope: where the answer applies
3. Evidence: what supports the answer
4. Limitations: what is not proven yet
5. Next step: what should be validated, fixed, or documented next

Bad answer:

- > It was suspicious.

Better answer:

- > The login pattern was suspicious because the same account had five failed
- > logins from one source IP followed by a successful login from a new location.
- > Evidence includes the authentication log excerpt, timestamps, source IP, and
- > affected username. The next step is to validate whether the user recognizes
- > the activity.

Cybersecurity Report Writing Starter Kit

Combined kit: reports, evidence notes, portfolio writeups, and resume bullets.

5. Resume bullet formula

Use:

- > Investigated [event/finding] using [tool/log source], documented
- > [evidence/report], and recommended [action/outcome].

Example:

- > Investigated SSH brute-force activity using SIEM alerts and authentication
- > logs, documented a timeline and source IP summary, and produced an incident
- > report with recommended account and access-control actions.

Core standard

Investigate. Document. Explain. Defend.