

Incident Report Template

Turn an alert or investigation into a clear report.

North Star Security

Use this template to document a security event in a way another person can understand, review, and act on.

1. Report header

Incident title:

Date/time discovered:

Date/time reported:

Analyst / owner:

Severity: Low / Medium / High / Critical

Current status: Open / Contained / Monitoring / Closed

2. Executive summary

Write 3-5 sentences:

- What happened?
- What evidence supports the finding?
- Who or what was affected?
- What is the current impact?
- What should happen next?

3. Timeline

Time	Event	Evidence source
------	-------	-----------------

4. Evidence reviewed

- Alert name / ID:
- Log source:
- Source IP / destination IP:
- Username / hostname / affected asset:
- Screenshots or exports:
- Ticket or case reference:
- Analyst notes and assumptions:

5. Findings

- What is confirmed?
- What is suspected?
- What is still unknown?
- What was ruled out?

Incident Report Template

Turn an alert or investigation into a clear report.

6. Impact

Explain business or operational impact in plain language. Avoid exaggeration. Tie the impact to the actual evidence.

7. Recommended actions

1. Immediate validation or containment step:
2. Remediation step:
3. Monitoring or follow-up step:
4. Evidence to collect after remediation:

8. Interview story version

- > I investigated [event] using [log/tool/source], built a timeline showing
- > [finding], documented [evidence], and recommended [action].

Core standard

Investigate. Document. Explain. Defend.