North Star Security - Mini-Range Lab 001

Incident Report Template: Suspicious Login Investigation

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

Incident title

Suspicious SSH login for [user] from [source IP]

Executive summary

Write 3-5 sentences explaining what happened, what evidence supports the conclusion, what risk exists, and what should happen next.

Scope

Alert ID:
Affected user:
Affected asset/service:
Source IP:
Review window:
Analyst:

Timeline

```
Time UTC  |  Event  |  Evidence
```

Evidence reviewed

- Alert summary:
- Authentication logs:
- VPN logs:
- User directory context:
- Other notes:

Findings

1. Confirmed:
2. Suspected:
3. Unknown / limitation:

Impact

Explain what could happen if the activity was unauthorized. Avoid exaggerating beyond the evidence.

Recommended actions

1. Immediate containment or validation:
2. Account/security control action:

North Star Security - Mini-Range Lab 001

Incident Report Template: Suspicious Login Investigation

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

---

3. Log review or monitoring action:
4. Documentation/reporting action:

Final status

Open / Needs validation / Contained / Closed

Resume bullet draft

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